Universidad de
SanAndrés

Universidad de San Andrés

Departamento de Ciencias Sociales

Licenciado en Ciencia Política y Licenciado en Relaciones Internacionales

Cibersecuritización: un análisis de discurso, instituciones y documentos oficiales para los casos de Estonia y Reino Unido

Autor: Milagros Urtasun

Legajo: 28112

Mentor: Carina Solmirano

Buenos Aires, noviembre de 2021

Abstract

La siguiente tesis consiste en un estudio que caracteriza los procesos securitizantes del Reino Unido y Estonia. Para ello, se realiza un análisis del discurso de funcionarios públicos, de las instituciones y de los documentos oficiales de cada país. Siguiendo la teoría de la securitización, se estima que las narrativas construirán discursivamente a una amenaza como tal, transformándola en una cuestión de seguridad. Finalmente, se concluye que el éxito del proceso securitizante dependerá de la percepción del riesgo por parte de la ciudadanía, así como del rol que tome la amenaza a securitizar: causante principal del riesgo a la supervivencia del objeto o modalidad que puede tomar otro tipo de amenaza.

Índice

1. Introducción

Gracias a la innovación, la tecnología posee un rol preponderante en el proceso de globalización, las sociedades y los individuos. Más aún, en las últimas décadas, y exacerbado por la pandemia, se ha observado una mayor dependencia a este factor debido a su utilización en todos los planos: desde el entretenimiento y la comunicación hasta el aprendizaje, el trabajo y el acceso a los servicios. Por ende, los beneficios que Internet ha traído causan que sea imposible imaginarnos la actualidad sin el mundo digital.

Sin embargo, la construcción del ciberespacio alteró las relaciones entre los actores estatales y no estatales creando nuevas vulnerabilidades que los ponen a prueba. De esta forma, la velocidad de las interacciones y el desdibuje de las fronteras han incrementado los riesgos y generado nuevos comportamientos como la "diplomacia por tweets", las *fake news* o la facilidad para llevar un tema doméstico a la esfera internacional. Por ello, es necesario estudiar a las Relaciones Internacionales y a la tecnología como fenómenos que se retroalimentan. En otras palabras, existe una relación recíproca y transformativa entre ambas: mientras la tecnología cambia la naturaleza de la política global, la política afecta el ritmo y rumbo del cambio tecnológico. Como refiere Drezner (2019), cada cambio tecnológico representa una nueva redistribución de poder dentro del sistema internacional.

En suma, la tecnología ha irrumpido completamente el ecosistema político, social y económico y, de igual manera, sacude los fundamentos de las Relaciones Internacionales -en particular, del realismo- al potenciar a los actores no estatales y modificar el statu quo. En otras palabras, el estudio de los factores tecnológicos introduce nuevas complejidades respecto a las transiciones de poder y la creación de hegemonías, así como el rol de las instituciones y la gobernanza global de Internet.

Siguiendo esta línea, la innovación tecnológica cuestiona fundamentalmente la mirada tradicional de la seguridad. Bajo esta perspectiva, solamente aquellos Estados con capacidades militares desarrolladas podrían realizar un ataque a gran escala contra otro país. No obstante, Internet ha cambiado esto y cualquier individuo con suficientes conocimientos puede afectar a las grandes economías (Ciolan, 2014). Por ejemplo, los ataques de *ransomware* "Wanna Cry"[1] y

[1] El 12 de mayo de 2017 comenzaron los ataques de ransomware "Wanna Cry" dirigidos al sistema operativo Windows llegando a más de 230.000 computadoras en 150 países. El servicio nacional de salud de Gran Bretaña, Telefónica de España, FedEx, Deutsche Bahn y aerolíneas LATAM fueron algunos de los damnificados cuyos datos fueron encriptados para lo que se les solicitó un rescate económico en Bitcoin.

"No Petya"[2] afectaron servicios vitales, interrumpieron la vida de los ciudadanos y costaron millones de dólares. Así, los ciberataques ponen en jaque el control soberano y poder de los Estados, interrumpiendo el orden y la estructura de la sociedad.

Debido a esto, se observa un cambio de paradigma respecto a la seguridad que nos hace repensar la lógica y la naturaleza de las prácticas. En este sentido, la agenda de seguridad se diversifica entendiendo que no hay temas *per se* de seguridad, sino que estos se construyen a partir del discurso. Dentro de esta transición, se incorpora la ciberseguridad a la agenda actual como uno de sus elementos más preponderantes. Sin embargo, esto dificulta determinar qué debe ser protegido y de qué amenaza (Cornish, Hughes y Livingstone, 2009). Para poder responder a estas inquietudes, la teoría de la securitización de la Escuela de Copenhague busca explicar, a través del análisis de discurso y narrativas, cómo un tema entra a la agenda de seguridad y recibe prioridad por parte de los tomadores de decisiones.

Cabe destacar que la naturaleza de la ciberseguridad no solo se ve modificada discursivamente sino también a través de las prácticas diarias. Debido a esto, y con el objetivo de mitigar posibles amenazas, los gobiernos han adoptado estrategias de ciberseguridad y adaptado sus legislaciones e instituciones (Banco Interamericano de Desarrollo, 2020; Renaud & Warketin, 2018). Así, ha aflorado el desarrollo de políticas y organizaciones domésticas, regionales e internacionales que buscan prevenir, informar y desarrollar las capacidades de ciberseguridad con el fin último de proteger las infraestructuras críticas y a los ciudadanos. A pesar de ello, no todos los gobiernos han sido capaces de instaurar el discurso de seguridad y las acciones consecuentes del mismo modo. Por ello, es posible cuestionarnos: ¿cómo se explica que algunos países logran securitizar la respuesta a las amenazas que plantea la ciberseguridad?

En este sentido, cabe destacar que la ciberseguridad comenzó a tener una mayor preponderancia en el sistema internacional a partir de los ciberataques sufridos por Estonia -identificados por algunos autores como la primera guerra en el ciberespacio-. En 2007, a partir del cambio de lugar de la escultura del Soldado de Bronce, el país báltico sufrió ciberataques continuos contra su infraestructura crítica y sistemas bancarios. A raíz de este hecho, el caso estonio se transformó en un punto crítico para el desarrollo del campo de la ciberseguridad que comenzó a recibir atención pública y priorizarse.

[2] El 27 de junio de 2017 comenzó el ciberataque "Not Petya" afectando principalmente a bancos, ministerios, diarios y empresas de electricidad ucranianas. Al igual que durante el ataque "Wanna Cry", se encriptaron los datos de las computadoras afectadas y se pidió un rescate en Bitcoin.

Sin embargo, Estonia no el único o último país en ser víctima de ciberataques. Por ejemplo, y a diferencia del país báltico, el Reino Unido no ha tenido un único ataque característico, sino que es víctima continuamente de ciberdelitos que, gradualmente, poseen una mayor gravedad. En este sentido, las empresas británicas reportaron 686,961 incidentes durante el 2020 mientras que en 2021 el 39% de los negocios sufrieron este tipo de hechos con 27% que los sufren semanalmente (Johns, 2021). Más aún, se destaca el impacto del ataque sufrido por el Servicio Nacional de Salud en 2017 que afectó a 61 hospitales causando la cancelación de turnos y el cambio de ruta de las ambulancias.

Como se observa, ambos países presentan la oportunidad de estudiar cómo se securitizó la temática en dos contextos de ciberseguridad diferentes. Por un lado, se encuentra un ciberataque de gran cobertura mediática con un límite temporal marcado mientras que, por el otro, una ciudadanía acostumbrada a ciberataques presentes a lo largo del tiempo. Debido a esto, para responder a la pregunta de investigación planteada se realizará un estudio de caso de Estonia y del Reino Unido aplicando como metodología el análisis de discurso para evaluar los procesos cibersecuritizantes. Con este objetivo, en primer lugar, se explorarán las explicaciones que ofrece la literatura. En segundo lugar, se relevarán las teorías que servirán de base para el análisis con foco en la Escuela de Copenhague. En tercer lugar, se precisan las características del diseño metodológico. En cuarto lugar, se analiza cada país de manera separada para luego contrastar los procesos securitizantes. Finalmente, arribaremos a las conclusiones del estudio.

2. Estado de la cuestión

La revolución de la información está incidiendo en el sistema internacional y modificando la estructura y distribución de poder dentro de los Estados. Internet, por ejemplo, cuestiona las ideas occidentales y declina la preponderancia política de las democracias (Lewis, 2021). Como bien se sabe, el poder es un elemento clave en el sistema internacional por lo que es necesario comprender cómo es afectado por el ciberespacio. Para ejemplificar, actualmente la arquitectura de poder se ha tornado cada vez más volátil y compleja enfrentándose a las conceptualizaciones tradicionales de las Relaciones Internacionales (Wenger, 2001).

En este sentido, la emergencia de la Nación-Estado como unidad central de poder fue resultado de la innovación y los cambios. De la misma forma, la revolución de las tecnologías de la información pone en jaque las estructuras cómo las conocemos. Así, estos avances han modificado la manera en la que los actores interactúan entre sí afectando las distribuciones de poder existentes. Para ejemplificar este punto, se ve una desproporción en las cantidades de poder "cibernético" que pueden tener pequeños estados como Estonia o Corea del Norte.

Dentro de este contexto, el campo de la ciberseguridad se ha posicionado en la academia recientemente por lo que su análisis y teorización se encuentra aún en estado madurativo. Si bien Nye (2012) observa que la velocidad de los cambios tecnológicos ha dificultado el desarrollo de teorías, resulta relevante revisar lo que se ha expresado al respecto. Para ello, se dividirá a la literatura en tres áreas que buscan captar la gestión del poder en el ámbito de estudio: la tecnología -y su control-, la seguridad y la comunicación. Cabe destacar que, si bien estos elementos no son mutuamente excluyentes, esta categorización permite ordenar el estado de la cuestión de manera representativa.

2.1. Control de la tecnología

Como se ha expresado, la revolución de la información y, en consecuencia, la influencia del mundo tecnológico en las políticas públicas ha afectado sistemáticamente el estudio de las Relaciones Internacionales (Whyte, 2018). De la misma forma que los barcos permitieron la expansión de Europa entre los siglos 16 y 18, Internet ha traído nuevas oportunidades y desafíos al mundo que se reflejan en rápidos cambios. Así, la aparición de la conectividad ha impactado las interacciones sociales lo que genera modificaciones en las estructuras políticas (Hewitt-Page, 2013). Por ejemplo, Internet tuvo tres grandes efectos en este campo de estudio: (1) amplificó la cantidad de voces interesadas en la toma de decisiones, (2) aceleró la diseminación de la información y (3) alteró la gestión de la diplomacia (Westcott, 2018).

Si bien Internet suele construirse como un espacio sin límites o barreras, sus componentes se encuentran dentro de territorios soberanos. En este sentido, cada gobierno determina el acceso de los ciudadanos a Internet y a la tecnología. Concretamente, países como China, Egipto o Vietnam han censurado páginas web por intereses sociales, políticos o económicos. Cabe destacar que la tecnología no solo es un elemento a controlar, sino que también representa una herramienta para controlar. Debido a esto, comprendemos que los Estados poseen el monopolio de la tecnología y este es un elemento crítico a tener en cuenta al momento de

pensar sobre ciberseguridad. Por ende, en este apartado se hará referencia a los autores que analizan cómo los gobiernos controlan e interactúan a través de Internet observando la infraestructura y operación de Internet, así como las instituciones y los procesos.

Al momento de interactuar con la tecnología, cada Estado utiliza un marco conceptual diferente según sus intereses, vulnerabilidades y, sobre todo, su posición geopolítica. En otras palabras, la preferencia del país respecto a Internet dependerá del régimen social, político y económico (Rousch, 2015). Así, autores como Hall, O'Hara, & Tsalikis (2019) y Fichtner (2018) estudian cómo el lente teórico de los gobiernos va a determinar la forma en la que se utiliza Internet en su territorio y qué políticas públicas implementarán. De esta manera, algunos estarán más enfocados en la protección de la información mientras que otros buscarán controlar la comunicación.

Sin embargo, Internet se encuentra gobernado por una multiplicidad de actores cuyo comportamiento sólo puede ser restringido voluntariamente lo que genera que su gobernanza no tenga una autoridad centralizada (Eggenschwiler, 2017; O'Hara & Hall, 2018). Debido a esto, y la abundancia de áreas interconectadas, los gobiernos deben cooperar con el sector privado si desean mitigar posibles ataques cibernéticos. Colaborar con las empresas genera que el campo de la ciberseguridad sea difuso, pero a su vez promueve la resiliencia nacional (Inglis & Jensen, 2020). En este sentido, compartir información relacionada a vulnerabilidades, tendencias de hackeos o anormalidades permite que tanto el sector de las TICs como el Estado puedan proteger mejor sus sistemas críticos y mitigar problemáticas emergentes (Goodwin & Nicholas, 2013). De acuerdo con la declaración de Charlevoix en el marco del G7, la protección del ecosistema digital global solo puede realizarse junto al sector privado, la sociedad civil y los ciudadanos (Pernice, 2019).

A pesar de esta característica del entorno digital, los gobiernos son capaces de determinar las políticas y los mecanismos que afectan a aquellos que controlan los recursos creando límites e incentivos a través de políticas públicas. Para ejemplificar, y como se analizará posteriormente, si el gobierno no posee control sobre la tecnología, buscará moldear las políticas, generar apoyo y crear justificaciones para cumplir sus objetivos (Calås, 2019). Esto se logrará principalmente moldeando la opinión pública para dar legitimidad a los rumbos de acción propuestos. En este marco, los mensajes estatales tenderán a ser más efectivos cuando coincidan con los intereses y las ideologías de la población o el grupo que recibe el discurso (Bada, Sasse, & Nurse, 2019).

2.2. Monopolio de la seguridad

Desde el comienzo de la convivencia social, los hombres han tenido la dificultad de coexistir bajo una relativa estabilidad y seguridad. Frente a esto, las sociedades aceptan tener un Estado que garantice las libertades básicas de las personas. Siguiendo lo expresado por Weber, el Estado será aquel que reclame para sí exitosamente el monopolio de la fuerza legítima en un territorio. Aún más, la legitimidad de la nación proviene de representar a las personas de ese territorio lo que genera que la noción abstracta de poder se encuentre vinculada fuertemente a la territorialidad (Funk, 2003; Hewitt-Page, 2013). Sin embargo, la tecnología y la globalización nos hace repensar esta cuestión: ¿cómo es capaz el gobierno de controlar un territorio cuando sus límites se vuelven cada vez más difusos y hay una desterritorialización de la política? Más aún, estos elementos generan constantemente nuevas vulnerabilidades que ponen en jaque la habilidad de los gobiernos de mantener el monopolio de la seguridad.

Ahondando en esto, a partir del fin de la Guerra Fría los conflictos se han desenvuelto en diferentes campos de batalla dentro de los cuales se encuentra el ciberespacio. La globalización, en conjunto con el surgimiento de nuevos actores, ha generado un nuevo tipo de guerra que oscurece las diferencias entre la guerra como la conocemos teniendo nuevos métodos, objetivos y accesos a financiamiento (Dewi, 2020). Por ejemplo, los grupos hostiles -que no se encuentran limitados por las mismas normas- pueden sobrepasar las fronteras y desafiar a los Estados en el ciberespacio (Calås, 2019; Lacy & Prince, 2018). Más aún, este dominio ofrece poder excesivo a actores pequeños o irrelevantes, facilita llevar adelante una agenda política sin conflicto armado, las fronteras dejan de existir claramente y la anonimidad protege a los perpetuadores dificultando, así, un monopolio legítimo y robusto de la seguridad.

Por ende, la naturaleza interconectada de nuestra realidad genera que un ataque en el ciberespacio se magnifique creando una gran inestabilidad para todo el sistema (Virilo, 2007). A modo de ejemplo, un ataque cibernético podría afectar transformadores eléctricos, trenes, redes de comunicación y entidades financieras, entre otros. En este sentido, la tecnología permite que se realicen delitos anteriormente inexistentes, así como que delitos convencionales se presenten de manera diferente (Tabansky, 2012). De esta forma, los límites entre intereses privados/económicos y públicos/de seguridad pasan a agregarse en una constelación de responsabilidades y autoridades.

Sin embargo, no hay ningún ejemplo de ciberataque que haya tenido la letalidad de un conflicto o una guerra "clásica" debido a su baja capacidad violenta. Por el contrario, el debate actual sobre esta temática utiliza principalmente analogías con grandes eventos históricos (Schmidt, 2014). Debido a esto, gran parte de los autores consideran que es muy poco probable que haya un conflicto en el cual la principal arma sea cibernética. Igualmente, cabe recalcar que Internet se presenta como una forma de financiamiento para grupos criminales y terroristas que utilizan fraudes y robos a cuentas bancarias para captar dinero y sostener su accionar (Vargas Vargas, 2014).

Para resumir, este tema se ha transformado en un punto estratégico de suma importancia para los tomadores de decisiones al desestabilizar la arquitectura de poder y ubicar como protagonistas a actores previamente rezagados. En este sentido, los ciberataques pueden ser desde crímenes individuales de bajo nivel hasta ataques organizados por terroristas y pueden afectar al Estado, a entidades privadas o a individuos. Frente a esto, los Estados van a alocar los recursos necesarios para preservar su soberanía, sin poder escapar al axioma de la primacía de la seguridad (Baldwin, 2011).

2.3. Narrativas y manejo de la comunicación

La confianza de los ciudadanos en los gobiernos es un elemento clave para una gobernanza exitosa. Gran parte de la política ingresa a la vida de las personas a través de los medios de comunicación los cuales facilitan que se instalen ideas y valores en la sociedad. Esto genera, junto a la globalización, que áreas previamente despolitizadas incluyan a una variedad de actores o que temas previamente domésticos movilicen a las sociedades en todo el mundo (Leander, 2002). En este sentido, los medios de comunicación pueden iluminar ciertas temáticas y generar que los ciudadanos demanden una respuesta de los gobiernos o convencerlos sobre el accionar del Estado.

Siguiendo este punto, según el tono y el contenido que muestran los medios de comunicación, estos podrán incidir en la legitimación del accionar estatal por parte de la ciudadanía (Joseph, 2014). De la misma forma, podrán acelerar o no cambios del statu quo; rol que ha ganado aún mayor preponderancia gracias a la tecnología. En este sentido, en un mundo globalizado cómo la información es mostrada y la calidad de esta ayudará a determinar las estructuras políticas y sociales (Joseph, 2014). Como se verá a continuación, este rol es de suma importancia dentro del campo de la seguridad.

El poder de los medios de comunicación de determinar la agenda, así como las percepciones de seguridad impactará fuertemente en las sociedades y sus propias conceptualizaciones. En este sentido, los discursos sobre temáticas de seguridad pueden generar mayor inseguridad en los ciudadanos al incorporar el sentimiento de riesgo (Kernic, 2008). Para ejemplificar, Hunt (1997) predice conflictos internacionales a través de indicadores de los medios de comunicación que reflejan cuándo los gobiernos buscan apoyo público. Kostyuk & Wayne (2020), en cambio, analizan las percepciones de ciberseguridad de los individuos y sus conocimientos concluyendo que mayor exposición a ciberataques genera mayor percepción de riesgo y, así, validación de una mayor inversión en políticas de ciberseguridad. De esta manera, conocer la percepción de riesgo de la audiencia es vital para comprender qué rumbos de acción tomará el Estado.

Entonces, la agenda de seguridad expresará quién decide, quién obedece, sobre qué y cómo (Attiná, 2001). De esta forma, si la audiencia está preocupada sobre una temática en particular, será más fácil para los políticos invertir en esa área (Kostyuk & Wayne, 2020). Contrariamente, si el público no problematiza una temática, será más costoso para los funcionarios poder cambiar el statu quo. En suma, a través del uso del lenguaje se puede articular una cultura estratégica sobre las cuestiones de seguridad que se expresará en creencias, actitudes y patrones de pensamiento (Bartolomé, 2016).

Cabe destacar que los ciberataques no suelen ser mostrados en los medios de comunicación masiva y sus efectos no exhiben violencia directa por lo que los ciudadanos suelen subestimar su frecuencia e impacto. A pesar de ello, también pueden causar muertes, disminuir la calidad de vida de las personas o afectar a los sistemas políticos a través de la interferencia en campañas electorales que inciden negativamente en la calidad democrática y la legitimidad estatal (Donahoe & Hampson, 2018; Straub, 2019; Whyte, 2018).

3. Marco teórico

En esta sección se analizarán brevemente los principales conceptos teóricos y desarrollos presentes en el área de la ciberseguridad para insertar este trabajo en la literatura de Relaciones Internacionales existente. Con este fin, se comenzará describiendo la evolución de la agenda de seguridad y el efecto que ha tenido la tecnología en ella. Luego, se focalizará en la securitización y los aportes de la Escuela de Copenhague. En suma, se rescata que las dinámicas sociales

inciden en la manera en la que los temas políticos y estratégicos son pensados y problematizados (Whyte, 2018). Por ende, este trabajo busca incorporarse dentro del cuerpo de literatura sobre la ciberseguridad, considerando que la falta de investigación y consensos en esta temática es una oportunidad para el análisis.

3.1. La agenda de Seguridad Internacional

Como se ha expresado, la globalización ha modificado las relaciones entre los actores del sistema internacional al generar interdependencia y una mayor penetración de las personas, las ideas y los bienes sin importar las fronteras. El campo de la seguridad no ha sido ajeno a estos cambios. A continuación, se relata brevemente la evolución de la seguridad para, luego, focalizar en el campo de la ciberseguridad.

3.1.2. Evolución del concepto de Seguridad Internacional

La noción de seguridad es en sí misma ambigua al ser un objetivo, una disciplina, un concepto y mucho más. A su vez, se encuentra categorizado en diferentes dominios: seguridad nacional, seguridad internacional y seguridad global, entre otros; cada uno respondiendo a valores y amenazas específicas (Haftendorn, 1991). Sin embargo, esta noción y sus derivaciones no son fijas. Por el contrario, se fueron transformando a lo largo del tiempo y, en particular, a partir de la Guerra Fría.

La Seguridad Internacional es un lente dentro de las Relaciones Internacionales que articula sus debates alrededor de las amenazas existentes en el sistema internacional y sus posibles efectos (Bartolomé, 2018; Orozco, 2006). En otras palabras, refiere a la aceptación de una vulnerabilidad propia del sistema y mutua de los actores que permite patrones de estabilidad. Por ende, buscará responder a las principales preguntas sobre la guerra y la paz, así como estudiar aquellos fenómenos que puedan desestabilizar a la arquitectura internacional (Freedman, 1998).

A partir del fin de la Guerra Fría, y en un mundo cada vez más interconectado, la seguridad internacional ha mutado, al igual que su alcance, sus agentes y objetos. En este sentido, tradicionalmente se conceptualizaba como agentes a los Estados mientras que actualmente aparecen unidades subestatales -como terroristas u organizaciones de crimen organizado- que generan que los conflictos sean irregulares. Así, los Estados no solo han perdido su lugar central como ejecutores, sino también como objetos en peligro. Gracias a la Escuela de Copenhague, se

ha expandido el alcance de la seguridad a nuevos dominios por fuera del ámbito militar. En esta línea, también han ganado primacía las temáticas regionales y étnicas (Cha, 2000).

Desde una perspectiva tradicional, la seguridad se encontraba fuertemente vinculada al territorio, es decir, al lugar físico y palpable. Sin embargo, la tecnología permitió la creación de nuevas armas que modifican la distribución de poder en el sistema internacional y trasladan la guerra a otra arena con reglas diferentes (Cha, 2000; Schmidt, 2014). Así, junto a la diversificación de amenazas aparece un novedoso plano no físico de la seguridad para los Estados, los actores no estatales y los individuos. Este trae aparejado nuevas formas en las que los Estados pueden perder su soberanía y legitimidad.

Sin embargo, estas amenazas deben ser enfrentadas conjuntamente por los actores del sistema internacional para que puedan defenderse con éxito. Por ende, como respuesta a esta necesidad aparece el concepto de seguridad global: un set de ideas desarrollado por las Naciones Unidas que descansa en la premisa que, sí sola nación no es segura, ninguna lo es (Holmes, 2015). Similarmente a la cultura kantiana, la seguridad de un Estado es la seguridad de todos y el interés nacional o individual será el interés del total (Wendt, 1999). Así, la cooperación y compañerismo son posibles.

Siguiendo esta línea, la seguridad global busca la transformación del sistema internacional para poder garantizar la seguridad común y la paz global. Para ello, se requiere un concepto universal de seguridad que permita normas, valores y prácticas compartidas por todos los actores del sistema (Haftendorn, 1991). Esta noción es de suma importancia al pensar la ciberseguridad ya que el ciberespacio borra los límites territoriales y sus amenazas deben ser enfrentadas de manera simultánea a nivel estatal, regional y global.

En suma, se observa un pase de la noción tradicional a la incorporación de actores, dimensiones de poder, objetos de estudio e interacciones (Oggesen, 2020). Frente a los desafíos del mundo globalizado, aparecen nuevos conceptos de seguridad que buscan captar la interdependencia de los actores y la necesidad de responder en conjunto. En particular, los ataques cibernéticos demuestran lo difuso de los límites territoriales y la incapacidad de defenderse individualmente. Entonces, es necesario integrar la tecnología al estudio de la seguridad ya que posee la capacidad de generar cambios sistémicos (Fritsch, 2011).

3.1.2. Ciberespacio, ciberseguridad y ciberguerra

En 2008, durante el conflicto armado entre Georgia y Rusia, se realizaron ataques cibernéticos a los sitios web del gobierno georgiano reduciendo su comunicación con los ciudadanos. En 2010, al inspeccionar una planta nuclear en Irán, los inspectores de la Agencia Internacional de Energía Atómica notaron que las centrifugadoras para enriquecer fallaban. Meses después se encontró la causa: el gusano Stuxnet había tomado control de máquinas de la producción atómica y les había ordenado autodestruirse. En 2013, tuvieron lugar las filtraciones de Edward Snowden sobre el alcance del espionaje de la Agencia Nacional de Seguridad de Estados Unidos, información que generó un clima de desconfianza mundial y tensionó las relaciones entre los aliados. Si bien todos estos hechos no tuvieron consecuencias a largo plazo, demostraron el potencial destructivo de los ataques cibernéticos y su capacidad para generar confusión y miedo.

Todas estas acciones responden a la definición tradicional de amenaza, aun teniendo lugar en el ciberespacio, ya que pueden afectar de manera drástica y en el corto plazo a la calidad de vida de la población y/o reducir las opciones del Estado (Bartolomé, 2016). Más aún, cualquier medio dependiente a Internet (como sistemas de transporte o servicios públicos) pueden ser objeto de ataques cibernéticos, convirtiéndose en un objetivo estratégico de seguridad. En este sentido, las personas son cada vez más dependientes de la tecnología generando que los Estados y sus infraestructuras críticas sean más vulnerables. Es importante destacar que el ciberespacio fue creado por las personas por lo que, a diferencia de los otros dominios, persigue determinados intereses políticos, sociales y económicos.

A continuación, se verán brevemente tres elementos con el objetivo de situar al lector en el campo del ciberespacio: su definición, la gobernanza de este dominio y el comportamiento de los individuos en él.

Definición

De acuerdo con Llongueras Vicente (2013), el ciberespacio se construye como un elemento de poder dentro de la seguridad al influenciar estratégicamente el siglo XXI y, así, transformarse en un aspecto clave en la política y la ejecución del poder. Por ende, se ha ampliado las disciplinas envueltas en el estudio de este campo que antes estaba focalizado en las Ciencias de la Computación. A pesar de ello, la veloz aparición de la ciberseguridad en las Relaciones Internacionales ha dificultado definir claramente el concepto (Calås, 2019). De esta manera, el

término se ha utilizado ampliamente de manera subjetiva y sin una descripción que capture su multidimensionalidad.

Craigen, Diakun-Thibault y Purse (2014) buscan solucionar esta problemática al crear una nueva definición utilizando los conceptos presentes en la literatura. Para los autores, la ciberseguridad es “the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." (pp. 13)

Gobernanza

Si bien la integridad, la autenticidad y la confidencialidad de la información dentro del ciberespacio se han transformado en una prioridad del siglo XXI, la aparición de amenazas que afectan la estabilidad de los Estados ha hecho que se requiera una gobernanza expansiva (European Network and Information Security Agency, 2012). Una verdadera administración de este dominio requiere una gran cooperación internacional, así como la realización de acuerdos y legislación internacional para regular los sistemas de información y combatir el cibercrimen (Vargas Vargas, 2014). Más aún, la dependencia transnacional que presenta Internet crea la necesidad de instituciones globales para que su regulación sea efectiva (Mueller, Schmidt, & Kuerbis, 2013).

Ahondando, los grupos cibercriminales no operan únicamente dentro de las fronteras nacionales por lo que los riesgos relacionados no pueden ser prevenidos solo a través de la defensa doméstica (Goodwin & Nicholas, 2013). Lograr la estabilidad cibernética global depende de la capacidad nacional de todos los países para prevenir, reaccionar e investigar delitos cibernéticos ya que estos hechos pueden propagarse con facilidad de un territorio a otro (Banco Interamericano de Desarrollo, 2020). En este sentido, y considerando el alto nivel de interconexión, las organizaciones regionales tienen un rol primordial para lograr la cooperación entre países. Así, debido a la naturaleza del ciberdelito y los elementos nombrados, los límites jurisdiccionales clásicos dejan de tener efecto (Temperini, 2018).

Comportamiento

No obstante, el principal origen de las vulnerabilidades son errores de los usuarios por lo que la ciberseguridad no depende únicamente de las acciones estatales sino también de las actitudes individuales. Frente a esto, los gobiernos pueden mitigar la amenaza desarrollando políticas de seguridad especificando el correcto uso para los ciudadanos. Sin embargo, influenciar el

comportamiento implica, más allá de la educación y disponibilidad de la información, comprender si los ciudadanos perciben el riesgo (Bada, Sasse, & Nurse, 2019). Esta percepción podrá depender, por un lado, de la cercanía a ataques cibernéticos y, por el otro, a las narrativas presentes en los medios de comunicación.

En suma, la ciberseguridad y ciberdefensa aparecen como ejemplo de nuevas amenazas en las que se requiere la colaboración público-privada y doméstica-internacional por sus características. En esta línea, las acciones estatales deberán ser complementadas por el sector privado a la vez que se educa a la ciudadanía para comprender el riesgo. Como se ha expresado, estos hechos tienen la posibilidad de interrumpir la vida en sociedad y el accionar de los Estados, sin embargo, no prepondera el estudio sobre estas temáticas desde las Relaciones Internacionales lo que dificulta definiciones claras (Rousch, 2015).

3.2. Escuela de Copenhague: argumentos y críticas

La incidencia de la globalización en las sociedades y las características del mundo interconectado generaron dificultades para aplicar los conceptos tradicionales a la nueva realidad. A pesar de ello, en la actualidad se ha observado una diversidad teórica en los fenómenos del mundo digital que captan de mejor manera sus vetas (Cavalety, 2000). Dentro de esta, la teoría de la securitización presentada por la Escuela de Copenhague se destaca como subdisciplina de los estudios de seguridad. Más aún, es uno de los enfoques que más influyó en la apertura de la agenda de seguridad (Hansen & Nissenbaum, 2009). En este apartado, se comenzará resumiendo el proceso de securitización para luego, focalizar en la cibersecuritización y la desecuritización. Finalmente, se hará referencia a las principales críticas de la literatura.

3.2.1. El proceso securitizante

La teoría de la securitización explica el proceso a través del cual se constituye discursivamente un problema de seguridad. Según Balzacq, Léonard y Ruzicka (2016), un actor securitizante moviliza elementos del discurso para incentivar a una audiencia a construir implicaciones sobre la vulnerabilidad de un objeto referente que debe ser protegido. En otras palabras, a través de narrativas se construye discursivamente a una amenaza como tal, transformando a una temática en una cuestión de seguridad. Así, se transforma al sujeto referente en una amenaza sin precedentes que debe ser combatida mediante políticas extraordinarias.

Dentro del proceso descrito por Buzan, Waever, & De Wilde (1998), existen ciertos elementos facilitadores para su éxito: (1) demanda interna que la comunicación siga la gramática de la seguridad, (2) condiciones sociales respecto al actor securitizante y, (3) características de la amenaza. De esta forma, gran parte del éxito del actor securitizante obedecerá a su habilidad de identificar los sentimientos, intereses y necesidades de la audiencia. Las ideas, entonces, tendrán un rol preponderante al construir los imaginarios políticos y sociales ya que guían el pensar ordenando racionalmente del mundo (Bartolomé, 2018).

Así, y en consonancia con la ampliación de la agenda de seguridad, el discurso puede incluir otros actores referentes más allá del Estado y el sector militar (Hansen & Nissenbaum, 2009). Por ejemplo, la Escuela de Copenhague posee diferentes niveles de análisis (sistemas, subsistemas, unidades, subunidades, individuos) que permiten dejar de lado la mirada tradicional de que el Estado es el único objeto referente (Rousch, 2015). En este sentido, la securitización ha sido de gran utilidad para comprender la formulación de la tecnología como una amenaza a la seguridad nacional y los intereses estatales, avalando la utilización de medios coercitivos (Mueller, Schmidt, & Kuerbis, 2013). La literatura dentro de este campo ha estudiado, principalmente, las estrategias de ciberseguridad, los discursos públicos de los dirigentes y las políticas públicas.

3.2.2. La cibersecuritización

Como se ha expresado, la securitización se ha aplicado a diversos contextos empíricos, transformándose en un punto focal para los debates teóricos sobre las implicancias del discurso de seguridad. Sin embargo, Hansen & Nissenbaum (2009) argumentan que la ciberseguridad debe ser considerada como un sector diferente dentro de la teoría debido a la diversidad y cantidad de amenazas y objetos referentes que posee. En otras palabras, al encontrarse interconectados diferentes objetos referentes el potencial de la ciberseguridad gana profundidad y cobertura de posibles futuros incidentes. Por ejemplo, gran parte del discurso securitizante ha utilizado analogías históricas como "el Hiroshima de la ciberguerra" o "un Pearl Harbor digital" (Geelen, 2016).

Siguiendo esta linea, las autoras identifican tres modalidades de securitización específicas para el sector de la ciberseguridad. En primer lugar, la hiper securitización implica la exageración de las amenazas y contramedidas. En segundo lugar, las prácticas de seguridad diarias refieren a la

forma en la cual los actores securitizantes movilizan las experiencias de la audiencia al relacionar experiencias familiares de la diaria con escenarios de desastre. En tercer y último lugar, la tecnificación surge al enfatizar en escenarios hipotéticos que crean un espacio para el discurso técnico.

En suma, la cibersecuritización se propone como un lente específico dentro de la teoría debido a las constituciones particulares de objetos referentes, amenazas y gramáticas de securitización que posee. Ahondando en esto, los orígenes de la ciberseguridad generan que en el discurso público sobresalga el lenguaje técnico y se dificulte la participación de personas no expertas. Más aún, las características propias del ciberespacio generan que los efectos de un ciberataque no puedan ser aislados y se potencian con otras temáticas securitizadas.

3.2.2. La desecuritización

Sin duda alguna, la cibersecuritización es extremadamente poderosa al involucrar un doble movimiento: de lo politizado a lo securitizado y de lo político a lo tecnificado (Lacy & Prince, 2018). Sin embargo, una vez securitizada una temática esta puede volver al espectro de lo politizado a través de la desecuritización. Este proceso remueve un tema de la posición trascendental y alivia la amenaza sobre el objeto referente (Rousch, 2015). Dicha transición dependerá de los cambios en las identidades y las dinámicas "nosotros-otros". En otras palabras, y según la Escuela de Copenhague, se moviliza al tema de la secuencia amenaza-defensa a la esfera pública ordinaria (Hansen & Nissenbaum, 2009).

De acuerdo con Rousch (2015), existen cuatro formas de desecuritización que sirven como herramienta para presuponer la trayectoria de un conflicto. En primer lugar, el cambio a través de estabilización. En segundo lugar, el reemplazo de un tema securitizado por un nuevo tema que se incorpora a la agenda de seguridad. En tercer lugar, la rearticulación ofrece una solución política a las amenazas mientras que, en cuarto lugar, el silencio genera que un tema sea removido totalmente.

3.2.3. Principales críticas

Los críticos a la Escuela de Copenhague recalcan que, al enfocarse en un solo momento, este proceso es estático y su definición de éxito depende de un criterio fijo y externo (Ooijen, 2020). En este sentido, durante los últimos años se ha expresado la necesidad de tomar en

consideración otras fuentes de securitización como imágenes o prácticas burocráticas. Asimismo, los críticos han resaltado que la cibersecuritización no garantiza resultados de seguridad actuales. Por ejemplo, Calås (2019) estudia cómo la capacidad del actor securitizante para contextualizar su mensaje depende de la calidad de las instituciones burocráticas. Similarmente, Bo (2016) considera que la mejor manera para medir la securitización son los resultados ya que el análisis del discurso deja de lado las diferencias sociales y culturales al focalizarse en el lenguaje y la audiencia.

Siguiendo este argumento, cabe destacar que la Escuela de París responde a las críticas presentadas y busca complementar la teoría de la securitización al enfocarse en las prácticas. Según los referentes de esta línea, la seguridad es un proceso rutinario que se produce y reproduce en las prácticas diarias (Ooijen, 2020). Es decir, esta se definirá en la toma de decisiones burocráticas. En otras palabras, no existe un único discurso que legitima públicamente a una amenaza de seguridad, sino que se construye gradualmente en la rutina.

Según Ooijen (2020), es posible encontrar un punto intermedio entre la escuela de Copenhague y la escuela de París al observar a la seguridad como un acto performativo: las prácticas discursivas y no discursivas generan significado. Entonces, la securitización es un proceso interactivo que incluye acciones rutinarias y excepcionales por lo que es necesario observar tanto el discurso como los mecanismos de reproducción. Esta idea se asimila a la teoría de la trayectoria dependiente: cada acción securitizante direcciona el significado de la seguridad para la audiencia y, análogamente, se asienta y reproduce con prácticas diarias. Más aún, al ser el contexto siempre cambiante, los procesos securitizantes terminan siendo iterativos e interactivos con luchas por la autoridad y legitimidad.

4. Metodología

Con el objetivo de responder a la pregunta de investigación planteada previamente se utilizará un diseño cualitativo. Esto se debe a su flexibilidad para construir el modelo metodológico a través de constantes iteraciones aplicando la interactividad e interconexión del esquema (Maxwell, 2012). Asimismo, debido a la pregunta guía enfocada en el cómo se realizará un estudio de caso comparativo sobre Estonia y Reino Unido. Uno de los principales beneficios de este tipo de estudio es la posibilidad de estudiar un conjunto de eventos con intensidad y

profundidad, aspecto que suele dejarse de lado en investigaciones con una gran cantidad de observaciones (Gerring, 2004). A continuación, se profundizará sobre la metodología aplicada.

4.1. Selección de los casos

En el presente trabajo se ha seleccionado estudiar la construcción de la ciberseguridad en Estonia y en el Reino Unido. Si bien los estudios de caso comparativos son extraños en la literatura de la ciberseguridad, aplicar este diseño permite comparar y detectar patrones en común para el ingreso de una temática en la agenda de seguridad. En este sentido, el foco de estudio suele darse en los eventos outliers como Estonia (2007) y Stuxnet (2010). Por ende, se ha seleccionado contrastar el proceso securitizante de Estonia con el del Reino Unido que, a diferencia del primero, posee una mayor cantidad de ciberataques a lo largo del tiempo, pero con menor intensidad y relevancia.

En este sentido, el estudio de caso comparativo permite entender la construcción del significado dentro del proceso securitizante (Ooijen, 2020). Más aún, se podrá captar las diferencias características de cada país y su contexto de ciberseguridad para identificar los elementos comunes y diferentes durante este desarrollo. Es decir, la tecnología genera cambios a nivel sistémico, pero sus efectos varían de acuerdo con las identidades y culturas nacionales lo que problematiza las generalizaciones (Fritsch, 2011). Asimismo, se podrá determinar si la cantidad e intensidad de la amenaza sufrida afecta la respuesta estatal y, consecuentemente, el resultado de la securitización.

Cabe destacar que gran parte de la literatura sobre ciberseguridad se ha enfocado en el caso estonio ya que se trata de un ancla histórica que reveló a los Estados las vulnerabilidades de una sociedad digital (Rousch, 2015). Sin embargo, se han instaurado argumentos contrarios sobre la securitización de la temática en el país báltico. Esta divergencia, como se verá próximamente, puede deberse a imperfecciones teóricas y metodológicas.

4.2. Análisis de discurso en el estudio de la securitización

Como se ha introducido previamente, la naturaleza de las ciberamenazas y la percepción de riesgo se construyen a través de narrativas. Debido a esto, hay una asociación inherente entre el discurso y la seguridad ya que la securitización depende de la construcción discursiva de un tema en particular (Rousch, 2015). En este marco, el análisis del discurso busca responder de dónde viene el significado a través del estudio del discurso y la realidad social. Como metodología, implica el análisis de diferentes fuentes del discurso tales como entrevistas, diarios, discursos, documentos, entre otros. Dentro de la literatura de la securitización, esta metodología ha sido utilizada ampliamente para analizar la emergencia y el desarrollo de patrones de representación de la amenaza. Esto se debe, en particular, a que un documento o discurso político construye problemas, objetos y sujetos y articula políticas; formando identidades y legitimando cursos de acción (Ooijen, 2020).

Sin embargo, y con el objetivo de captar las críticas a la Escuela de Copenhague, se complementará el análisis de discurso con el estudio de las prácticas. Así, se utilizará primero un modelo intertextual incorporando los documentos oficiales para luego elaborar en el contexto institucional y la normativa. En este sentido, se entiende a las instituciones y la legislación como conjuntos estables de normas, intereses e identidades que impactan el proceso de socialización y la participación colectiva. Por ende, se buscará estudiar estos elementos para contemplar cómo la securitización puede tener lugar más allá de las narrativas expresas.

De esta manera, se profundizará en tres niveles de análisis de las prácticas discursivas y no discursivas para comprender si hubo una securitización de la temática: (1) discursos públicos en medios de comunicación, (2) documentos oficiales y (3) instituciones. Para ello, primero se estudiarán estos tres elementos por separado para cada país. Posteriormente, se identificarán las similitudes y diferencias en los procesos securitizantes. Cabe destacar que no se trata de un análisis exhaustivo ya que existen desarrollos sectoriales, regulaciones especializadas o agencias gubernamentales a las que no se está haciendo referencia.

4.3. Consideraciones metodológicas

El análisis de discursos posee dos grandes problemas de acuerdo con Yin (2009). Por un lado, puede haber aseveraciones que no sean del todo precisas a pesar de que los textos estudiados surjan de una fuente oficial gubernamental. Por el otro, al ser uno de los casos Estonia se están

utilizando discursos y documentos traducidos en lugar de su idioma original lo que puede derivar en errores de interpretación o inexactitudes. Asimismo, los documentos analizados son seleccionados por el autor lo que puede explicar diferentes resultados para el proceso securitizante. Además, la Escuela de Copenhague suele focalizarse en declaraciones oficiales por parte de altos funcionarios ignorando las prácticas de los actores (Dunn Cavelty, 2020).

Si bien para el estudio de la securitización ha preponderado el análisis del discurso lo que genera una falta de diversidad metodológica, la literatura más reciente ha comenzado a aplicar métodos cuantitativos. Respondiendo a lo planteado anteriormente, autores como Baele y Sterck (2015) constatan cuantitativamente la presencia de palabras claves para medir objetivamente el nivel de securitización de una temática. Este método es de gran utilidad al analizar un solo actor, pero posee desventajas al contar con un cuerpo de estudio más amplio debido a las formas y estructuras del discurso en cada país (Calås, 2019). De la misma manera, Valeriano y Maness (2018) buscan evaluar datos estadísticos para determinar las intenciones de los gobiernos mientras que Gomez y Villar (2018) miden los sentimientos de "peligro" a través de información experimental.

5. Estudios de caso: Estonia y Reino Unido

En esta sección se estudiará el proceso cibersecuritizante de Estonia y Reino Unido analizando la respuesta de cada país frente a los ciberataques que han sufrido. Para comenzar, se estudiará a cada país por separado con el fin de captar sus características propias y matices para la securitización. Así, primero se describe el contexto geopolítico de cada uno de los países considerando que su rol e identidad determinará cómo se construyen las amenazas. Luego, se hará referencia al proceso securitizante comenzando por los ciberataques sufridos por el país para poder focalizar en los tres elementos fundamentales: (1) discursos públicos, (2) documentos oficiales e (3) instituciones. Posteriormente, se determinará en cada caso si la securitización fue exitosa o no. Finalmente, se buscará identificar similitudes y diferencias en los procesos para responder a la pregunta de investigación.

5.1. Estonia

Estonia, uno de los países más pequeños de Europa, se independizó en 1991 de la Unión Soviética transitando rápidamente cambios institucionales, sociales y políticos radicales. Estos

procesos fueron acompañados por una transformación en la identidad nacional que buscaba imaginarse a sí misma como un país occidental y una democracia neoliberal (Kohler, 2020; Ooijen, 2020). Por ende, implementó una estrategia para distanciarse de su ocupante original a través del foco en la tecnología, así como la reforma de su economía e instituciones.

Ser un país moderno, occidental y avanzado para Estonia estaba profundamente relacionado con la innovación y las tecnologías de la información. En este sentido, la digitalización del país ha sido uno de sus elementos centrales y una forma de incorporarse a las organizaciones internacionales. Este interés por lo digital, sin embargo, generó que el país sea más vulnerable a ciberataques.

Siguiendo lo expresado, la histórica negación de Rusia para aceptar la soberanía estonia, junto al riesgo que presenta ser vecino de país, generó que la seguridad ocupase un rol central para su integración e independencia (Kohler, 2020). En este sentido, ser miembro de la Unión Europea (UE) y la Organización del Tratado del Atlántico Norte (OTAN) le permitió consolidar su nueva identidad y sus valores al mismo tiempo que robustece su seguridad a través de acuerdos colectivos.

5.1.2. Análisis del proceso securitizante

5.1.2.1. Ciberataques

El 26 de abril de 2007 el gobierno movió la figura del Soldado de Bronce, estatua ubicada originalmente en la capital de Estonia, que conmemora a los soldados soviéticos que murieron luchando contra los nazis en el territorio (Rousch, 2015). Esta acción generó una protesta por parte de la minoría rusa en el país ya que mientras que para ellos simbolizaba la victoria del Ejército Rojo, para los estonios era una representación visual de los años de ocupación soviética (Ooijen, 2020). A partir de este hecho, desde 27 de abril hasta el 18 de mayo, el país enfrentó diversos ciberataques y protestas cuya violencia aumentó gradualmente para culminar en arrestos, cientos de heridos y un muerto.

Durante este periodo fueron atacados los websites del gobierno estonio, agencias de comunicación, proveedores de servicios de Internet y servicios bancarios online (Rousch, 2015). Cabe destacar que las ciberoperaciones incrementaron en su intensidad hasta tener el pico máximo en la celebración rusa del Día de la Victoria (9 de mayo). Al mismo tiempo, se tomó la embajada estonia en Moscú y se atacó físicamente al embajador durante una conferencia de

prensa el 2 de mayo (Kohler, 2020). De esta forma, los ataques limitaron la habilidad del gobierno de comunicarse con la población y afectaron al sector financiero.

Cabe destacar que, hasta este momento, no existía jurisprudencia que defina qué es un ciberataque y de qué forma se lleva a cabo ya que las inseguridades en el ciberespacio se consideraban problemas técnicos (Ooijen, 2020). Sin embargo, los ataques demostraron la capacidad destructiva de las herramientas digitales y cambiaron la forma en la que los Estados pensaban su seguridad (Rousch, 2015). Por ende, el caso de Estonia se transformó en un ancla histórica para la construcción de la ciberseguridad.

5.1.2.2. Discursos públicos

El discurso de los funcionarios públicos de Estonia y los medios de comunicación tiene siempre presente un elemento digital fuerte. Esto se debe, por un lado, a la prioridad de la tecnología en el desarrollo económico del país y, por el otro, al interés del país de marcar el rumbo de acción internacional. En este sentido, a partir de los ataques sufridos en 2007 se observan dos públicos receptores: los residentes de Estonia y la Unión Europea. Las narrativas orientadas a los habitantes del país buscaban legitimar la importancia de la ciberseguridad para la política estonia -y, por ende, un mayor presupuesto- mientras que las palabras dirigidas a la Unión Europea tenían como objetivo mostrarse como país experto y líder en esta temática. Para ejemplificar, en la Estrategia Nacional de Ciberseguridad de 2008, el entonces Ministro de Defensa Jaak Aavikso expresó:

> Owing to Estonia's unique experience in dealing with cyber-attacks in the spring of 2007 and subsequent policy initiatives, the international community expects a major contribution from us (...) more extensive participation in international organizations is vital to ensuring recognition of the problems of cyber security (Ministerio de Defensa, 2008, pp. 22).

Seguido a los ataques, el proceso de securitización fue construido alrededor de tres pilares: (1) el ciberespacio es inherentemente inseguro para los objetos referentes, (2) las amenazas son reales en este nuevo campo de batalla, (3) existen riesgos a futuro (Ooijen, 2020). Como se observa, se utilizó un léxico militar que denota la búsqueda del gobierno estonio de asociar los hechos con la ciberguerra. En esta línea, el New York Times expresó que esta fue la primera guerra real en el ciberespacio (Landle & Markoff, 2007). Por su lado, Jaak Aavikso consideró que: "(...) what took place was according to our interpretation cyberwarfare and cyber terrorism. In

essence, cyber-attacks against Estonia demonstrated that the Internet already is a perfect battlefield of the 21st century" (Aaviksoo, 2008).

Más aún, para Toomas Hendrik Ilves, presidente de 2006 a 2016, la implicación militar era clara:

Estonia was attacked with a weapon and in a manner whose full significance is just beginning to dawn on the whole world in the 21st century (...) The continuing cyber-attacks from the servers of Russian state authorities (...) indicates that our sovereign state is under a heavy attack (Ilves, 2007).

Impulsar la narrativa de la ciberguerra implica que otro actor relevante del sistema internacional ha sido el perpetrador. Como se observa en el discurso del presidente Ilves, Estonia identificó y denoto rápidamente a Rusia como culpable. Esto se debió al tráfico de las redes en lenguaje ruso, la distribución de las indicaciones para los ataques en foros rusos y las motivaciones políticas por el traslado del Soldado de Bronce (Rousch, 2015). Más aún, a pesar de que el país negó su involucramiento, en el mismo periodo implementaron medidas económicas hostiles y se negaron a cooperar con la investigación de los ciberataques. Debido a esto, Merit Kopli, editor de un diario estonio, declaró que "no había duda" que los ciberataques provenían de Rusia (Traynor, 2007). A su vez, el ministro de Relaciones Exteriores, Urman Peat, expresó que era la primera vez que Rusia ejecutaba esos ataques contra otro país (Peat, 2007).

Como se ha argumentado en apartados anteriores, el ciberespacio posee un gran problema de atribución que dificulta denotar quiénes son responsables de los ataques ya que, por ejemplo, las direcciones de IP originales podrían estar enmascaradas gracias a VPN. Sin embargo, Mikko Hypponen, experto de IT finlandés, expresó que Rusia tenía las capacidades técnicas para llevar a cabo un ataque similar (Traynor, 2007). Asimismo, a pesar de la negación del país, el líder de un grupo nacionalista ruso, Konstantin Goloshokov, asumió los ataques (Tikk, Kaska y Vihul, 2010).

Haber caracterizado al hecho como la primera guerra en el ciberespacio tuvo dos implicancias para las audiencias. Por un lado, para la audiencia nacional generó la aceptación de medidas excepcionales y un mayor gasto público para desarrollar las capacidades de ciberseguridad. Por el otro, un claro pedido de accionar por parte de la Unión Europea para actuar contra Rusia y aplicar los mismos principios que si se tratase de una guerra tradicional. En este sentido, el Primer Ministro de Estonia expresó luego de los ataques: "we expect from the European Union a straightforward reaction to the well-coordinated attacks of Russia" (Ansip, 2007).

Cabe destacar que en estos discursos preponderó también los imaginarios del pasado o futuro para comparar a los ataques de 2007 con visiones catastróficas o grandes tragedias. Por ejemplo, en los comunicados del Parlamento al respecto comparaban a los hechos de mayo de 2007 con explosiones nucleares (Dunn Cavelty, 2013). En este sentido, el nivel de urgencia del discurso buscaba generar que se amplíe la posibilidad de tomar medidas extraordinarias y se involucren las organizaciones internacionales posicionando a los ataques como un problema de seguridad que habilitaba soluciones militares.

Actualmente, estas analogías ya no tienen el mismo lugar en los discursos de funcionarios públicos. A pesar de ello, Estonia continúa sus esfuerzos para que la ciberseguridad posea cada vez un rol mayor en las organizaciones internacionales. Para ejemplificar, en septiembre del 2021 el Ministro de Emprendedurismo y Tecnologías de la Información del país expresó que a nivel Unión Europea el objetivo debería ser "no less than to agree on a global framework on cybersecurity, just like NATO has the 2% target of GDP on defence, we have to have a comparable target, methodology and benchmark for cybersecurity" (Noyan, 2021).

5.1.2.3. Documentos oficiales

Los ataques de 2007 le dieron autoridad a Estonia para hablar en temas de seguridad, promover publicaciones e influenciar la legislación internacional. A su vez, en ellos se plasman las intenciones expresadas en los discursos que han sido aceptadas por las audiencias. En este sentido, gran parte de los documentos publicados buscaban aliviar la amenaza a través de medios no legislativos y/o iniciativas de política pública (Rousch, 2015). Cabe resaltar que Estonia fue el primer país en producir legislación doméstica sobre esta temática y una Estrategia de Ciberseguridad.

Estrategias de Ciberseguridad

La primera Estrategia de Ciberseguridad de Estonia del Ministerio de Defensa publicada en 2008 tiene el objetivo primordial de solucionar la amenaza asimétrica que representa el ciberespacio y las vulnerabilidades inherentes a este dominio (Rousch, 2015). Como respuesta, promueve la educación, capacidad técnica y la legislación nacional. Así, busca aumentar sus capacidades de ciberdefensa politizando la amenaza y disminuyendo la autoridad de los expertos técnicos. En este marco, resalta que, a pesar de que Estonia posee una responsabilidad para identificar sus vulnerabilidades y generar políticas, la ciberseguridad debe ser gestionada a nivel global.

Luego de esta Estrategia, y a partir de 2011, el Ministerio de Asuntos Económicos y de Comunicación pasó a ser el responsable de la coordinación de las políticas de ciberseguridad. La Estrategia de Ciberseguridad (2014 a 2017) publicada por este organismo muestra un enfoque diferente ya que establece que la ciberseguridad impacta en la protección del sistema económico, la libertad de la sociedad y la integridad de la soberanía nacional. Así, vuelve a establecerse la ciberseguridad como una evidente amenaza a la seguridad nacional, pero por sus efectos en la vida cotidiana en lugar de por las distribuciones asimétricas de poder entre los Estados.

Para el periodo 2019-2022, la última Estrategia de Ciberseguridad publicada posee un presupuesto de 2.1 millones de euros por año con objetivos que siguen los lineamientos de la Estrategia anterior. En este sentido, busca (1) promover los derechos y libertades en el ciberespacio, (2) amplificar el desarrollo digital de Estonia como base para su crecimiento socioeconómico, (3) reconocer la seguridad de las soluciones criptográficas y (4) potenciar la transparencia y la confianza pública. En suma, el país está implementando acciones para lograr una democracia digital sostenible y resiliente ante las posibles crisis (Kohler, 2020).

Otros documentos

Además de las Estrategias de Ciberseguridad, se destacan las publicaciones realizadas por la Asociación Estonia de Información de la Seguridad (EISA), entidad que busca la cooperación del sector privado, el gobierno y la academia. Los documentos que han generado denotan un gran foco en la educación para generar resiliencia y en la cooperación multistakeholder para la gobernanza del ciberespacio. Por ejemplo, el reporte Summary on Ensuring Cyber Security de 2012 y el Reporte Anual de 2013 de la Autoridad de los Sistemas de Información recalcan el rol de la educación para mitigar los efectos dañinos de las ciberamenazas así como de la cooperación internacional y entre agencias de gobierno. Sin embargo, el Reporte Anual de 2015 cambia el foco expresando que la seguridad se ha deteriorado debido al aumento de los ciberataques en Europa caracterizándolo como un nuevo campo de batalla.

Focalizando en este último punto, en 2013 fue publicado el Manual de Tallin sobre las leyes aplicables a la ciberguerra. Si bien es un documento no vinculante, su objetivo es relacionar los elementos jurídicos del derecho internacional con la ciberguerra. Así, sugiere que las ciberoperaciones ejecutadas en el contexto de un conflicto armado deben estar sujetas a la misma jurisprudencia que un conflicto tradicional. En otras palabras, no considera al

ciberconflicto como un conflicto armado en sí mismo, sino una herramienta para enfrentamientos mayores.

5.1.2.3. Instituciones

A partir de los ataques de 2007, se ha observado una reestructuración en las organizaciones de Estonia para reflejar el rol prioritario que tomó la ciberseguridad. A continuación, se comentará brevemente sobre las principales incorporaciones tanto en el plano doméstico como internacional.

Plano doméstico

En 2009 se creó el Consejo de Ciberseguridad del Comité de Seguridad que reúne a siete ministerios y la oficina de gobierno para fomentar la colaboración interagencial y monitorear la implementación de las Estrategias de Ciberseguridad. En 2014, el Ministerio de Defensa inauguró el Departamento de Tecnologías de la Información, Comunicaciones y Políticas Cibernéticas mientras que en 2018 se lanzó el Ciber comando de las Fuerzas de Defensa. Se espera que para el 2023 este sea completamente operacional con 300 empleados representando 5% del personal de las Fuerzas Armadas (Kohler, 2020).

Más aún, las fuerzas armadas paramilitares "Liga de Ciberdefensa" poseen 16.000 miembros y fueron integradas al sistema de seguridad nacional junto a la Unidad de Cibercrimen de la policía. Esta organización voluntaria es un ejemplo de la coproducción ciudadana de los servicios policiales. En este sentido, la democratización de la vigilancia digital está respondiendo a las inseguridades del ciberespacio y la necesidad de educar a los ciudadanos como principales vulnerabilidades (Chang, Zhong, & Grabosky, 2016).

Plano internacional

Participando en OTAN, Estonia recomendó la creación de un nuevo Centro de Excelencia para la Seguridad de las Telecomunicaciones en Tallin durante 2003 cuya creación se vio acelerada frente a los ataques de 2007 (Vargas Vargas, 2014). A su vez, como miembro de la UE usa su rol para promover el progreso digital y la mutua asistencia para responder ante ciber operaciones (Kohler, 2020). Más aún, incluyó la Directiva de Seguridad de Redes e Información (2016) de esta organización a su Ley Nacional con el Acta de Ciberseguridad (2018).

En 2017 Estonia realizó un acuerdo con Luxemburgo para abrir la primera Embajada de Datos en el mundo pudiendo guardar sus datos fuera de su territorio, pero manteniendo jurisdicción (Kohler, 2020). En 2018, designó al primer Embajador por la Ciberseguridad y, al año siguiente, creó el Departamento de Ciber diplomacia dentro del Ministerio de Relaciones Exteriores. En este sentido, Estonia busca ser un defensor de la ciberseguridad en el sistema internacional; entendiendo que su seguridad, influencia y participación depende de su reputación.

Finalmente, participa también de mesas regionales e internacionales en las que fomenta la gobernanza de la tecnología. Por ejemplo, desde 2015 en la mesa anual sobre temas de ciberseguridad de la Cooperación Nórdico-Báltica. Recientemente (2020-2021) Estonia fue elegido como miembro no permanente del Consejo de Seguridad de Naciones Unidas anunciando como prioridades la e-gobernanza y la ciberseguridad.

5.1.3. ¿Securitización exitosa?

Gracias al análisis de discurso se identificó que, luego de los ataques de 2007, hubo una clara narrativa con elementos militares, la presencia de ciberguerra y Rusia como perpetuador. Sin embargo, para poder determinar los resultados de la securitización, es necesario evaluar de manera separada el proceso dirigido a la ciudadanía y aquel con foco en la Unión Europea.

Respecto al primero, es posible concluir que la securitización en los años posteriores a los ciberataques fue exitosa. Esto se debe a que en los discursos se realizó una hiper securitización de la temática que fue trasladada a una restructuración estatal que plasmó la importancia y la militarización del ciberespacio. Sin embargo, en los años más recientes, el desarrollo de capacidades y la promulgación de la resiliencia de Estonia han generado que los efectos negativos de los ciberataques sean más fáciles de mitigar. Por ende, se identifica un proceso de desecuritización gracias a la estabilización. Para ejemplificar, recientemente el gobierno estonio se alejó de una descripción de ciberguerra al tratar lo ciber como un plano más de la gestión estatal.

Sin embargo, en las audiencias internacionales el resultado fue diferente. La falta de consecuencias físicas que hubiera tenido un ataque tradicional, así como de normas, protocolos y políticas para ciberguerra dificultó el framing de guerra. Así, se invalidó la aplicación de medidas extraordinarias en los años cercanos al ataque. Más aún, las instituciones que surgieron lideradas por Estonia se instalaron de manera gradual y sin el sentido de urgencia que

caracterizaría a una gramática de seguridad. Por ende, el proceso de securitización estonio dirigido a la Unión Europea no fue exitoso.

5.2. Reino Unido

El Reino Unido es un país isla al noroeste de Europa continental y está conformado por Inglaterra, Gales, Escocia e Irlanda del Norte. El país se destacó por ser uno de los principales creadores de normas con un rol determinante en la seguridad internacional hasta la emergencia de Estados Unidos como hegemón. Debido a esto, a partir de 1970 comenzó a integrarse a Europa a través de organizaciones como la Comunidad Económica Europea mientras mantenía tratados económicos con el gigante americano (Friedman, 2018). Así, buscaba un punto medio entre los dos países que le representaban un balance de poder: Estados Unidos y Alemania.

La importancia del Reino Unido en el sistema internacional y el ajedrez político ha implicado que sean conscientes de la rúbrica de seguridad y las posibles amenazas a su rol. En este sentido, los tomadores de decisiones han reconocido tempranamente los cambios en la agenda de seguridad y sus implicancias para el sistema internacional. Sin embargo, en los últimos años el foco de las Estrategias de Seguridad Nacional ha estado en el terrorismo islámico, así como la posibilidad de que este ponga en jaque los valores occidentales y liberales (Gow, 2009). Si bien el ciberterrorismo ha sido un término acuñado rápidamente por los medios de comunicación, lo cibernético no se observa como una amenaza en sí sino como una herramienta para otros tipos de conflictos (Mott, 2016).

5.2.1. Análisis del proceso securitizante

5.2.1.1. Ciberataques

A diferencia del caso estonio, el Reino Unido no ha sido víctima de un ataque de semejante magnitud repentinamente. Por el contrario, esté país ha recibido constantes ciberataques a lo largo del tiempo con intensidad baja-media. En este sentido, la cuarta revisión anual del Centro de Ciberseguridad Nacional reveló que la organización defendió al Reino Unido de 723 incidentes entre el primero de septiembre de 2019 y el 31 de agosto de 2020 (NCSC, 2020). Más aún, solamente en 2017 los ciberataques representaron gastos de 32.2 millones de libras para los negocios británicos (Saleem, 2019).

Sin embargo, dentro de los constantes ataques que ha sufrido el país a lo largo de los años, se destacan dos hechos: las filtraciones de Snowden y los efectos del virus WannaCry en el Servicio Nacional de Salud. Por un lado, en 2013, Edward Snowden reveló que el GCHQ había estado interceptando comunicaciones privadas secretamente inclusive de personas sin interés para la inteligencia. Si bien organizaciones como Amnistía Internacional llevaron al país a la Corte, este hecho generó principalmente desconfianza por parte de la ciudadanía y preocupación de los agentes de inteligencia ya que Rusia y China habían accedido a su información confidencial. Por otro lado, en mayo de 2017, un ciberataque afectó al Servicio Nacional de Salud (NHS) del Reino Unido con 61 hospitales estando fuera de línea. Este ataque, que fue dirigido a computadoras de todo el mundo, costó para el NHS 92 millones de libras.

5.2.1.2. Discursos públicos

Como se ha nombrado previamente, en los discursos públicos preponderan los elementos cibernéticos como aspectos de otras amenazas a la seguridad nacional. En particular, puede observarse un claro discurso respecto al ciberterrorismo sobre los detractores "sin cara". Esta caracterización hace referencia a la distancia espacial entre aquel que comete el hecho y la víctima, así como la dificultad para ver o identificar al perpetrador (Mott, 2016). Esto no es solamente un aspecto del Internet, sino también de cómo los medios de comunicación han decidido representar al accionar cibernético.

Sin embargo, la aparición de los elementos cibernéticos en la seguridad está cada vez más presente en los discursos aún por fuera del terrorismo. Por ejemplo, en 2010, de la Cámara de los Lores, John Anderson, declaró que "suicide bombings have been the weapon of choice in certain quarters, carefully targeted cyberattacks will be the weapon in tomorrow's world" (Anderson, 2010).

En 2014, Jim Shannon, miembro del Parlamento del Reino Unido, expresó que

> Businesses and livelihoods now depend on cyber-security for protection, and we have a duty to protect ourselves, to protect Government Departments, and to protect our constituents (…) Cyberspace is a continually evolving environment, and if we are to defend ourselves from the threats that emanate from it, we must keep pace with that change (Shannon, 2014).

Durante este mismo año, en las encuestas de Yougov el 43% de los ciudadanos seleccionó online/cyber attacks that disrupt life in the UK como una de las principales amenazas para el país (Mott, 2016).

A su vez, en 2015, David Blunkett de la misma institución, identificó en una entrevista con el Yorkshire Post que ahora la amenaza era cibernética, con posibles efectos en todos los ámbitos de la vida (Blunkett, 2015). Similarmente, durante su primera charla como director del GCHQ, Jeremy Fleming comentaba principalmente que el Reino Unido debía prepararse frente al desarrollo de capacidades cibernéticas por parte de países vecinos. Sin embargo, en dicho discurso de 2018, focaliza principalmente en los hechos cometidos por Rusia: "We'll continue to expose Russia's unacceptable cyber behaviour, so they're held accountable for what they do, and to help the Government and industry protect themselves (Fleming, 2018)"

En 2019, Ciaran Martin identificó el riesgo que diferentes países representan en el ciberespacio:

> We face a determined, aggressive Russia, seeking traditional political advantage by new, high-tech means. We live in a business and corporate environment where Chinese cyber attacks on our commercial interests is now something our companies treat as business as usual (...) We face intrusions from Iran, and attempts to steal money from North Korea. Both nations being prepared to launch aggression digitally in a way they never would dare physically (NCSB, 2019).

En este sentido, la pandemia modificó la realidad de las empresas y los ciudadanos con muchos servicios pasando al plano digital. En palabras de Fleming: "The world changed in 2020 and so did the balance of threats we are seeing (NCSC, 2020)." De igual manera, Penny Mordaunt, Canciller de la Hacienda, consideraba en 2020 que "It is vital that cyber security remains a priority for government, industry and the public in building UK resilience to a spectrum of risks (NCSC, 2020)."

5.2.1.3. Documentos oficiales

Estrategias de Ciberseguridad

La visión de la Estrategia de Ciberseguridad del Reino Unido (2010-2015) fue buscar un ciberespacio seguro debido a los efectos sociales y económicos que este podía tener. El objetivo guía de este documento era no solo asegurar el ciberespacio para el uso de los ciudadanos, sino también mejorar sus capacidades y resiliencia estatal. Como se verá a continuación, esta estrategia era implementada por diversas agencias. Cabe destacar que cada año el Programa

Nacional de Ciberseguridad revisa este documento en línea con los reportes anuales de incidentes del Equipo de Respuesta de Emergencia de la Comunidad. Similarmente, la Estrategia de Ciberseguridad refiere al uso terrorista del Internet ampliamente y pone luz en la vulnerabilidad de las infraestructuras críticas del país.

En la renovada Estrategia de Ciberseguridad (2016-2021) los ciberataques continúan siendo una de las principales amenazas para la economía y la seguridad nacional del Reino Unido. En este sentido, este documento se encuentra desarrollado a partir de tres grandes pilares: defender, desalentar y desarrollar.

Siguiendo esta línea, en la Estrategia Nacional de Seguridad se nombra tanto al ciberterrorismo como a los ciberataques dentro de las amenazas Tier 1 que enfrenta el Reino Unido. A pesar de ello, en 2011, el gobierno publicó una nota POST destacando a la infraestructura del Reino Unido, pero a la vez aclarando que: "Cyber attacks have not caused physical disruption in the UK to date" (POST 2011, como se citó en Mott, 2015).

Otros documentos

Luego de los ciberataques de 2007, se observa un boom de documentos que hacen referencia a la ciberseguridad. Este hecho se encuentra en línea con el rol que tuvo Estonia para despertar el interés internacional en la temática. Por ejemplo, el gobierno del Reino Unido publicó en 2008 "The National Security Strategy of the United Kingdom: Security in an interdependent world". Más aún, dentro del Programa Cibernético se publicaron la Estrategia Nacional de Defensa y Seguridad y "A Strong Britain in an Age of Uncertainty: The National Security Strategy".

Siguiendo esta línea, la edición 2020 del Registro Nacional de Riesgos de Reino Unido describió claramente el potencial efecto que pueden tener las ciberamenazas en el país, así como la variedad en la que estas se presentan.Sin embargo, este concepto continúa estando atado al terrorismo: "Regional warfare can enable terrorist activity and an increasing number of non-state actors will likely exert power in arenas such as cyber space" (Cabinet Office, 2020)

5.2.1.4. Instituciones

Desde el punto de vista gubernamental, la respuesta frente a posibles ciberataques se caracteriza por diferentes agencias respondiendo de distintas maneras (Cornish, Hughes y

Livingstone, 2009). En este sentido, algunas de las organizaciones involucradas en temas de ciberseguridad son: la Sede de Comunicación del Gobierno, el Servicio de Seguridad, la policía, Hacienda del Reino Unido (HM), la Agencia de Fronteras, la Agencia de Crimen Organizado Serio y los servicios de inteligencia.

Si bien en 2007, se creó el Centro para la Protección de la Infraestructura Crítica (CPNI) que buscaba coordinar los esfuerzos, la respuesta continúa variando de acuerdo con el sector. Por ejemplo, diferentes entidades estatales fundaron el Grupo de Resiliencia Operativa de Mercado Cruzado (CMORG) para la industria financiera mientras que el Consejo de Seguridad de la Industria de Telecomunicaciones (TISAC) se encarga de los hechos relacionados a las comunicaciones. Esta última agencia forma parte de la Oficina de Gabinete del Gobierno del Reino Unido, dentro de la Oficina de Ciberseguridad.

La última Estrategia de Ciberseguridad del país (2016-2021) creó un nuevo Centro de Ciberseguridad Nacional (NCSC) que busca unificar a todas las agencias relacionadas con la ciberseguridad en un único organismo. Asimismo, esta entidad será la encargada de implementar la estrategia y trabajar directamente con el gobierno y la industria. Cabe destacar que este documento recalca la importancia de compartir información y trabajar internacionalmente con el resto de los actores (Kriz, s.f). Paralelamente, también se implementó el nuevo Programa de Ciberdefensa Activa que busca automatizar la respuesta a los incidentes sufridos por el país y solucionar posibles problemas de protocolo (Levy, 2016).

Similarmente, dentro del Equipo de Respuesta de Emergencia de la Comunidad (CERT-UK), se encuentra la Alianza de Ciberseguridad para Compartir Información (CiSP), organización que busca ser proactiva frente a los reportes de incidentes en el ciberespacio (Bada, et al., 2016). Cabe destacar que de esta entidad también participa el sector privado con la intención de compartir información. Asimismo, hay un sistema oficial de respuesta que, en caso de hechos mayores de ciberseguridad, es coordinado por la Oficina del Gabinete. Durante una emergencia, entonces, pueden ser activados los Grupos Estratégicos o el Comité de Contingencia Civil. A su vez, en 2013, el Ministerio de Defensa del Reino Unido anunció la creación de una nueva Ciber Reserva Conjunta para proteger la información y las redes de computación críticas.

Cabe destacar que, como se ha expresado en este trabajo, un país no puede responder sólo a las ciberamenazas. Por el contrario, es necesaria una respuesta en conjunta, así como una colaboración para generar resiliencia a nivel nacional, regional y sistémico. Debido a esto, es

importante analizar a futuro qué efectos tendrá el Brexit sobre las capacidades cibernéticas del Reino Unido. En este sentido, el país perderá su lugar en el Consejo de Administración de Europol y, consecuentemente, en el Centro Europeo de Cibercrimen. Sin embargo, seguirá los frameworks de protección de la información de la Unión Europea. Como expresa Saleem (2019), esto implica que pasarán de hacer las reglas a simplemente seguirlas.

5.3.3. ¿Securitización exitosa?

Como se ha expresado, partir de los ataques sufridos por Estados Unidos en el 2001, el terrorismo y la seguridad nacional han sido una de las principales temáticas de los discursos públicos del Reino Unido (Hersee, 2019). Si bien la ciberseguridad ha ganado relevancia en los últimos años, continúa presentándose como una modalidad para otras amenazas. En este sentido, no se observa un proceso securitizante debido a la falta de utilización de gramáticas de seguridad que inciten medidas extremas. Por el contrario, el ámbito ciber es simplemente un potenciador o una expresión de otras temáticas que sí pueden ser securitizadas.

Esto puede deberse, en parte, a que el Reino Unido no ha recibido un ataque lo suficientemente poderoso que sorprenda a la ciudadanía y ponga en peligro el accionar estatal. Contrariamente, se observan ciberoperaciones continuas de menor escala que han generado que los ciudadanos y el gobierno se acostumbre a ellas. De acuerdo con Mott (2016), la carencia de discusión pública podría deberse a la falta de grandes ataques en suelo británico y a las discrepancias para definir esta temática genera que su imaginario no sea claro para la ciudadanía. Así, se coincide con las teorías que argumentan que la exposición a largo plazo a ciberataques mitiga la respuesta emocional de los ciudadanos normalizando las amenazas (Gomez, 2021).

5.3. Similitudes y diferencias

Como se observa en ambos países, la ciberseguridad ha ganado importancia a lo largo de los años y cada vez es tenida en cuenta mayormente por los tomadores de decisiones. Sin embargo, el rol que esta posea en la agenda pública dependerá del punto de partida del país, así como de su historia y vivencia de ciberataques. En este sentido, el Reino Unido y Estonia presentan situaciones disímiles lo que explica la diferencia de sus procesos securitizantes si bien en ambos casos la temática está en la agenda de seguridad.

En el caso de Estonia, se observa claramente un intento de hiper securitización por parte de los funcionarios públicos a partir de los ataques debido al léxico de guerra y militarización presente en los discursos. Los hechos, a su vez, por ser los primeros de su estilo permitían el uso de analogías y metáforas de un futuro violento por el potencial destructivo de las operaciones en el ciberespacio. En este sentido, Estonia poseía un claro peligro en Rusia y la necesidad de ser protegido por las organizaciones internacionales para garantizar su soberanía. Así, refuerzan las nociones de un conflicto entre países para justificar la toma de medidas extraordinarias. A pesar de ello, el éxito del proceso securitizante para la audiencia nacional no se vio reflejado para la Unión Europea.

El Reino Unido, en cambio, no sufrió un hecho bisagra, sino que sus experiencias con los ciberataques estaban vinculadas a otros conflictos. Es decir, los aspectos cibernéticos aparecían como una modalidad dentro de otros ataques y amenazas como, por ejemplo, el terrorismo. Esto se puede observar en los discursos ya que el sentimiento de amenaza suele estar en el potencial uso de Internet por parte de organizaciones criminales u otros actores. Cabe destacar también que este país sufre constantemente de ciberoperaciones por lo que el potencial riesgo que percibe la ciudadanía es cada vez menor al acostumbrarse a este tipo de hechos.

En los últimos años, ambos países han desarrollado instituciones para coordinar los esfuerzos de ciberseguridad, así como desarrollado su resiliencia nacional. Para Estonia, estar preparado frente a posibles amenazas cibernéticas significó una estabilización del proceso securitizante. Así, se ve un cambio en el discurso público que tiende a reforzar la postura del país como experto y determinante del rumbo frente a otras Naciones respecto a este dominio. Mientras tanto, en el Reino Unido se observa que el ciberespacio está comenzando a tener mayor presencia, aunque todavía unido al terrorismo y otras amenazas.

En suma, es posible observar que las experiencias de cada país con el ciberespacio son diferentes lo que genera distintos modos en los que ingresa el tema en la agenda de seguridad. Para Estonia, los ataques de 2007 junto con su dependencia a los servicios digitales implicaron la necesidad de prepararse ante futuras amenazas y securitizar el riesgo inherente a la tecnología. En el Reino Unido la exposición gradual y de baja intensidad a ciberataques permitió que la ciudadanía normalice estos hechos y que el peso de los procesos securitizantes esté en otros fenómenos como el terrorismo.

6. Conclusiones

El presente trabajo tenía como objetivo responder a la siguiente pregunta de investigación: ¿cómo se explica que algunos países logran securitizar la respuesta a las amenazas que plantea la ciberseguridad? Para ello, se realizó un estudio de caso comparativo y se aplicó como metodología el análisis de discurso. Los países seleccionados para el análisis fueron el Reino Unido y Estonia ya que ambos presentaban experiencias distintas con ciberataques lo que permite evaluar qué elementos generan un proceso securitizante exitoso.

Gracias al análisis de discurso, de las instituciones y de los documentos oficiales se puede concluir que en los años posteriores a los ataques de 2007 hubo un proceso cibersecuritizante exitoso en Estonia para la audiencia doméstica. Sin embargo, en el caso del Reino Unido la alta exposición del país a ciberataques ha generado que estos hechos se normalicen y se identifiquen principalmente como modalidades en las que se expresan otras amenazas. De esta forma, para el caso británico no hay una securitización de la temática. Respondiendo a la pregunta de investigación, y retomando los conceptos teóricos de la Escuela de Copenhague, las características de la ciberseguridad para cada país parecieran ser las que facilitan la securitización. En otras palabras, cómo cada actor -y las sociedades- percibe a la amenaza va a permitir que ésta justifique medidas extraordinarias y un mayor gasto público.

Cabe destacar que la principal debilidad de este estudio son las limitaciones lingüísticas ya que no permiten captar las sutilezas propias de los discursos. Asimismo, los procesos securitizantes son dinámicas multifacéticas y complejas por lo que responder con “si” o “no” a la securitización de una temática está simplificando la realidad y dejando de lado posibles matices dentro del espectro de la securitización.

En suma, el presente trabajo busca contribuir al estudio de la ciberseguridad a través de un enfoque de las Relaciones Internacionales. Los beneficios de la globalización y la tecnología están acompañados de grandes amenazas para las sociedades. Por ende, el estudio de estas temáticas es de suma importancia para comprender cómo los Estados pueden adaptarse a un mundo interconectado y vulnerable. Frente a esto, y de manera posterior a esta investigación, se presenta la oportunidad de explorar los procesos y las situaciones de seguridad de otros países que hayan sido víctimas de ciberataques para comparar los procesos de securitización.

De la misma manera, también sería beneficioso complementar el análisis de discurso con métodos cuantitativos para salvar posibles limitaciones metodológicas.

Bibliografía

Attiná, F. (2001). *El Sistema Político Global.* Buenos Aires: Paidós.

Bada, M., Sasse, A., & Nurse, J. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society.

Bada, M., et al. (2016). Cybersecurity Capacity Review of the United Kingdom. Global Cyber Security Capacity Centre, University of Oxford.

Baele, S., & Sterck, O. (2015). Diagnosing the securitisation of immigration at the EU level: A new method for stronger empirical claims. *Political Studies*, 63(5), 1120-1139.

Baldwin, D. (2011). Security Studies and the end of the Cold War. *World Politics*, 117-141.

Balzacq, T., Léonard, S., & Ruzicka, I. (2016). 'Securitization' revisited: theory and cases. *International Relations*, 494-531.

Banco Interamericano de Desarrollo. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.* Obtenido de https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-seguir-en-america-latina-y-el-caribe

Bartolomé, M. (2016). Algunas aproximaciones a la agenda de la Seguridad Internacional contemporánea y la influencia teórica en sus contenidos. *Revista Política y Estrategia*, 101-133.

Bartolomé, M. (2018). La Seguridad Internacional contemporánea: contenidos temáticos, agenda y efectos de su ampliación. *Relaciones Internacionales*, 123-145.

Bo, Y. (2016). Securitization and Chinese Climate Change Policy. *Chinese Political Science Review*, 94-112.

Buzan, B., Waever, O., & De Wilde, J. (1998). *Security: A new framework for analysis.* Lynne Rienner Publishers.

Calås, T. (2019). Quality of Governance and Cybersecurity: A quantitative study into Securitization-theory and Cyberspace. *Tesis de grado*. Uppsala, Suecia: Universidad de Uppsala.

Dunn Cavelty, M. (2020). Cybersecurity between hypersecuritization and technological routine. In Routledge Handbook of International Cybersecurity (pp. 11-21). Routledge.

Cha, V. D. (2000). Globalization and the Study of International Security. Journal of Peace Research, 37(3), 391–403. doi:10.1177/0022343300037003007

Chang, L., Zhong, L., & Grabosky, P. (2016). Citizen co-production of cyber security: self-help, vigilantes, and cybercrime. *Regulation & Governance*.

Ciolan, I. M. (2014). Defining cybersecurity as the security issue of the twenty-first century. A constructivist approach. Revista de Administratie Publica si Politici Sociale, 12(1), 40.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, Journal 4, Issue 10.

Collier, D. (2011). Understanding process tracing. PS: Political Science & Politics, 44(4), 823-830.

Cornish, P., Hughes, R., & Livingstone, D. (2009). Cyberspace and the National Security of the United Kingdom. London, Chatham House.

Dewi, M. K. (2020). Failure of Securitizing the Climate Change Issue at the United Nations Security Council (2007-2019). Andalas Journal of International Studies (AJIS), 9(2), 168-184.

Dockendorff, A., & Duval, T. (2013). Una mirada a la seguridad internacional a la luz de las estrategias de seguridad nacional. *Estudios Internacionales*, 31-49.

Donahoe, E., & Hampson, F. (13 de Noviembre de 2018). *Governance Innovation for a Connected World: Protecting Free Expression, Diversity and Civic Engagement in the Global Digital Ecosystem*. Obtenido de Centre for International Government Innovation: https://www.cigionline.org/publications/governance-innovation-connected-world-protecting-free-expression-diversity-and-civic-0/

Drezner, D. W. (2019). Technological change and international relations. International Relations, 004711781983462. doi:10.1177/0047117819834629

Eggenschwiler, J. (2017). Accountability challenges confronting cyberspace governance. *Internet Policy Review*, Volume 6, Issue 3.

European Commission. (13 de Septiembre de 2017). *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.* Obtenido de EU CYBER DIRECT: https://eucyberdirect.eu/content_knowledge_hu/1624/

European Network and Information Security Agency. (2012). *National cyber security strategies: Setting the course for national efforts to strengthen security in cyberspace.* Union Europea.

Freedman, L. (1998). International Security: Changing Targets. Foreign Policy, (110), 48. doi:10.2307/1149276

Friedman, G. (14 de marzo de 2018). The Geopolitics of Britain. Geopolitical Futures. Obtenido de: https://geopoliticalfutures.com/the-geopolitics-of-britain/

Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, 1-19.

Fritsch, S. (2011). Technology and Global Affairs. *International Studies Perspective*, 27-45.

Funk A. (2003) The Monopoly of Legitimate Violence and Criminal Policy. In: Heitmeyer W., Hagan J. (eds) International Handbook of Violence Research. Springer, Dordrecht. https://doi.org/10.1007/978-0-306-48039-3_54

Geelen, M. (29 de Febrero de 2016). Cyber Securitization and Security Policy. The impact of the Discursive Construction of Computer Security on (National) Security Policymaking in the Netherlands. *Tesis de Maestría*. Universiteit Leiden.

Geneva Centre for the Democratic Control of Armed Forces. (2015). *The Security Sector (SSR Backgrounder Series).* Geneva: Geneva Centre for Security Sector Governance.

Gerring, J. (2004). What is a case study and what is it good for?. American political science review, 341-354.

Goodwin, C., & Nicholas, J. (2013). *Developing a National Strategy for Cybersecurity. Foundation for Security Growth and Innovation.* Microsoft.

Gomez, M. A. N., & Villar, E. B. J. (2018). Fear, uncertainty, and dread: Cognitive heuristics and cyber threats. Politics and Governance, 6(2), 61–72.

Gomez, M. A., & Whyte, C. (2021). Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats. International Studies Quarterly. doi:10.1093/isq/sqab034

Gow, J. (2009). The United Kingdom National Security Strategy: the Need for New Bearings in Security Policy. The Political Quarterly, 80(1), 126–133. doi:10.1111/j.1467-923x.2009.01969.x

Gray, J. (2004). *Al Qaeda y lo que significa ser moderno.* Buenos Aires: Paidós.

Guzzini, S. (2011). Securitization as a causal mechanism. *Security Dialogue*, 329-341.

Haftendorn, H. (1991). The Security Puzzle: Theory-Building and Discipline-Building in International Security. International Studies Quarterly, 35(1), 3. doi:10.2307/2600386

Hall, W., O'Hara, K., & Tsalikis, C. (13 de Junio de 2019). *The Four Visions Shaping the Way We Use the Internet*. Obtenido de Centre for International Governance Innovation: https://www.cigionline.org/articles/four-visions-shaping-way-we-use-internet

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 1155-1175.

Helpman, E. (2009). The mystery of economic growth. Harvard University Press.

Hewitt-Page, D. (29 de Mayo de 2013). Technology and the nation-state: Governing social complexity. Obtenido de Open Democracy: https://www.opendemocracy.net/en/opendemocracyuk/technology-and-nation-state-governing-social-complexity/

Holmes, R. (2015). What Is National Security? *The Heritage Foundation*, 17-26.

Horsman, G. (2017). Can we continue to effectively police digital crime? *Science & Justice*, 448-454.

Hunt, W. B. (1997). Getting to war: Predicting international conflict with mass media indicators. University of Michigan Press.

Inglis, C., & Jensen, B. (12 de Mayo de 2020). *Government cybersecurity commission calls for international cooperation, resilience and retaliation*. Obtenido de The Conversation: https://theconversation.com/government-cybersecurity-commission-calls-for-international-cooperation-resilience-and-retaliation-133610

Johns, E. (2021). Cyber Security Breaches Survey 2021. Departamento de Digital, Cultura, Medios y Deporte, gobierno del Reino Unido.

Joseph, T. (2014). Mediating War and Peace: Mass Media and International Conflict. India Quarterly: A Journal of International Affairs, 70(3), 225–240. doi:10.1177/0974928414535292

Keohane, R. (2008). The Oxford Handbook of International Relations. En C. Reus-Smit, & S. Duncan, *Big questions in the study of world politics.* Nueva York: Oxford University Press.

Keller, W. (2004). International technology diffusion. Journal of economic literature, 42(3), 752-782.

Kernic, F. (2008). La producción de inseguridad en la sociedad global. En C. Navajas, & D. Iturriaga Barco, *Crisis, dictaduras, democracia* (págs. 71-78). Universidad de la Rioja.

Kohler, K. (2020). *Estonia's National Cybersecurity and Cyberdefense Posture.* Zurich: Center for Security Studies.

Kostyuk, N., & Wayne, C. (2020). The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public. *Journal of Global Security Studies*.

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, 1-16.

Leander, A. (2002). Conditional legitimacy, reinterpreted monopolies: globalisation and the evolving state monopoly on legitimate violence (p. 2). Copenhagen Peace Research Institute.

Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High volume cybercrime and the organization of the police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, 7(1).

Levy, I. (1 de noviembre de 2016). Active Cyber Defence - tackling cyber-attacks on the UK. National Cybersecurity Center. Obtenido de: https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

Lewis, J. (29 de enero de 2020). A Short Discussion of the Internet's Effect on Politics. Center for Strategic & International Studies. Obtenido de: https://www.csis.org/analysis/short-discussion-internets-effect-politics

Maxwell, J. A. (2012). Qualitative research design: An interactive approach (Vol. 41). Sage publications.

Mott, G. (2016). Terror from behind the keyboard: conceptualising faceless detractors and guarantors of security in cyberspace. Critical Studies on Terrorism, 9(1), 33-53.

Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet security and networked governance in international relations. *International Studies Review*, 86-104.

Nye Jr, J. S. (2010). Cyber power. Harvard Univ Cambridge MA Belfer Center for Science and International Affairs.

Nye, J. (2012). The Third Annual Ernest May Memorial Lecture. En N. Burns, & J. Price, *Securing Cyberspace: A New Domain for National Security* (págs. 21-40). Washington: The Aspen Institute.

Oggesen, L. (29 de Octubre de 2020). *The questions you should ask in International Security*. Obtenido de Center for Youth and International Studies: https://www.cyis.org/post/the-questions-you-should-ask-in-international-security

O'Hara, K., & Hall, W. (7 de Diciembre de 2018). *Four Internets: The Geopolitics of Digital Governance*. Obtenido de Centre for International Governance Innovation: https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance/

Ooijen, M. (2020). Cyber securitization or cyberization of conflict?–the militarization of Cyber Security in Estonia. *Master's Thesis*. Utrecht University.

Orozco, G. (2006). El concepto de Seguridad en la Teoría de las Relaciones Internacionales. *Revista CIDOB d'Afers Internacionals*, 161-180.

Pernice, I. (5 de Marzo de 2019). *Protecting the global digital information ecosystem: a practical initiative*. Obtenido de Internet Policy Review: https://policyreview.info/articles/news/protecting-global-digital-information-ecosystem-practical-initiative/1386

Renaud, K., & Warketin, M. (29 de Noviembre de 2018). *Swamped by cyberthreats, citizens need government protection*. Obtenido de The Conversation: https://theconversation.com/swamped-by-cyberthreats-citizens-need-government-protection-104827

Rousch, M. (Mayo de 2015). Securitization And Desecuritization in Estonia's Cyber Politics. *Master's Thesis*. Tampere, Finlandia: Universidad de Tampere.

Sain, G. (2018). La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal. En R. Parada, & J. Errecaborde, *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de Internet* (págs. 7-32). Erreius.

Saleem, M. (2019). Brexit Impact on Cyber Security of United Kingdom. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). doi:10.1109/cybersecpods.2019.888

Schmidt, N. (2014). Critical Comments on Current Research Agenda in Cyber Security. *Obrana a strategie*, 29-39.

Shackelford, S. (3 de Septiembre de 2019). *In a world of cyber threats, the push for cyber peace is growing*. Obtenido de The Conversation: https://theconversation.com/in-a-world-of-cyber-threats-the-push-for-cyber-peace-is-growing-119419

Straub, J. (16 de Agosto de 2019). *A cyberattack could wreak destruction comparable to a nuclear weapon*. Obtenido de The Conversation: https://theconversation.com/a-cyberattack-could-wreak-destruction-comparable-to-a-nuclear-weapon-112173

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. Politics and Governance, 6(2), 1-4.

Tabansky, L. (2012). Cybercrime: A national security issue? *Military and Strategic Affairs*, 4(3).

Temperini, M. (2018). Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de Internet. En R. Parada, & J. Errecaborde, *Delitos informáticos y cibercrimen: alcances, conceptos y características* (págs. 7-32). Erreius.

Valeriano, B., & Maness, R. C. (2018). International relations theory and cyber security. The Oxford Handbook of International Political Theory, 259.

Valeriano, B., & Maness, R. (2018). How we stopped worrying about cyber doom and started collecting data. Politics and Governance, 6(2), 49–60.

Vargas Vargas, E. (2014). Ciberseguridad y ciberdefensa: ¿qué implicaciones tienen para la seguridad nacional? *Trabajo de grado*. Bogotá D.C., Colombia: Universidad Militar Nueva Granada.

Wendt, A. (1999). Three cultures of anarchy. Social Theory of International Politics, 246-308.

Wenger, A. (Ed.). (2001). The internet and the changing face of international relations and security. ProCon.

Westcott, N. (2008). Digital diplomacy: The impact of the internet on international relations.

Whyte, C. (2018). Dissecting the digital world: A review of the construction and constitution of cyber conflict research. *International Studies Review*, 520-535.

Yin, R. K. (2009). Case study research: Design and methods. Sage publications. *Thousand oaks*.

Documentos analizados

Aaviksoo, J. (8 de mayo de 2008). Cyber Defese – The Unnoticed Third World War. Ministerio de Defesa, República de Estonia. Obtenido de: https://kaitseministeerium.ee/en/news/defence-minister-jaak-aaviksoo-cyber-defense-unnoticed-third-world-war

Anderson, J. (14 de octubre de 2020). Cámara de los Lores. Obtenido de: https://publications.parliament.uk/pa/ld201011/ldhansrd/text/101014-0003.htm

Ansip, A. (2 de mayo de 2007). Prime Minister Andrus Ansip's speech in Riigikogu on 2 May 2007. Vabariigi Valitsus. Obtenido de: https://www.valitsus.ee/en/news/prime-minister-andrus-ansips-speech-riigikogu

Autoridad de los Sistemas de Información (2013). Summary of the Estonian Information System's Authority on Ensuring Cyber Security in 2012. República de Estonia.

Autoridad de los Sistemas de Información (2014). 2013 Annual Report: Cyber Security Branch of the Estonian Information System Authority. República de Estonia.

Autoridad de los Sistemas de Información (2016). 2015 Annual Report: Cyber Security Branch of the Estonian Information System Authority. República de Estonia.

Blunkett, D. (4 de abril de 2015). "UK Not Ready for Cyber Terror Attacks – Blunkett", The Yorkshire Post. Obtenido de: http://www.yorkshirepost.co.uk/news/main-topics/politics/uk-not-ready-for-cyber-terror-attacks-blunkett-1-7192952

Cabinet Office (2008). The National Security Strategy of the United Kingdom: Security in an interdependent world. Gobierno de Reino Unido. Obtenido de: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf

Cabinet Office. (2015). 2010 to 2015 Government Policy: Cyber Security. Gobierno de Reino Unido. Obtenido de: https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security

Cabinet Office. (2020). National Risk Register. Gobierno de Reino Unido. Recuperado de: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/952959/6.6920_CO_CCS_s_National_Risk_Register_2020_11-1-21-FINAL.pdf

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. International Studies Review, 15(1), 105-122.

Fleming, J. (22 de marzo de 2019). Director's speech at Cyber UK 2018. GCHQ. Obtenido de: https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018

Gobierno del Reino Unido (2015). National Security Strategy and Strategic Defence and Security Review 2015. Obtenido de: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf

Gobierno del Reino Unido. Estrategia de Ciberseguridad Nacional 2016-2020. Obtenido de: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643420/Spanish_translation_-_National_Cyber_Security_Strategy_2016.pdf

Ilves, T. (23 de junio de 2007). President of the Republic On Victory Day, Rapla, 23 June 2007. Esilehele. Obtenido de: https://vp2006-2016.president.ee/en/official-duties/speeches/2584-president-of-the-republic-on-victory-day-23-june-2007-in-rapla/

Kriz, D. (s.f.). *A Global Model: UK's "National Cyber Security Strategy"*. Security Roundtable. Obtenido de: https://www.securityroundtable.org/global-model-uks-national-cyber-security-strategy/

Landler, M., & Markoff, J. (28 de mayo 2007). In Estonia, what may be the first war in cyberspace. The New York Times. Obtenido de: https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html

Martin, C. (6 de septiembre de 2019). Ciaran Martin's speech at the Billington Cyber Security Summit. National Cyber Security Centre. Obtenido de: https://www.ncsc.gov.uk/speech/ciaran-martins-speech-at-billington-cyber-security-summit-2019

Ministerio de Defensa. (2008). Estrategia de Ciberseguridad. Tallin: República de Estonia.

Ministerio de Asuntos Económicos y de Comunicación (2014). Estrategia de Ciberseguridad 2014-2017. Tallin: República de Estonia.

Ministerio de Asuntos Económicos y de Comunicación (2019). Estrategia de Ciberseguridad 2019-2022. Tallin: República de Estonia.

Noyan, O. (8 de septiembre de 2021). Estonia proposes NATO-like expenditure rule for cybersecurity. Euractiv. Obtenido de: https://www.euractiv.com/section/cybersecurity/news/estonia-proposes-nato-like-expenditure-rule-for-cybersecurity/

National Cyber Security Center. (3 de noviembre de 2020). NCSC defends UK from more than 700 cyber attacks while supporting national pandemic response. National Cyber Security

Centre. Obtenido de: https://www.ncsc.gov.uk/news/ncsc-defends-uk-700-cyber-attack-national-pandemic

National Cyber Security Center. (2020). *Annual Review 2020*. Government Communications Headquarters.

Peat, U. (1 de mayo de 2007) Declaration of the Minister of Foreign Affairs of the Republic of Estonia. Republica de Estonia. Obtenido de: https://valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia

POST (2011). POSTnote: Cyber Security in the UK, London: POST

Schmitt, M. N. (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.

Shannon, J. (4 de marzo de 2014). Cámara de los Lores. Obtenido: https://publications.parliament.uk/pa/cm201314/cmhansrd/cm140304/debtext/140304-0002.htm

Tikk, E., Kaska, K., & Vihul, L. (2010). International cyber incidents: Legal considerations. Cooperative Cyber Defence Centre of Excellence (CCD COE).

Traynor, I. (17 de mayo de 2007). Russia Accused of Unleashing Cyberwar to Disable Estonia. The Guardian. Obtenido de: https://www.theguardian.com/world/2007/may/17/topstories3.russia#:~:text=A%20three%2Dweek%20wave%20of,the%20offensive%20and%20its%20implications.