

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE CIENCIAS POLITICAS Y SOCIOLOGIA

MÁSTER EN POLÍTICA INTERNACIONAL

ESTUDIOS SECTORIALES Y DE ÁREA



**LAS RELACIONES BILATERALES RUSIA-ESTONIA Y SU
ESCALADA EN EL CASO DE LOS CIBERATAQUES DE 2007**

Jara Atienza Pastor

Tutor: Felipe Maraña Marcos

Madrid, junio 2020

“No nos conocéis, ni conocéis nuestro mundo. El Ciberespacio no se halla dentro de vuestras fronteras. No penséis que podéis construirlo, como si fuera un proyecto público de construcción. No podéis. Es un acto natural que crece de nuestras acciones colectivas.

No os habéis unido a nuestra gran conversación colectiva, ni creasteis la riqueza de nuestros mercados. No conocéis nuestra cultura, nuestra ética, o los códigos no escritos que ya proporcionan a nuestra sociedad más orden que el que podría obtenerse por cualquiera de vuestras imposiciones.

Estamos creando nuestro propio Contrato Social. Esta autoridad se creará según las condiciones de nuestro mundo, no del vuestro. Nuestro mundo es diferente. El Ciberespacio está formado por transacciones, relaciones, y pensamiento en sí mismo, que se extiende como una quieta ola en la telaraña de nuestras comunicaciones. Nuestro mundo está a la vez en todas partes y en ninguna parte, pero no está donde viven los cuerpos”.

**Declaración de independencia del ciberespacio
John Perry Barlow, 1996**

ÍNDICE

Índice de Ilustraciones _____	3
Lista de abreviaturas _____	4
1.INTRODUCCIÓN _____	5
1.1 Delimitación del tema y objetivos _____	5
1.2 Justificación de la investigación _____	6
1.3 Enfoque metodológico empleado _____	7
1.3.1 Preguntas de investigación _____	7
1.3.2 Hipótesis _____	8
1.3.3 Técnicas de obtención, análisis de la información y limitaciones _____	8
1.4 Plan general y contenido de la obra _____	10
2 . MARCO TEÓRICO _____	12
2.1 El ciberespacio en las relaciones internacionales _____	12
2.2 Naturaleza y tipos de ciberataques _____	15
2.3 Desarrollo de las estrategias de ciberseguridad _____	17
2.4 Estado de la Cuestión y contexto _____	22
3. RELACIONES BILATERALES RUSO- ESTONIAS _____	26
3.1 Relaciones antes de la incorporación de Estonia a la UE y a la OTAN _____	26
3.1.1 Procesos de desmilitarización _____	29
3.1.2 Contencioso fronterizo _____	31
3.1.3 Conflicto de minorías étnicas _____	35
3.2 Relaciones bilaterales tras la adhesión de Estonia a la UE y la OTAN _____	47

4. RELACIONES RUSIA-OTAN _____	50
5. DESARROLLO DEL CONFLICTO _____	54
5.1 Crisis del soldado de bronce _____	54
4.1.1 Reacciones diplomáticas a las protestas _____	58
5.2 El ciberataque _____	58
5.2.1 Desarrollo, naturaleza y alcance nacional de los ciberataques _____	58
5.2.1 Reacciones diplomáticas a los ciberataques _____	62
6. IMPLICACIONES EN EL MARCO DE LA OTAN Y DESARROLLO DE LA CIBERSEGURIDAD _____	65
6.1 Alcance de los ciberataques en el marco de la OTAN _____	65
6.2 Desarrollo de la Ciberseguridad Estonia-OTAN _____	68
7. CONCLUSIONES _____	71
7.1. Determinación de la validez de la hipótesis _____	71
7.2. Cumplimiento de los objetivos y objetivos secundarios de la investigación _	74
BIBLIOGRAFÍA _____	76

Índice de Ilustraciones

Tabla 1: Principales ataques cibernéticos

Figura 1: Principales riesgos globales en términos de probabilidad e impacto

Tabla 2: Ejemplos de Estrategias Nacionales de Ciberseguridad

Tabla 3: Estimación de militares rusos en las Repúblicas bálticas 1992-1993

Figura 2: Fronteras definidas en el Tratado de Tartu vs la línea de control

Tabla 4: Evolución de la estructura étnica de Estonia 1922-59

Tabla 5: Estructura de la población por nacionalidad, 1989- 2000

Figura 3: Mapa de las principales zonas urbanas de Estonia (Tallin, Maardu, Pärnu, Narva, Sillamae, Khotla-Järve)

Tabla 6: Cambios de la población estonia en Tallin, Narva, Sillamae, Khotla-Jarve según los censos 1934-2000

Figura 4: Distribución de la población de lengua rusa en Estonia, censo 2000

Tabla 7: Población según su origen étnico y su lengua materna, censo 2000

Tabla 8: Población por lugar de residencia y ciudadanía, 2000 (porcentajes)

Tabla 9: Población por ciudadanía y nacionalidad, 2000

Figura 5: Evolución de la sociedad digital de Estonia 1994-2007

Tabla 10: Reacciones diplomáticas de Estonia a los ciberataques en 2007

Tabla 11: Reacciones diplomáticas de Rusia a los ciberataques en 2007

Tabla 12: Reacciones diplomáticas de la OTAN en los ciberataques en 2007

Lista de abreviaturas

CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCN-CERT Team	Centro Criptológico Nacional Computer Emergency Response
CdE	Consejo de Europa
CE	Comisión Europea
CERT	Equipo Nacional de Respuesta ante Incidentes Informáticos (CERT)
ICI	Infraestructuras Críticas de Información
OTAN	Organización del Tratado del Atlántico Norte
OSCE	Organización para la Seguridad y la Cooperación en Europa
TIC	Tecnologías de Información y Comunicación
TFM	Trabajo de Final de Máster
UE	Unión Europea
URSS	Unión Soviética

1. INTRODUCCIÓN

1.1 Delimitación del tema y objetivos

La escalada de conflictos interestatales y regionales en el ciberespacio de los últimos años ha significado que la construcción de normas nacionales e internacionales de ciberseguridad sea cada vez más investigadas en el plano teórico y práctico. En este escenario, la República de Estonia ha desempeñado un papel de liderazgo en los esfuerzos internacionales de desarrollo de la ciberseguridad (Zaaiman y Leenan, 2015), sobre todo en el marco de la Alianza Atlántica. Desde 2008 lidera las diferentes estrategias de seguridad y defensa de la de la OTAN y de la Unión Europea en el ciberespacio.

En 2007, Estonia fue víctima de una oleada masiva de ciberataques, a raíz de la cual se impulsó el desarrollo del modelo estatal de gobernanza digital y de ciberseguridad. A día de hoy es el país más digitalizado y seguro del mundo. Aunque existen diferentes teorías sobre la autoría de los ataques y no se ha encontrado evidencias concluyentes, la naturaleza y el desarrollo de la crisis del Soldado de Bronce apunta a una escalada de tensión en el marco de las relaciones bilaterales con Rusia definidas por diversos puntos de confrontación desde la independencia de la ex república soviética en 1991 y, a su vez, marcadas por dilemas de seguridad, diferencias en las concepciones de la narrativa histórica (Galbreath y Lasas, 2013) y un conflicto de identidad (Viktorova, 2006). A este aspecto se le suman las tensiones acaecidas por la adhesión de Estonia a la OTAN y la Unión Europea en 2004.

Atendiendo a este contexto, este Trabajo Final de Máster busca realizar una exploración sobre las relaciones bilaterales entre Rusia y Estonia, y su implicación en el estallido del conflicto del Soldado de Bronce, los ciberataques posteriores y el desarrollo cibernético de Estonia dentro y fuera del marco de cooperación con la OTAN. En este sentido, a pesar de existir controversia teórica sobre la conexión de las relaciones Estonia-Rusia y OTAN-Rusia en su implicación en el conflicto, hemos creído conveniente analizar –a través de fuentes secundarias (institucionales e investigaciones previas)– no sólo las

relaciones bilaterales desde una perspectiva histórica, sino incluyendo una breve revisión de la relación Rusia-OTAN y Estonia-OTAN.

En el sentido de lo arriba descrito y en concordancia con las preguntas de investigación posteriormente concretadas, el objetivo general del TFM será: “Definir el peso de las relaciones bilaterales entre Rusia y Estonia en los ciberataques de 2007”. Para llevar a cabo este objetivo se atenderán los asuntos político-militares, las realidades demográficas y la importancia de cada uno de los actores.

Asimismo, planteamos como objetivos específicos los siguientes:

- Describir la naturaleza de las relaciones bilaterales entre Rusia y Estonia
- Concretar los principales puntos de tensión y su evolución hasta 2007
- Determinar el papel de las relaciones OTAN-RUSIA en los ciberataques
- Analizar las implicaciones de los ciberataques en el marco de seguridad de Estonia y de la OTAN

1.2 Justificación de la investigación

Las relaciones entre Rusia y Estonia han sido objeto de estudio desde una doble perspectiva: desde el punto de vista de las relaciones ruso-bálticas y desde el punto de vista de las relaciones Rusia-OTAN. En este sentido, consideramos esencial aportar un análisis específico de las relaciones ruso-estonias hasta el ciberataque, teniendo en cuenta la influencia actual que tiene Estonia en los esfuerzos internacionales de desarrollo de la ciberseguridad. Así, a través de un análisis histórico evaluaremos los principales puntos de tensión entre ambos países en dos fases: desde la independencia de Estonia hasta su incorporación a la OTAN y la UE (2004), y desde 2004 hasta 2008, pasando por los ciberataques hasta la creación de uno de los principales organismos en materia de ciberseguridad en Estonia y la OTAN; el Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN (CCDCOE).

El presente trabajo no tiene como principal consideración el análisis de los hechos acontecidos en 2007 (ciberataques) ni la ratificación de su autoría, sino que centrará su

enfoque en la evolución de las relaciones bilaterales de ambos países considerando los ciberataques como un punto de inflexión en el ámbito bilateral e internacional. Por un lado, nos dedicaremos a aportar información sobre las principales problemáticas entre la potencia heredera de la Unión Soviética y la ex república soviética; algunas de ellas resueltas durante la década de los 90 y otras persistentes a lo largo del siglo XXI. Por otro lado, estudiaremos la continuación de las mismas y los problemas añadidos durante y tras la adhesión de Estonia a las organizaciones occidentales. De modo transversal, prestaremos especial interés al papel del ciberespacio en el marco de las relaciones internacionales para intentar comprender el por qué del refuerzo de las estructuras digitales de Estonia (en el marco de la Alianza) como respuesta a los ciberataques de 2007.

Por último, consideramos que es necesario seguir trabajando en el análisis y estudio de esta cuestión, puesto que es un tema que sigue afectando a las relaciones internacionales y al desarrollo de las estrategias nacionales de defensa cibernética. De la misma manera, se recomienda continuar con la profundización de las cuestiones investigadas, ya que la naturaleza del ciberespacio hace necesaria la continua revisión de las estrategias de ciberseguridad, y la evolución de las relaciones Estonia y Rusia, y el desarrollo estratégico de los sistemas de ciberdefensa hace posible el cambio de las variables de la investigación.

1.3 Enfoque metodológico empleado

1.3.1 Preguntas de investigación

Esta investigación busca resolver la pregunta general (PG): ¿Hasta qué punto las relaciones entre Rusia y Estonia, y no las relaciones OTAN-Rusia, influyeron en la perpetuación de los ciberataques masivos y el posterior desarrollo de Estonia en materia de ciberseguridad?

Para lograr contestar a esta pregunta se plantean las siguientes preguntas específicas que guiarán el estudio:

1. ¿Cuál fue el principal detonante el primer ataque cibernético contra el Estado de Estonia?

2. ¿Qué papel juega el ciberespacio en el marco de la defensa nacional de Estonia?
3. ¿A qué responde la evolución de Estonia en materia de ciberseguridad inmediatamente después de los ataques de 2007 en el marco de la OTAN?

1.3.2 Hipótesis

La hipótesis principal (HP) que se presenta es que “las tensiones acumuladas en las relaciones ruso-estonias motivaron un ciberataque masivo que ha impulsado el desarrollo de Estonia y la OTAN en materia de ciberseguridad”.

En cuanto a las hipótesis secundarias (HS) tenemos las siguientes:

1. El estallido del conflicto de 2007 responde a una evolución de las relaciones bilaterales desde la independencia de Estonia (marcada por diversos puntos de tensión desde la disolución de la URSS) y no a la evolución de las tensiones en el marco OTAN-Rusia
2. El desarrollo de la seguridad Estonia responde a una necesidad de protegerse de Rusia por un dilema de seguridad existente desde la independencia de Estonia
3. El desarrollo de la excelencia en ciberseguridad de Estonia ha mejorado la posición de Estonia en la OTAN y a su vez, la de la OTAN en el marco OTAN-Rusia.

De esta manera, la relación entre preguntas de investigación e hipótesis formuladas quedaría como sigue:

-Pregunta 1 → HP, HS1

-Pregunta 2 → HS2, HS3

-Pregunta 3 → HS3

1.3.3 Técnicas de obtención, análisis de la información y limitaciones

Para el desarrollo de la presente investigación se llevará a cabo una aproximación cualitativa, dado que permite el desarrollo de preguntas e hipótesis después o durante la recolección y análisis de la información recogida (Hernández Sampieri et. al., 2010). Al

tratarse de un estudio de caso, esta investigación tiene un carácter interpretativo y no posibilista que estará basado en una combinación de procedimientos metodológicos.

A través de las informaciones indirectas obtenidas de la revisión de fuentes secundarias, se parte del método descriptivo, cuya finalidad es *“obtener, interpretar y presentar, con el máximo rigor o exactitud posible, la información sobre una realidad de acuerdo con ciertos criterios previamente establecidos por cada ciencia”* (Calduch, 2014: 29). Este método nos ofrecerá una primera aproximación al ciberespacio, su naturaleza y alcance en las relaciones internacionales y el papel de ciertas actividades desarrolladas en él (ciberataques) en las estrategias de ciberseguridad.

Posteriormente se emplea el método analítico, que consiste en *“la utilización de la descripción general de una realidad para realizar la distinción, conocimiento y clasificación de sus elementos esenciales y las relaciones que mantienen entre sí”* (Ibid., 30). A través de él se estudiará la realidad de las relaciones bilaterales entre Rusia y Estonia, atendiendo a los principales puntos de tensión y el desarrollo de los acontecimientos de 2007.

Para completar este análisis se utilizará el método comparativo que, de acuerdo con Calduch, permite realizar *“una contrastación entre los principales elementos de la realidad que se investiga con los de otras realidades que se consideran similares y que ya son conocidas”* (Ibid.,34) y que precisa de la búsqueda de semejanzas y diferencias de una misma realidad. Este procedimiento nos permitirá captar la dimensión dinámica en términos históricos de la realidad de las relaciones bilaterales entre Estonia y Rusia en su contexto internacional más próximo en cada momento histórico.

Para finalizar, se aplicará una combinación del método inductivo que nos permitirá articular relaciones de causalidad generales sobre las realidades concretas estudiadas y facilitar las formulación de proposiciones de validez general. A su vez, el método deductivo facilitará el refuerzo de las formulaciones extraídas a través del método inductivo y favorecerá el conocimiento de las características de la realidad investigada.

En cuanto a las principales limitaciones de la investigación que se han encontrado, la principal deriva de los métodos descriptivos y analíticos utilizados previamente mencionados. En este caso en concreto, tanto las deducciones como las conclusiones recogidas se refieren exclusivamente a las relaciones bilaterales entre Rusia y Estonia en el contexto de los ciberataques de 2007. Por tanto, las conclusiones no pueden extrapolarse a otras relaciones entre dos actores ni siquiera aunque se den dentro del mismo marco contextual y temporal.

En relación a la obtención de información y datos, una de las principales dificultades ha sido el idioma en el que se encuentran algunos contenidos de relevancia, como la Ley de Ciudadanía de Estonia de 1992, cuya única versión disponible está en estonio. Este hecho ha dificultado la traducción literal de ciertos contenidos, aunque se ha utilizado el traductor predeterminado del buscador. Asimismo, otra de las dificultades más acusadas ha sido que algunos contenidos eran de pago, por lo que una de las soluciones ha sido acceder a documentos secundarios.

1.4 Plan general y contenido de la obra

El presente TFM consta de siete capítulos. El primer capítulo está compuesto por esta introducción, el segundo lo constituye el Marco Teórico, dentro del cual abordaremos desde una perspectiva teórica tres cuestiones: el papel del ciberespacio en las relaciones internacionales, las ataques que tienen lugar en él y su relevancia en el desarrollo de las estrategias de seguridad nacionales.

A continuación del Marco Teórico se incluye el estado de la cuestión, en el cual se detallan las principales investigaciones sobre las relaciones internacionales entre Rusia y Estonia, atendiendo a su relación con el conflicto de Estonia de 2007.

En el tercer capítulo se desarrollarán las relaciones bilaterales entre Rusia y Estonia a lo largo del siglo XX e inicios del XXI, analizando los principales puntos de tensión antes –a saber, el proceso de desmilitarización, el contencioso fronterizo y el problema de las minorías rusas– y después de las adhesión de la incorporación de Estonia a la UE y la OTAN.

El cuarto capítulo está compuesto por un análisis de las relaciones Rusia-OTAN definido en el marco temporal de 1991 a 2007 y en el que se presentan las principales concepciones previas sobre la naturaleza y desarrollo de las relaciones entre ambas.

En el quinto capítulo se presenta el desarrollo del conflicto, empezando con la descripción del conflicto del Soldado de Bronce de Tallin y las reacciones diplomáticas posteriores en el ámbito bilateral. Se continúa con un análisis del desarrollo cronológico y la naturaleza de los ciberataques. Se incluye también una evaluación de las respuestas diplomáticas de las dos partes.

En el quinto capítulo se especifica el impacto de los ciberataques en el marco de ciberseguridad de la OTAN, así como el desarrollo conjunto de los sistemas de defensa del ciberespacio entre la Alianza Atlántica y Estonia.

En el séptimo y último capítulo presentamos las principales conclusiones y un contraste de las hipótesis principal y secundarias planteadas en la introducción.

2. MARCO TEÓRICO

2.1 El ciberespacio en las relaciones internacionales

La inclusión del ciberespacio en las relaciones internacionales ha sido objeto de debate teórico en las ciencias militares y en la literatura sobre seguridad y defensa debido a su naturaleza singular en comparación con el resto de espacios operacionales. De acuerdo con Joyanes Aguilar (2010), se diferencia de los escenarios tradicionales de batalla –tierra, mar, aire y espacio– por ser “*un dominio que no es físico, sino virtual*”. Aunque esta característica es aceptada en el amplio de las opiniones académicas, la discusión gira en torno a la definición completa de esta nueva realidad y sus posibles implicaciones dentro del ámbito de la seguridad y defensa nacional.

La primera referencia al ciberespacio se encuentra en la novela de ficción *Neuromante* (1984), en la que su autor, el escritor norteamericano William Gibson, describe una “*alucinación consensuada [...] experimentada por una representación gráfica de la información abstraída de los bancos de datos de todos los ordenadores del sistema humano*”.

Tras esta primera aproximación literaria, durante los años 90 se multiplicaron las diferentes perspectivas sobre las dimensiones y el alcance del ciberespacio. En su libro *Information Warfare: Chaos on the Electronic Superhighway* (1994), el experto en ciberseguridad Winn Schwartau aporta una de las primeras definiciones de ciberespacio en el marco de la seguridad. Su visión incide en la capacidad de transmisión de información de este espacio virtual que expone a individuos, instituciones y gobiernos a una situación de vulnerabilidad sin precedentes:

“Se trata de un lugar intangible entre ordenadores donde la información existe momentáneamente en su trayecto desde un destino de la red global hacia otro... Una realidad etérea, infinidad de electrones acelerando a través del cobre o de fibras de vidrio a la velocidad de la luz... El ciberespacio no tiene límites, pero a la vez pensemos en el

ciberespacio como algo dividido en grupos locales o regionales de ciberespacio –cientos de millones de pequeños ciberespacios alrededor del mundo” (Schwartau, 1994: 26-27).

Otros autores, como la investigadora Dorothy Denning (1999), introducen un enfoque centrado en el carácter tecnológico del ciberespacio. Lo define como “*un lugar de información basado en la suma total de todas las redes de ordenadores*” (citado en Kramer et al., 2009:25, traducción propia). En la misma línea, Walter Gary Sharp (1999) lo presenta como “*un entorno creado por la confluencia de redes cooperativas de ordenadores, sistemas informáticos e infraestructuras de las telecomunicaciones*” (Ibidem).

En el marco internacional, entidades y organizaciones recogen definiciones amplias como la de la Comisión Europea que lo describe como “*el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo*”.

Junto a estas definiciones, Daniel T. Kuehl recoge en *From Ciberspace to Cyberpower: Defining the Problem* (2009) la evolución del término hasta mediados de los años 2000, momento en el que, debido al crecimiento masivo de la interacción y las conexiones, y a los riesgos y amenazas asociados a su utilización, comienza a ganar peso el concepto de *ciberespacio* como un nuevo campo de batalla de los actores internacionales (Joyanes Aguilar, 2010). No obstante, con anterioridad, las diferentes agencias de seguridad ya contemplaban el ciberespacio como una potencial amenaza.

El 27 de junio de 1991 Schwartau compareció ante al Congreso estadounidense y alertó de la alta probabilidad de que se materializase un “Pearl Harbour electrónico”; un ataque digital masivo que interfiriera en las infraestructuras críticas del país. Años antes, en 1984, la administración Reagan ya advirtió que la era de la información traería consigo nuevos desafíos en materia de seguridad. Sin embargo, según sostienen Michèle Flournoy y Michael Sulmeyer (2018) en su artículo *Batterfield Internet*, desde la propia existencia del ciberespacio, este ha sido reconocido como un “*nuevo ámbito de competición entre estados*”.

En 2010, la revista *The Economist* declaraba por primera vez el ciberespacio el quinto dominio después de la tierra, el mar, el aire y el espacio (citado en Joyanes, 2010:14). Ese mismo año, el vicesecretario de Defensa del Gobierno de los Estados Unidos, William J. Lynn, solicitaba que el “*ciberespacio debía ser reconocido como un territorio de dominio igual que el resto en lo relativo a la guerra*” (Pellerin, 2010).

Con la concepción del ciberespacio como un dominio global, este ha quedado definido, desde el punto de vista del Derecho Internacional como uno de los cuatro Espacios Comunes (del inglés, *Global Commons*), aquellos espacios que no están bajo la soberanía de ningún Estado en concreto, pero que pueden ser utilizados por cualquiera. Estos son: el mar, el espacio ultraterrestre, el espacio aéreo y el ciberespacio (Stang, 2013). Sin embargo, la condición inmaterial o no física de este dominio lo sitúa en un plano diferente al resto de Espacios.

Al inicio de su trabajo teórico, Ángel Gómez de Ágreda (2010) cita el carácter inmaterial y artificial como principal elemento distintivo. Posteriormente, el autor identifica su naturaleza o “esencia” (transversal, sin fronteras y global) como verdadero factor diferencial:

“Lo distintivo es el modo en que altera las realidades de los otros tres dominios. Mientras que los Commons materiales tienen límites definidos de forma más o menos precisa, el ciberespacio es absolutamente transversal a todos ellos y se solapa con los tres alterando la percepción que tenemos de los mismos” (citado en Robles Carrillo, 2015)

La consideración del ciberespacio como un escenario estratégico y operativo de naturaleza diferente (virtual) a los ámbitos convencionales supone un reto en el campo de la seguridad. El intento de los Estados por defender este nuevo dominio ha provocado un cambio en las concepciones de seguridad y defensa tradicionales, así como en sus estrategias o conceptos nacionales, debido a que la defensa del ciberespacio –también conocido como ciberseguridad– se rige por parámetros distintos a los usados para la seguridad marítima, terrestre o espacial (Ibid.).

2.2 Naturaleza y tipos de ciberataques

Los ciberataques engloban todas aquellas acciones realizadas dentro del ciberespacio que se utilizan para producir daño o desestabilizar a empresas, organismos o individuos. Aunque no existen definiciones comunes para términos cibernéticos, en el Manual Tallinn sobre el Derecho Internacional aplicable a la Ciberguerra (2013) –texto académico publicado por el Centro de Excelencia de Defensa Cooperativa de la OTAN tras el ciberataque contra Estonia, objeto principal de este trabajo–, el término ciberataque viene definido como *“cualquier operación cibernética, ofensiva o defensiva, de la que razonablemente se espera que pueda causar pérdidas de vidas humanas, lesiones a personas, o daño o destrucción de bienes materiales”*.

Según el Glosario de terminología de uso conjunto del Instituto Español de Estudios Estratégicos, estas operaciones se pueden materializar *“comprometiendo la disponibilidad, integridad o confidencialidad de la información, mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan”*. Amenazas como el ciberterrorismo, el ciberdelito, el cibercrimen, el ciberespionaje o el hacktivismo se vertebran a través de ciberataques, aunque cada agencia de seguridad cuenta con sus propias definiciones conceptuales para estos términos en función del objetivo o el alcance de la agresión (J. Ureña, 2015).

La literatura existente sobre los tipos de ciberataques es muy amplia y se encuentra en constante cambio debido a las cada vez más numerosas y nuevas amenazas cibernéticas derivadas del rápido desarrollo de las TIC. Caro Bejarano (2010) recoge algunos de los ataques cibernéticos básicos más conocidos siguiendo las definiciones recogidas en la Guía de Seguridad del Centro Criptológico Nacional (CCN-CERT, 2015). Podemos resumir algunas de las amenazas cibernéticas básicas en función de su naturaleza informática en el siguiente cuadro:

Tabla 1: Principales ataques cibernéticos

Malware	También conocido como <i>código dañino</i> o <i>software malicioso</i> , es un tipo de software cuyo objetivo es infiltrarse en un sistema de información sin autorización del propietario, para dañarlo o ser perjudicial de alguna manera. Esta definición general recoge diferentes tipos de ciberataques como virus, gusanos, troyanos, spyware, que se diferencian en la forma de actuar.
Virus	Es un programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.
Gusano	Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red de ordenadores.
Bomba Lógica	Es una cadena de códigos que se ejecuta cuando se produce determinada condición, por ejemplo, tras encender el ordenador cierto número de veces, o pasados una serie de días desde el momento en que la bomba lógica se instala en el ordenador.
Troyano	Es un programa que no se replica ni hace copias de sí mismo, sino que tiene la apariencia de ser un programa útil o inocente, pero en realidad oculta un subprograma que tiene propósitos dañinos, como permitir intrusiones o borrar datos.

Fuente: Glosario de Términos de Seguridad del Centro Criptológico Nacional. Elaboración propia

Paralelamente a esta catalogación, encontramos otro tipo de ciberataques más complejos que vienen definidos por la técnica utilizada o por el objetivo. En ocasiones su desarrollo emplea una o varias de las amenazas anteriormente descritas. A continuación, la compilación de algunos de los tipos de ciberataques pertinentes para el desarrollo de este trabajo atendiendo a las definiciones recogidas dentro del Glosario de Términos de Seguridad del Centro Criptológico Nacional:

- **Ataque de Denegación de Servicio (DoS).** Se trata de un conjunto de técnicas que se utilizan para dejar un servidor inoperativo, sobrecargándolo a través de códigos dañinos para que no pueda ser utilizado por su usuario legítimo. El ataque consiste en enviar una alta cantidad de peticiones al servidor de un dispositivo de tal manera que este no pueda responder y acabe colapsándose.
- **Ataques de Denegación de Servicio Distribuido (DDoS).** Cuando las solicitudes se envían de manera simultánea y coordinada a varios equipos se le denomina DDoS. Es, al fin y al cabo, un ataque DoS en el que participan numerosos atacantes contra numerosos objetivos.
- **Botnet.** Se denomina así a una red de ordenadores controlados de manera remota por un atacante (previa infección por *malware*) y que, en su conjunto, acostumbran a ser utilizados para realizar actividades maliciosas como el envío de Spam o realizar ataques de denegación de servicio.

A pesar de las diferencias en el método operacional que presentan los diferentes tipos de ciberataques, en general comparten algunas características. En primer lugar, suelen ser de bajo coste –ya que las herramientas son de fácil acceso y se pueden descargar en Internet– y de fácil empleo –puesto que no se necesitan grandes conocimientos para su utilización y, en ocasiones, cuentan con indicaciones sencillas de aplicar–. Además, son de gran efectividad en comparación con el bajo riesgo que suponen para el atacante. Dicho de otro modo: la probabilidad de que se alcance el objetivo buscado con el ataque es muy alta, mientras que resulta complicado atribuir un ataque debido a que éste se puede realizar en remoto y desde distintas herramientas (Candau Romero, 2011:259-261).

2.3 Desarrollo de las estrategias de ciberseguridad

El rápido desarrollo de las nuevas tecnologías de la información ha propiciado que el ciberespacio haya modificado de manera sustancial el modo que tienen empresas, gobiernos y ciudadanos de relacionarse e intercambiar información, y bienes y servicios. Este escenario de interacción internacional no tiene fronteras, su alcance es global y las

actividades o ataques que pueden desarrollarse en él suponen un potencial riesgo para la seguridad y prosperidad nacional. De ahí se deriva que en los últimos años, la protección del ciberespacio se haya colocado en el centro del debate de la seguridad.

Como bien expone Caro Bejarano (2010), “la seguridad del ciberespacio es un objetivo estratégico de la seguridad nacional”. En este sentido, urge la constitución de sistemas de ciberseguridad nacionales sólidos y, por ende, la creación de Estrategias Nacionales de Ciberseguridad, algunas de las cuales se analizarán a continuación atendiendo a su carácter defensivo.

Figura 1: Los cinco principales riesgos globales en términos de probabilidad e impacto



Fuente. Global Risk Report, WEF

La consideración de la protección del ciberespacio como un elemento relevante para la seguridad nacional ha sido progresiva y asimétrica. Hasta 2012, en el Informe de Riesgos Globales (*Global Risk Report 2012*), elaborado en base a un análisis de una red de expertos internacional en colaboración con el World Economic Forum y con el apoyo de Marsh & McLennan, no se incluyeron los ataques cibernéticos entre los cinco principales riesgos globales para la estabilidad mundial en términos de probabilidad. Aunque es cierto que en 2007 se incluyeron los ataques tecnológicos contra las Infraestructuras Críticas de la Información como principal riesgo en términos de probabilidad (véase Figura 1).

No obstante, entidades como la Organización del Tratado del Atlántico Norte (OTAN), ya habían elaborado su propio análisis de riesgos. En la primavera de 2010, un grupo de expertos liderado por la antigua Secretaria de Estado de Estados Unidos, Madeleine Albright, publicó un informe en el que se contemplaban los ciberataques como una de las tres principales amenazas más probables para la Alianza Atlántica (Joyanes, 2010:33).

En febrero de 2003, el Gobierno de Estados Unidos presentó su primera estrategia de Seguridad Nacional en el Ciberespacio, coincidiendo con el impulso de las estrategias de defensa nacionales que se realizaron en el país tras los ataques del 11 de septiembre de 2001. Esta fue revisada posteriormente en 2009 por orden del presidente Barack Obama. A excepción de EE.UU., la mayoría de las estrategias de ciberseguridad nacionales se publicaron entre el 2009 y 2011, después de los ciberataques de Estonia (2007) y Georgia (2008). Fue precisamente Estonia el primer país en publicar su *Estrategia de Ciberseguridad* (febrero de 2008), seguido de Eslovaquia (*Estrategia Nacional Eslovaca de Seguridad de la Información*, 2008). Otros países europeos como Países Bajos, Francia o Reino Unido presentaron sus estrategias en 2011. En la siguiente tabla se recogen algunas de las estrategias nacionales de seguridad y su publicación:

Tabla 2: Ejemplos de Estrategias Nacionales de Ciberseguridad

<i>País</i>	<i>Mes/Año</i>	<i>Estrategia</i>
Estados Unidos	Feb. 2003	<i>The National Strategy to Secure Cyberspace</i>
Estonia	Sep. 2008	<i>Cyber Security Strategy</i>
Canadá	Oct. 2009	<i>Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada</i>
Australia	Nov. 2009	<i>Cyber Security Strategy</i>
Japón	Mayo.2010	<i>Information Security Strategy for Protecting the Nation</i>
Alemania	Feb. 2011	<i>Cyber Security Strategy for Germany</i>
Francia	Feb. 2011	<i>Information systems defence and security. France's Strategy</i>
India	Abr. 2011	<i>Discussion Draft on National Cyber Security Policy</i>
Países Bajos	Feb. 2011	<i>The National Cyber Security Strategy (NCSS). Strength through Cooperation</i>
Rumanía	Mayo 2011	<i>Estrategia de Seguridad Cibernética de Rumanía</i>
Nueva Zelanda	Jun. 2011	<i>New Zealand's Cyber Security Strategy</i>
República Checa	Jul. 2011	<i>Cyber Security Strategy of the Czech Republic for the Period 2011-2015</i>
Corea del Sur	Ago. 2011	-
Uganda	Nov. 2011	<i>National Information Security Strategy</i>

Reino Unido	Nov. 2011	<i>The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world</i>
Sudáfrica	Mar. 2012	<i>Notice of Intention to Make South African National Cyber- security Policy</i>
Suiza	Jun. 2012	<i>National Strategy for Protection of Switzerland against Cyber Risks</i>

Fuente: National Cyber Security Framework (2012)

De acuerdo con Luijff, Besseling y Graaf (citado en Klimburg, 2012) cada Estado define su estrategia en función de la propia interpretación de conceptos como el ciberespacio o los ciberataques. Asimismo, la definición de las diferentes líneas estratégicas varía según la percepción de las amenazas cibernéticas. No obstante, del análisis de las principales estrategias de seguridad cibernética arriba expuestas se derivan seis dimensiones para las que los ciberataques suponen una amenaza. Estas son: las Infraestructuras Críticas de la Información (ICI), la prosperidad económica, la seguridad nacional, el bienestar social, la confianza pública en las TIC y la globalización.

Cabe destacar que la amenaza a las Infraestructuras Críticas de la Información –entendidas como las instalaciones, redes, sistemas y equipos físicos y de la tecnología de la información necesarias para el buen funcionamiento de los servicios esenciales de un país y cuya interrupción puede repercutir gravemente en el bienestar económico o de seguridad de un Estado (CCN-CERT, 2015)– están presentes en prácticamente todas las estrategias, mientras que otros, como la amenazas a la globalización, no aparecen explícitamente en todas.

De la revisión y comparación de las diferentes estrategias se identifican también las principales fuentes de ciberamenazas: amenazas cibernéticas a través de ataques a gran escala, terroristas, Estados extranjeros, espionaje, crimen organizado o activismo político contra las ICI (Ibídem). Estos agentes con capacidad de ataque pueden estar interrelacionados entre sí, y sus motivaciones y finalidades son también diversas. No obstante, actualmente los ataques promovidos por Estados son la principal fuente de

amenazas. Así lo señalan los últimos informes publicados por el Centro Criptológico Nacional:

“Los Estados, y los grupos patrocinados por ellos, y sus acciones contra otros países, sus instituciones, empresas y ciudadanos siguen representando la ciberamenaza más significativa. El objetivo perseguido por este tipo de ataques es siempre el mismo: sustraer información para mejorar su posición estratégica, política, económica o innovadora (espionaje). A este objetivo se ha unido el intento de influir en la opinión pública de los países atacados” (CCN-CERT, 2019:6).

En los últimos años se han registrado múltiples ataques a nivel internacional en el que un Estado o grupos patrocinados por él son sospechosos de haber perpetrado un ciberataque. En base a los datos recogidos por el Rastreador de Operaciones Cibernéticas del *think tank* Council on Foreign Relations, desde 2005, 28 países (incluido Estados Unidos) han sido acusados de haber promovido operaciones cibernéticas en defensa de sus intereses en materia de política exterior.

2.4 Estado de la Cuestión y contexto

Actualmente los ciberataques son considerados uno de los diez primeros riesgos para la prosperidad global, tanto en impacto como en probabilidad, según el *Global Risk Report* de 2020 elaborado por el Foro Económico Mundial. Se espera además (el 76,1% de los expertos consultados), que a lo largo del año y en la próxima década aumenten los ciberataques a infraestructuras. En retrospectiva, los ataques cibernéticos son considerados un riesgo a nivel mundial desde 2012, aunque existen registros de ataques a los ordenadores estratégicos de OTAN en Kosovo en 1999 y consideraciones, como las expuestas anteriormente, sobre las potenciales amenazas asociadas al origen del ciberespacio.

No obstante, a nivel internacional, la concepción de los ataques cibernéticos como un riesgo para la seguridad nacional ha ido evolucionando –y materializándose en estrategias definidas orientadas a la defensa de este dominio– a lo largo de los años en función de las

propias percepciones sobre el ciberespacio. Según lo expuesto en el Marco Teórico, la naturaleza transnacional y cambiante, y el desarrollo y las actividades realizadas en él, han convertido el ciberespacio en un escenario estratégico y un punto central en el desarrollo de los sistemas de seguridad internacionales. El especialista nacional de la División de Operaciones de la OTAN, Dr. Olaf Theiler, exponía su relevancia de la siguiente manera:

“A menudo se dice que el 11 de septiembre de 2001 fue el día en que todo cambió. Quizás no tanto para nuestra vida cotidiana, pero en el terreno de la seguridad supuso el inicio de una nueva era. Nuestra percepción tradicional de la seguridad se derrumbó junto a las Torres Gemelas. El escenario dominado por la guerra fría durante más de 50 años quedó radical e irreparablemente modificado.

Las amenazas ya no tenían un remitente claro (y estatal). Las fronteras territoriales dejaron de tener sentido, al igual que el dominio militar del espacio y tiempo. El uso de aviones civiles en un atentado terrorista demostró que casi cualquier cosa puede convertirse en un arma, en cualquier momento. De pronto nada parecía imposible o impensable.

Prácticamente se podría decir lo mismo de las amenazas cibernéticas” (publicado en Revista de la OTAN, 2001).

En este contexto, los ciberataques de Estonia de 2007 supusieron un antes y un después en el marco de la seguridad internacional. Según expone Feliu Ortega (2012:65): *“Aunque muchas naciones recibían y reciben a diario ciberataques –de la misma envergadura y mayor– contra la infraestructura crítica del país (...) en el caso de Estonia fue diferente, pues debido a la dimensión del país, los ataques le llevaron a una situación de crisis de Seguridad Nacional”*. Asimismo, fue la primera vez que la OTAN recibía la solicitud de apoyo técnico por un ataque a las Infraestructuras Críticas de Información del país (Ibid., 65).

A nivel internacional, los ciberataques de Estonia abrieron una reflexión sobre el papel de las actividades del ciberespacio dentro del marco de la Seguridad Nacional. Como consecuencia, Estonia y la OTAN desarrollaron paralelamente y conjuntamente

normativas y organismos en el campo de la ciberseguridad, como quedan explicados en el Capítulo 5.

La magnitud de la transformación inmediata (2007-2008) de las estrategias cibernéticas inmediata de Estonia y de la OTAN nos remite a la relación bilateral de cada una con la presunta autora de los ciberataques: Rusia, siendo su análisis el Estado de la Cuestión de este trabajo.

Autores como Galbreath y Lañas (2013) conectan la adhesión de Estonia a la OTAN en 2004 como punto de inflexión en las relaciones ruso-bálticas. No obstante, aunque estudian las relaciones entre Rusia y Estonia diferenciando claramente dos marcos temporales (antes y después de la adhesión), concluyen que la persistencia de algunos conflictos derivados de la independencia de Estonia son los que *“definen la naturaleza y la trayectoria de las relaciones ruso-bálticas”* incluso después su incorporación a la OTAN y la UE. ¿Quedan por tanto enmarcados los ciberataques dentro de un contexto de tensión de las relaciones entre ambos países?

En esta línea, Viktorova (2006) propone el estudio de las relaciones entre Estonia y Rusia dentro de un marco de construcción de la identidad estonia y de la percepción de Rusia como una amenaza para su soberanía también después de 2004: *“A pesar de la ampliación de la UE y la integración a la OTAN contribuyó a normalizar las relaciones bilaterales, el discurso político de Estonia sobre Rusia está todavía dominado por una lógica conflictiva”* (Ibid., 2).

Por el contrario, para autores como Herzog (2011), los puntos de tensión en el ámbito bilateral (como la cuestión de las minorías étnicas) no fueron los detonantes de los ciberataques, sino la ambición estratégica en el ámbito internacional: *“Fueron consecuencia de los intereses nacionales de Rusia de testar en Rusia las capacidades de Moscú en el ámbito de la ciberguerra así como la capacidad respuesta de la OTAN”*.

Paralelamente a estas investigaciones se desarrollan otras que exponen directamente la perpetuación de los ciberataques como una consecución de las relaciones bilaterales entre

Rusia y Estonia. Uno de los trabajos más completos al respecto es el elaborado por el teniente coronel Néstor Ganuza, jefe de Adiestramiento y Doctrina del Centro de Ciberdefensa de la OTAN, que contempla el estudio del caso estonio para hacer una radiografía de la ciberseguridad en el ámbito internacional y en la OTAN. Ganuza, en base a datos recogidos por el CERT, elabora un doble análisis: uno que define las relaciones bilaterales entre Rusia y Estonia como detonante de los ciberataques y otro que establece la naturaleza de la relación Rusia-OTAN como causa de la utilización del ciberespacio como campo de batalla y desestabilización.

3. RELACIONES BILATERALES RUSIA Y ESTONIA

El inicio de las relaciones bilaterales entre Rusia y Estonia debe enmarcarse dentro de la relaciones ruso-bálticas. De acuerdo con Galbreath y Lašas (2013), las relaciones entre ambas regiones han sufrido altibajos a lo largo de los años, pero la naturaleza de estas viene definida por dos factores. Por un lado, por una histórica falta de confianza entre las distintas partes de la región y, por otro lado, por los grandes dilemas de seguridad, entendidos según la definición de Herz (1950), como aquellas situaciones en las que las acciones de un estado para ganar seguridad aumentan la inseguridad de los otros; puesto que mientras unos entienden como defensivas sus propias actuaciones, interpretan como amenazas potenciales las de los demás.

Para estos autores, la incorporación de Estonia a la Unión Europea y a la Organización del Tratado del Atlántico Norte (OTAN) en 2004 supone un punto de inflexión en las relaciones bilaterales entre ambos países, pudiéndose estas analizar en dos períodos diferenciados: antes de la primera ampliación de la Unión Europea y después. En este capítulo proponemos el estudio de las relaciones exteriores entre ambos países atendiendo a esta división.

3.1 Relaciones bilaterales antes de la incorporación de Estonia a la UE y a la OTAN

Galbreath y Lašas (2013) estudian el origen de las relaciones bilaterales entre ambos países tomando como punto de partida la restauración de la independencia de Estonia el 20 de agosto de 1991 y la posterior culminación de la disolución de la Unión Soviética en diciembre de ese año. Otros autores, como Kauppila (1999) analizan también el desarrollo de las relaciones desde mencionado acontecimiento. Sin embargo, cabe recordar que las diferentes interpretaciones sobre la historia soviética revelan distintas versiones sobre el inicio de las relaciones bilaterales entre ambos estados.

El Gobierno estonio señala el inicio de las relaciones el 2 de febrero de 1920, cuando se firmó el Tratado de Paz de Tartu en el que la entonces República Soviética Socialista

Federativa de Rusia reconoció la independencia *de iure* de la República de Estonia. El documento que puso fin a la Guerra de Independencia Estonia (1918-1920) y en el que se delimitan las fronteras ruso-estonias “*es considerado por el país como el primer tratado internacional del estado estonio y se ve así como la partida de nacimiento de Estonia*” (Aalto, 2001 citado en Viktorova, 2006/2007). No obstante, de acuerdo con la narrativa rusa este tratado “*dejó de ser legalmente relevante cuando Estonia ingresó en la URSS en 1940*” (Mälksoo, 2005). El ex ministro de Asuntos Exteriores y del ministerio de Defensa estonio, Kalev Stoicescu, explicaba las discrepancias en su artículo *The Tartu Peace Treaty and Estonia’s Eastern Border* (2020) de la siguiente manera:

“Las relaciones bilaterales entre los dos países empezaron en febrero de 1920, pero Moscú no está de acuerdo con este factor por varios motivos, no solo por el conflicto territorial. Si se necesitan pruebas, puedo revelar que el presidente Putin ha preparado un artículo en profundidad sobre la «verdad histórica» de la Segunda Guerra Mundial y el periodo que le precede”

La primera etapa del estudio comprende el período que va de 1991 a 2004 y que, según de Galbreath y Lašas (2013), está definido por una política exterior estonia orientada a escapar de la esfera de influencia de Rusia a través del refuerzo de las relaciones con Occidente.

Cabe recordar que el 8 de diciembre de 1991 las repúblicas bálticas y Georgia rehusaron unirse a la Comunidad de Estados Independientes, lo que ya indicaba un intento de romper todo vínculo con la Federación Rusa. De acuerdo con los autores, estas primeras relaciones giran en torno a la resolución de tres cuestiones prácticas: –la retirada de tropas soviéticas en territorio estonio, la delimitación de las fronteras y la gestión de las minorías rusas (ver puntos 3.1.1, 3.1.2, 3.1.3). Así, la propuesta de los autores contempla un inicio tenso de las relaciones bilaterales.

Sin embargo, de acuerdo con Kara-Murza (2015) el primer contacto entre Rusia y Estonia a inicios de la década de los 90 estuvo marcado por la colaboración entre ambos: “*hubo un tiempo en el que los movimientos de independencia de los Estados bálticos no tuvieron*

mejor aliado que Rusia y su líder Boris Yeltsin". El autor hace referencia a la declaración conjunta que el 13 de enero de 1991 firmaron los líderes de Estonia, Lituania, Letonia y de la Federación Rusa –que todavía formaba parte de la Unión Soviética– y en la que *“las partes reconocían mutuamente su soberanía nacional”* (citado en Cucó, 1998: 204-2005).

A nivel internacional, este primer acercamiento fue uno de los más relevantes al considerarse una de las primeras declaraciones de Yeltsin en contra de la opinión del líder de la Unión Soviética, Mikail Gorbachev, que ese mismo día había ordenado una operación militar orientada a impedir la independencia de Lituania. No obstante, el tratado de cooperación (*Treaty on the Principles for the Interstate Relations*) que paralelamente firmaron la República Socialista Federativa Soviética de Rusia y la República de Estonia el 12 de enero de ese año sería determinante de cara al futuro de las relaciones ruso-estonias. En el documento, ambas partes reconocían que los ciudadanos de la Unión Soviética que estuviesen permanentemente residiendo en cualquiera de los dos territorios tenían, según el Artículo III, *“el derecho de mantener o adquirir la nacionalidad rusa o estonia según su libertad de expresión”* (Arp, 2008: 263, traducción propia). Los académicos Kirch y Kirch lo consideran o históricamente relevante por ser *“el primer acuerdo bilateral firmado entre Estonia y su vecino del este en condición de igualdad de derechos”* (citado en Dunlop: 1993-1994: 614, traducción propia).

Mientras que este pacto reafirmaba la dicotomía Rusia-Unión Soviética, para Estonia supuso una victoria política: implicaba el reconocimiento de su condición de Estado en un momento en el que la Unión Soviética se oponía. Esta dinámica culminó con el reconocimiento formal por parte de Boris Yeltsin de la independencia de la república báltica de Estonia el 24 de agosto de 1991 (Dunlop, 1993-1994).

De acuerdo con la tesis de Galbreath y Lañas (2013), a partir de ese momento las relaciones de Estonia y de Rusia comenzaron a deteriorarse por tres problemas interconectados derivados del restablecimiento de la independencia estonia. Estos son: la desmilitarización rusa de Estonia, el desconocimiento de la situación legal en la que quedaban las minorías rusas residentes en el país y, el conflicto sobre la delimitación definitiva de las fronteras.

3.1.1 Proceso de desmilitarización

En el momento en que quedó oficializada la restauración de la independencia de Estonia, la retirada de las tropas soviéticas estacionadas en suelo estonio se convirtió en una de las prioridades del país en materia de política exterior. Asimismo, lo que parecía ser una continuación de las buenas relaciones entre Rusia y Estonia acabó por convertirse en uno de los principales puntos de tensión entre ambos. Las tropas soviéticas pasaron a estar bajo potestad rusa a lo largo del primer semestre de 1992, cuando mediante decreto presidencial, Rusia, como Estado sucesor de la URSS asumió la jurisdicción de las tropas soviéticas estacionadas en el extranjero y la jurisdicción de la guardia fronteriza de los Estados bálticos (Falkenrath, 1995:174).

Las primeras negociaciones tuvieron lugar en abril de ese año y ambos Estados se posicionaron a favor de la desmilitarización de Estonia, que solicitó el apoyo de los países europeos, de Estados Unidos y de organizaciones internacionales como la Commission on Security and Cooperation in Europe (CSCE). Cabe destacar el interés de Estados Unidos en la resolución de esta cuestión, que en octubre anunció un paquete de ayudas de 24 mil millones de dólares americanos para la retirada de tropas rusas en las tres repúblicas bálticas, siempre que esta se materializase antes de julio de 1993 (Freedom Support Act, 1992).

No obstante, ese mismo mes, Yeltsin anunció la paralización de la desmilitarización en Estonia, Letonia y Lituania hasta que se modificaran las legislaciones de ciudadanía de estos países de tal manera que se garantizaran los derechos de los soldados soviéticos retirados residentes en esos países y del resto de ciudadanos rusos. En 1993 Lituania, que contaba con un menor porcentaje de antiguos ciudadanos soviéticos que en las otras dos repúblicas (González Martín, 2018), accedió a la modificación de la legislación y las tropas abandonaron el país en agosto de ese año.

En este sentido, de acuerdo con la tesis inicial, fue Rusia quien primero conectó la desmilitarización de los bálticos con la cuestión de las minorías. Para Park (1995), la interconexión política entre ambas cuestiones convirtió la retirada de tropas en “*el más*

complicado y a la vez más simple conflicto en materia de seguridad entre ambos países". Por un lado, Moscú justificaba la moratoria de su compromiso alegando que la Ley de Ciudadanía de Estonia de 1992 no garantizaba los derechos de los ciudadanos rusos que vivían en el país. De hecho, Rusia denunció a Estonia ante la Commission on Security and Cooperation in Europe por “*violar los derechos humanos de las minorías rusas*” (Helsinki Watch, 1992). Por su lado, la República de Estonia esgrimía que la presencia de soldados (y ex combatientes) soviéticos era una amenaza *per se* para la seguridad nacional y que debía ser resuelta de manera independiente.

Se calcula que en 1990 había entre 50.000 y 60.000 militares soviéticos en territorio Estonio. No obstante, con el proceso de desintegración de la URSS, el número de efectivos fue disminuyendo hasta alcanzar los 23.000 - 25. 000 efectivos. También durante el período de negociación la cifra fue disminuyendo progresivamente hasta los 2.500 efectivos en agosto de 1994. Park (1995) resume la evolución de las tropas rusas en las Repúblicas bálticas en función de diversas estimaciones rusas y bálticas en el siguiente cuadro:

Tabla 3: Estimación de militares rusos en las Repúblicas bálticas 1992-1993

<i>Año</i>	<i>Estonia</i>	<i>Letonia</i>	<i>Lituania</i>
1992	23 - 25.000 (<i>Febrero</i>)	50.000 (<i>Primavera</i>)	34 -43.000 (<i>Invierno</i>) 38. 000 (<i>Primavera</i>) 34. 000 (<i>Verano</i>) 20. 500 (<i>Septiembre</i>)
	10.000 (<i>Enero</i>) 7.000 (<i>Abril</i>)	23.000 (<i>Abril</i>)	10.000 (<i>Enero</i>)
1993	6.500 (<i>Mayo</i>) 3.800 (<i>Octubre</i>) 2.600-3.000 (<i>Diciembre</i>)	13.000 (<i>Diciembre</i>)	9.000 (<i>Junio</i>) 0 (<i>31 Agosto</i>)

Fuente: Park, 1995. Basado en estimaciones de “The Baltic Independent, 24 December 1993-6 January 1994, p. 6; Hommikuleht, 12 January 1994, p. 7; RFE/RL Research Report, 2, 25, 18 June 1993, pp. 50-56; 3, 1, 7 January 1994, pp. 92-102”. Traducción propia.

El 26 de julio de 1994 los presidentes de Estonia, Lennart Meri, y de Rusia, Borís Yeltsin, firmaron un tratado sobre la retirada de las tropas rusas de Estonia en agosto de ese año. Paralelamente, se firmó otro acuerdo en el que se garantizaba a todos los militares rusos jubilados el acceso a los mismos derechos que a los ciudadanos estonios sin una criba en función de la edad de nacimiento o la edad de jubilación (inicialmente se excluían aquellos nacidos después de 1930). No obstante, Rusia concedió al Gobierno estonio el derecho de retirar la solicitud de residencia a aquellos militares que fuesen considerados “*un riesgo para la seguridad nacional*” (Starr y Dawisha, 2016) y de estudiar de manera individual cada solicitud.

Según Galbreath (2005), la concesión de Rusia ante esta cuestión responde más a su inestabilidad nacional (el país estaba inmerso en la construcción de una nueva Constitución) que a un intento de mejorar las relaciones con Estonia. De acuerdo con el autor, “*la naturaleza contenciosa de la resolución de la retirada de tropas sentaría los precedentes de las relaciones báltico-rusas en la próxima década*”. Primero, por el surgimiento de la cuestión de las minorías en el panorama internacional y, segundo, por el establecido interés de Rusia por influir en las políticas sobre las minorías en los Estados bálticos.

3.1.2 Contencioso fronterizo

En el Tratado de Tartu de 1920, Tallin y Rusia no firmaron únicamente la paz, sino que fijaron la delimitación de las fronteras terrestres. De acuerdo con el pacto, el total de la superficie del condado de Narva y de la ciudad de Pechory y el territorio circundante –condado de Setomaa, que pasó a ser el condado de Petsori o Peipsi–, quedaron bajo la soberanía de Estonia. Sin embargo, con la anexión de las Repúblicas Bálticas a la Unión Soviética en 1940, la frontera ruso-estonia se convirtió en la línea de separación entre dos unidades administrativas, conocida también como línea de control, de la potencia soviética.

Tras la Segunda Guerra Mundial, la URSS ajustó unilateralmente las fronteras, de tal manera que cerca del 75% del área de Petsori pasó a formar parte de la zona (óblast) de Pskov, mientras que se estableció una partición en la región de Narva, de manera que esta

ciudad quedó en la zona de la república soviética de Estonia, mientras la ciudad de Ivangorod y los municipios circundantes pasaron a formar parte del óblast de la Federación Rusa de Leningrado. En total, se calcula que cerca del 5% del territorio estonio previo a la I Guerra Mundial fue incorporado a la Federación Rusa (Maalksoo 2005). Según datos del Gobierno estonio, esto supone la pérdida de 2.334 kilómetros cuadrados (véase Figura 1).

Tras la independencia de Estonia, la recuperación de estos territorios ha sido una de las cuestiones claves de la política exterior de la república y un elemento de tensión en las relaciones bilaterales. En 1991, el presidente del Consejo Supremo de la República de Estonia, Arnold Ruutel y el presidente Ruso, Boris Yeltsin, acordaron abordar esta cuestión. Sin embargo, las diferentes interpretaciones sobre el fin de la Segunda Guerra Mundial y el desarrollo de la etapa soviética han dilatado las conversaciones. De acuerdo con la narrativa rusa, el fin de la Segunda Guerra Mundial es motivo de orgullo nacional, puesto que la potencia se percibe a sí misma como víctimas principales y liberadores de los Nazis: *“esta página de la historia supone la base de la identidad postsoviética rusa”* (Ibid.). Para los estonios, en cambio, este período es recordado por la ocupación soviética y la anexión ilegal a la URSS. Brüggemann and Kasekamp (2009: 51) lo definen de la siguiente manera: *“lo que los rusos perciben como una liberación, los estonios lo ven como una ocupación”*.

Figura 2: Fronteras definidas en el Tratado de Tartu vs línea de control



Las fronteras estonias definidas en el Tratado de Paz de Tartu en 1920 vienen marcadas con la línea verde gruesa mientras que la actual *línea de control* entre Rusia y Estonia está definida por la línea verde fina. Fuente: <https://official-estonia.tumblr.com/post/156712477414/estonian-borders-as-defined-by-tartu-peace-treaty>

Bajo esta interpretación, Estonia defiende que la independencia proclamada en 1991 es en realidad la restauración *de facto* de la independencia reconocida en 1920 en el Tratado de Tartu, por lo que se entiende como una vuelta al status quo, incluyendo las fronteras definidas a inicios de siglo. Por su parte, Rusia entiende la independencia de Estonia como consecuencia del colapso de la Unión Soviética. Según Galbreath (2005:205), esto significa que según la narrativa rusa, “*los Estados Bálticos, ‘decidieron’ ser independientes, de la misma manera que ‘decidieron’ convertirse en Repúblicas Soviéticas. En este sentido, de la misma manera que Rusia no intentar recuperar las fronteras del Imperio, los Estados Bálticos deben trabajar dentro de las fronteras soviéticas*” (traducción propia).

Para Viktorova (2006), las tensiones provocadas por esta cuestión trascienden el interés territorial y deben ser consideradas como un conflicto de identidades. El autor sostiene que para Estonia, la restauración de las fronteras según el Tratado de Tartu (que es considerado ‘la partida de nacimiento del país’) supone el reconocimiento de la continuidad política del

Estado de entreguerras y de la *“injusticia histórica que sufrió en manos de la Unión Soviética”*. Cabe por tanto destacar que desde el principio, Estonia insistió en destacar la continuidad de su estado, a pesar de haber estado durante 50 años bajo dominio soviético, como eje central de su configuración nacional. Por su parte, Rusia considera que la representación que hace Estonia sobre la Unión Soviética es indiscriminada y que la desconfianza del país báltico hacia la política exterior actual de Rusia resulta ofensiva a varios niveles, ya que considera que *“Estonia ganó (infraestructura y desarrollo industrial) formando parte de la URSS”*. En este sentido, Viktorova arguye que la percepción del otro como un obstáculo para la propia construcción de identidad nacional presenta el consenso como algo inalcanzable y sitúa las negociaciones bilaterales a un punto muerto. Lo define de la siguiente manera: *“En múltiples ocasiones, Estonia y Rusia han articulado percepciones del otro como una amenaza fundamental para la percepción de la propia identidad. En particular Estonia ha construido su identidad nacional como una amenaza a las políticas presentes y pasadas de Rusia Estonia in particular often constructed its statehood and identity as endangered by Russia’s past and present policies”*.

Si bien es cierto que los reclamos territoriales de Estonia comenzaron tras la restauración de la independencia, durante la primera mitad de la década de los 90 Rusia rechazó abordar esta cuestión sin resolver previamente otros problemas políticos como el de las minorías. Estonia prefirió abordar en primera instancia el abandono de las tropas rusas. A pesar de ello, ambas potencias se posicionaron al respecto. En junio de 1992, se aprobó la Constitución estonia, cuyo Artículo 122 constataba que *“la frontera terrestre de Estonia queda determinada por el Tratado de Paz de Tarty del 2 de febrero de 1920 y por acuerdos internacionales”* (traducción propia). De esta manera, el reconocimiento de la validez del tratado se convertía en un requerimiento constitucional (Malksoo, 2005). En junio de 1994, un mes antes de acordarse la retirada de tropas, Boris Yeltsin ordenó unilateralmente la demarcación de Rusia en base a las fronteras internas de la URSS.

A partir de 1995 la política exterior de Estonia adoptó una actitud conciliadora debido, según reconoce el propio Gobierno Estonio en la web de su ministerio de Asuntos Exteriores, a que la falta de un acuerdo fronterizo bilateral dificultaba la tramitación del proceso de anexión de Estonia a la OTAN y a la Unión Europea. Esto dio lugar a la

‘Iniciativa Tarand’ (en alusión al primer ministro estonio de entonces, Andres Tarand) que consistía en separar la cuestión fronteriza de la petición de reconocimiento político de la vigencia del Tratado de Tartu como un documento básico de continuidad del Estado de Estonia. Esto fue resultado de un estudio sobre el derecho internacional, que concluía que un acuerdo sobre unas nuevas fronteras que no hiciese referencia al Tratado de Tartu no invalidaba su vigencia desde el punto de vista legal (Ibíd.).

El Gobierno de Estonia aprobó ese año una suerte de tratado fronterizo ‘técnico’ que recogía aspectos prácticos sobre la línea de demarcación sin incluir ningún tipo de preámbulo político ni mención al acuerdo de 1920. La naturaleza del nuevo acuerdo permitió el desarrollo de las negociaciones entre ambos países de tal manera que en 1998 este estaba listo para firmarse. No obstante, Rusia aplazó las negociaciones en vistas a retrasar la adhesión de Estonia a la Unión Europea y la OTAN, solicitada en 1995. La falta de un acuerdo fronterizo no impidió que Estonia entrase a formar parte de ambas instituciones 2004. Lejos de relajar las tensiones, estas se acentuaron a partir de la segunda mitad de la nueva década.

En este sentido, de acuerdo con la tesis de Viktorova, la renuncia parcial al reconocimiento del Tratado de Paz de Tartu por parte de Estonia, en vistas a orientar su política exterior hacia Occidente y las trabas impuestas por Rusia de cara a dificultar la anexión a la OTAN y la UE, responden, no sólo a criterios estratégicos, sino también identitarios, quedando reflejada la prevalencia de un conflicto de identidad motivado por las diferentes interpretaciones históricas. Estonia pretende construir la propia identidad a través de la oposición a su vecino del este.

3.1.3. Minorías étnicas

La cuestión de las minorías étnicas ha estado en el centro de las relaciones bilaterales entre ambos países desde el inicio de las mismas. Para entender la naturaleza del conflicto cabe destacar la evolución de la estructura étnica de la población de Estonia y las políticas sobre las minorías aplicadas tras 1991.

- Evolución y distribución de la diversidad étnica de la población

La evolución de la estructura étnica en Estonia durante el siglo XX ha constituido un factor esencial que ha condicionado la construcción de la identidad nacional del nuevo Estado tras la recuperación de la independencia. De acuerdo con la Agencia Estatal de Estadística Estonia (*Statistics Estonia*), a inicios del siglo cerca del 92% de la población era de origen estonio (sin contar las regiones de Petseri y las del este del río Narva que actualmente pertenecen a Rusia).

Si bien durante el período entreguerras se registró un aumento de la emigración de los países vecinos, durante la Segunda Guerra Mundial desaparecieron la mayoría de las minorías étnicas del país de tal manera que al finalizar la guerra, cerca del 97% de la población era de origen estonio. Como se puede observar en la Tabla 4, tras la anexión soviética hubo un aumento de la emigración de ciudadanos soviéticos, la mayoría procedentes de Rusia, pero también de Ucrania y Bielorrusia.

Tabla 4: Evolución de la estructura étnica de Estonia 1922-59

<i>Grupo étnico</i>	<i>1922</i>		<i>1934</i>		<i>1959</i>	
	<i>N</i>	<i>%</i>	<i>N</i>	<i>%</i>	<i>N</i>	<i>%</i>
<i>Estonios</i>	955.100	91,7	977.600	92	892.700	74,6
<i>Rusos</i>	45.900	4,4	46,600	4,4	2240.200	20,1
<i>Alemanes</i>	18.200	1,7	16.200	1,5	700	0,1
<i>Suecos</i>	–	–	7.600	0,7	–	–
<i>Fineses</i>	–	–	1.900	0,1	16.700	1,4
<i>Ucranianos</i>	–	–	–	–	15.800	1,3
<i>Bielorrusos</i>	–	–	–	–	10,900	0,9
<i>Judíos</i>	–	–	4.400	0,4	5.400	0,5
<i>Letones</i>	–	–	4.000	0,4	2.900	0,2
<i>Polacos</i>	–	–	1.500	0,1	2.300	0,2

<i>Otros</i>	24,600	2,2	2,900	0,3	12,403	0,7
<i>TOTAL</i>	1.043.800		1.117.400			1.196.800

Fuente: Kazmina (1991)

Durante el período 1947-1989 se registró un incremento sustancial de la inmigración como consecuencia del proceso de rusificación de la Unión Soviética. Según se recoge en Statistics Estonia, “*la mayoría eran obreros, ingenieros de nivel medio y personal militar*”. En 1989 los estonios representaban cerca del 61,5% de la población, mientras que los rusos étnicos representan el 30,3%, seguidos de los ucranianos (3,1%), los bielorrusos (1,8) y los fineses (1,0%). En términos absolutos, durante este periodo la población de Estonia aumentó 1,2 puntos porcentuales anualmente pero lo hizo de manera desigual según la etnia: mientras la población rusa aumentaba, la estonia disminuía. Según señalan Ebenhardt y Owsinski (2015) en su libro *Ethnic Groups and Population Changes in Twentieth Century Eastern Europe*, el fin de la dominación soviética salvó a la comunidad estonia de una catástrofe demográfica, puesto que la permanencia bajo control soviética podría haber convertido a los estonios “*en minoría dentro de su propio país*”. Como se puede observar en la Tabla 5, tras la independencia hubo un repunte de la población de origen estonio. Sin embargo, la estructura étnica del país ha tendido a estabilizarse de manera que durante la década de los 90, los principales grupos étnicos eran los estonios, los rusos y los ucranianos.

Tabla 5: Estructura de la población por nacionalidad, 1989- 2000

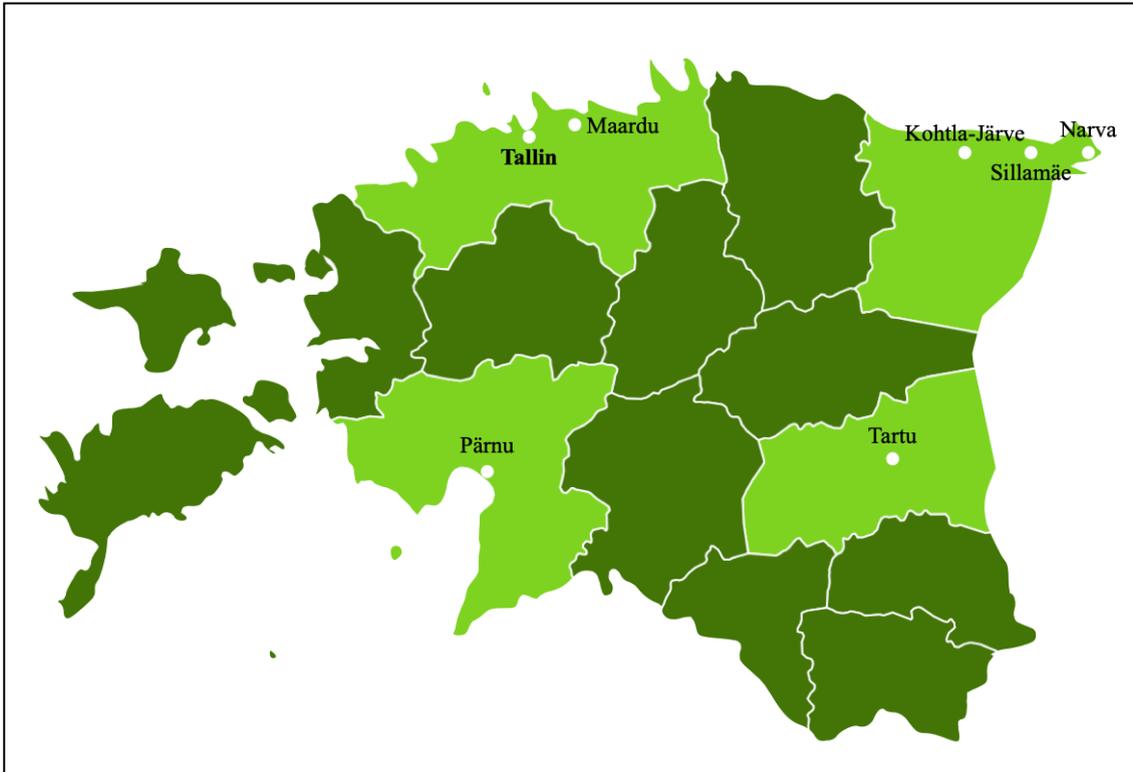
<i>Nacionalidad</i>	<i>1989</i>		<i>2000</i>	
	<i>número</i>	<i>%</i>	<i>número</i>	<i>%</i>
<i>Total</i>	1 565 662	100.0	1 370 052	100.0
<i>Estonios</i>	963 281	61.5	930 219	67.9
<i>Rusos</i>	474 834	30.3	351 178	25.6
<i>Ucranianos</i>	48 271	3.1	29 012	2.1
<i>Bielorrusos</i>	27 711	1.8	17 241	1.3
<i>Fineses</i>	16 622	1.1	11 837	0.9
<i>Tártaros</i>	4 058	0.2	2 582	0.2
<i>Letones</i>	3 135	0.2	2 330	0.2
<i>Polacos</i>	3 008	0.2	2 193	0.2
<i>Judíos</i>	4 613	0.3	2 145	0.1
<i>Lituanos</i>	2 568	0.2	2 116	0.1
<i>Alemanes</i>	3 466	0.2	1 870	0.1
<i>Otras</i>	14 088	0.9	9 410	0.7
<i>Desconocido</i>	7	0.0	7 919	0.6

Censo Estonio, 2000

El aumento del flujo migratorio de los étnicos rusos durante la segunda mitad del siglo XX fue resultado del proceso de rusificación de la Unión Soviética, por lo que no se dio ningún proceso de asimilación cultural de los rusos a la cultura estonia. El fenómeno de integración se dio a la inversa: “*el idioma ruso llegó a usurpar el estatus social que previamente había pertenecido a Estonia*” (Ibíd.). No obstante, la incorporación del lenguaje ruso a la vida política y social en Estonia no fue homogénea, sino que fue especialmente pronunciada en las zonas urbanas, sobre todo en Tallin donde se concentra casi la mitad de la población rusa de Estonia (43%) y en las principales ciudades del distrito de Ida Virumaa, al noreste del país, donde solo en Narva, Sillamäe, Khotla-Jarve se

concentra el 32% de la población rusa. De hecho, en esta última región, situada en la frontera con Rusia, la población estonia fue reduciéndose considerablemente de 1934 a 2000 hasta alcanzar los 9,4 puntos porcentuales a inicios del siglo XXI (véase tabla 6).

Figura 3: Mapa de las principales zonas urbanas de Estonia (Tallin, Maardu, Pärnu, Narva, Sillamäe, Kohtla-Järve)



Fuente: elaboración propia

Tabla 6: Cambios de la población estonia en Tallin, Narva, Sillamäe, Khotla-Jarve según los censos 1934-2000

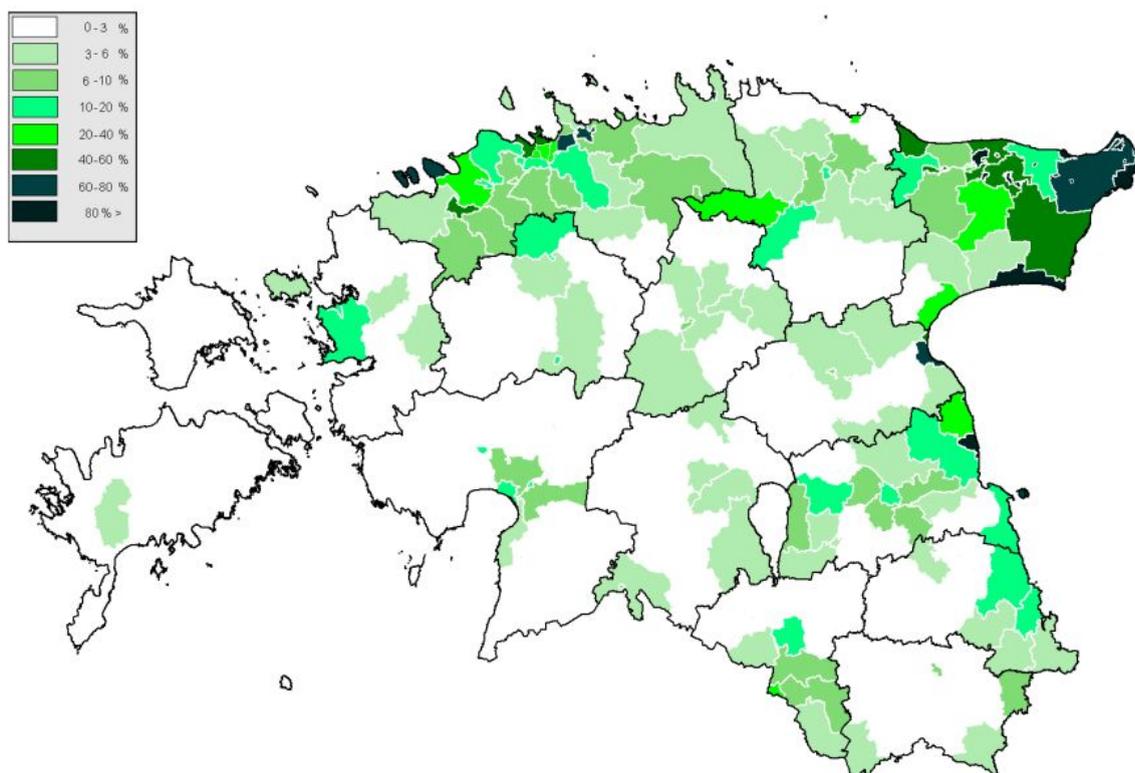
<i>Año</i>	<i>Población origen estonio (%)</i>	
	<i>Tallin</i>	<i>Narva, Kohtla- Järve, Sillamäe</i>
1934	85,8	64,8
1959	60,2	27,6
1970	55,7	21
1979	51,9	16,7
1989	47,4	12,9
2000	53,7	9,4

Fuente: Statistics Estonia

La población de habla estonia y de habla rusa coinciden con la distribución étnica. En base al censo de 2000, 67,3% de la población afirmó tener el estonio como lengua materna, mientras que el 29,7% dijo tener la rusa. El resto de idiomas hablados en el país no suponen en ningún caso ni un 1%, por lo que su representación es muy baja. La mayor parte de los rusoparlantes se concentra en las regiones norestes previamente mencionadas (véase figura 3).

Tal y como se recoge en la Tabla 7, en Narva se calcula que solo el 4,9% de la población es de origen estonio mientras que cerca del 94% es de origen ruso y un 93% del total de la población de la ciudad habla ruso. En Kohtla-Järve, que cuenta con una representación de cerca del 82% de la población rusa, solo el 15% tiene el estonio como lengua materna. En la ciudad de Sillamäe la situación es similar: con solo un 4,2% de representación de población estonia étnica, solo cerca del 2% de la población habla estonio. En términos generales, se estima que en 1989 prácticamente todos los habitantes de estonia sabían hablar ruso, mientras solo el 67,4% de la población sabía hablar estonio.

Figura 4: Distribución de la población de lengua rusa en Estonia, censo 2000



Fuente: Ministerio de Cultura de Estonia, 2015.

Tabla 7: Población según su origen étnico y su lengua materna, censo 2000

<i>Ciudad</i>	<i>% origen estonio</i>	<i>% aproximado origen ruso</i>	<i>Hablantes nativos estonia %</i>	<i>Hablantes nativos de ruso %</i>
<i>Tallin</i>	53,7	46	52	43
<i>Narva</i>	4,9	94	3	93
<i>Kohtla-Järve</i>	17,8	82	2	80
<i>Sillamäe</i>	4,2	96	2	94
<i>Maardu</i>	19,9	80	18	75

Fuente: *Oficina de Estadística de Estonia, 2000 population and Housing Census; Citizenship, Nationality, Mother Tongue and Command of Foreign Languages, Tallin 2001. Tablas 12, 15 y 17.*

- Restauración de la ley de Ciudadanía y las políticas idiomáticas

Con todo, los datos reflejan cómo el proceso de rusificación, que duró casi 50 años, provocó una gran transformación demográfica y lingüística de la república báltica. En su análisis para el 100 aniversario de las repúblicas bálticas, González Martín (2018) expone que las leyes de ciudadanía y de nacionalidad de Estonia deben ser comprendidas en base a la memoria histórica de Estonia marcada por la ocupación soviética: *“estas se fundamentan en el mismo principio de continuidad del Estado y por lo tanto en la impuesta transitoriedad de su inserción en el imperio comunista soviético”*. En este sentido, la construcción de la identidad cultural de Estonia tras la recuperación de la independencia se fundamentó en base a la recuperación de los símbolos y tradiciones nacionales previos a la ocupación soviética.

La restauración de las políticas de ciudadanía fue una de las primeras medidas tomadas por el Gobierno estonio y uno de los principales puntos de tensión entre Estonia y Rusia. De acuerdo con Park (1994), de agosto de 1991 a septiembre de 1992 (cuando se celebraron las elecciones parlamentarias de Estonia), las políticas de ciudadanía fueron muy severas con las minorías. El autor refiere a febrero de 1992, cuando se recuperó la Ley de Ciudadanía vigente en 1938 basada en la relación de consanguinidad (*ius sanguinis*). Esto significa que, de acuerdo con la legislación, únicamente las personas que poseían nacionalidad Estonia antes del 16 de junio de 1940 –inicio de la ocupación soviética– y sus descendientes obtenían automáticamente la nacionalidad Estonia. Se estima que cerca de 80.000 ciudadanos no estonios consiguieron la ciudadanía. El resto de personas podía acceder a la ciudadanía a través de un proceso de naturalización siempre y cuando cumplieren los siguientes requisitos para solicitar la ciudadanía:

- Haber residido en el país al menos dos años (a partir de 1992)
- Jurar lealtad a la República de Estonia y a su constitución
- Demostrar conocimiento de la lengua Estonia a través de un examen.

Los requisitos lingüísticos quedaron estipulados en una ley separada aprobada por el parlamento estonio (Riigikogu) en 1989 y entrada en vigor el 10 de febrero de 1993 que

exige superar unas pruebas para acreditar el conocimiento suficiente del idioma. Aunque la legislación no responde a criterios étnicos, los requisitos para la solicitar la ciudadanía y, concretamente las exigencias lingüísticas han supuesto una línea de fractura social importante. De acuerdo con Park (1994), incluso con la modificación de la Ley de Ciudadanía de 1995 –con la que se relajaron algunas medidas– los requisitos lingüísticos pueden ser entendidos en términos étnicos: de acuerdo con el censo de 1989, solo el 15% de los rusos étnicos era capaz de hablar estonio, por lo que muchos no pudieron votar en las elecciones parlamentarias de 1992. Además, la modificación de la ley establecía que no era necesario que los ciudadanos de etnia estonia realizaran las pruebas lingüísticas.

Puesto que la ley concreta que un ciudadano estonio no puede tener simultáneamente la ciudadanía de otro estado, de manera alternativa, aquellos que no soliciten la ciudadanía por naturalización cuentan con tres opciones: convertirse en ciudadanos de otros países, abandonar el país o permanecer como “individuos con ciudadanía indefinida” (Ibíd.). Este último grupo de habitantes es identificado por el estado como los no ciudadanos, que aunque se les reconocen los mismo derechos sociales que al resto de residentes no cuentan con ciertos derechos políticos: pueden votar en las elecciones a las administraciones locales pero no en los comicios nacionales y no pueden acceder a puestos de trabajo en la administración ni a las fuerzas armadas (González Martín, 2018). Son personas apátridas, de nacionalidad indeterminada que poseen el conocido como pasaporte gris. Este limita la libertad de movimientos: aunque pueden viajar por los países del Espacio Schengen, en algunos únicamente pueden estar un período determinado de tiempo y necesitan un visado para viajar a Rusia (Riigikogu, 1999).

Los últimos datos referentes a la posesión de nacionalidad vienen representados en la Tabla 8 y pertenecen al censo del 2000, año en el que un 12,4% (170.349 personas) de la población de Estonia formaba parte de este grupo de nacionalidad indefinida, en su mayoría concentrada en las principales ciudades de Kohtla-Järve, Narva y Tallin donde, como se ha observado anteriormente, había una mayor concentración de rusos étnicos. De acuerdo con el censo, un 38% de los rusos tenían el pasaporte gris, frente al 40% que poseía la ciudadanía estonia y el 20,9% que poseía la rusa (véase Tabla 9).

Tabla 8: Población por lugar de residencia y ciudadanía, 2000 (porcentajes)

	<i>Ciudadanos estonios</i>	<i>Ciudadanos rusos</i>	<i>Ciudadanos de otros países</i>	<i>Personas con ciudadanía indefinida</i>	<i>Ciudadanía desconocida</i>
<i>Total</i>	80.0	6.3	0.7	12.4	0.6
<i>Población de ciudades</i>	72,6	8.9	0.8	16.9	0.8
<i>Tartu</i>	91.0	3.5	0.6	4.4	0.5
<i>Pärnu</i>	90.1	4.7	0.5	4.1	0.6
<i>Tallin</i>	71.1	8.7	1.2	18.0	1.0
<i>Kohtla-Järve</i>	41.8	13.4	0.6	42.7	1.5
<i>Narva</i>	36.4	28.9	0.4	33.6	0.7

Fuente: Censo estonio, 2000. Statistics Estonia

Tabla 9: Población por ciudadanía y nacionalidad, 2000

	<i>Ciudadanos estonios</i>	<i>Ciudadanos rusos</i>	<i>Ciudadanos de otros países</i>	<i>Personas con ciudadanía indefinida</i>	<i>Ciudadanía desconocida</i>
<i>Total</i>	1 095 743	86 067	8 941	170 349	8 952
<i>Estonios</i>	922 204	692	165	4 896	2 2262
<i>Rusos</i>	141 907	73 379	1 048	133 346	1 498
<i>Otros</i>	29 774	11 581	7 560	31 554	267
<i>Desconocidos</i>	1 858	415	168	553	4 925
<i>Porcentajes</i>					
<i>Estonios</i>	84.2	0.8	1.8	2.9	25.3
<i>Rusos</i>	12.9	85.3	11.7	78.3	16.7
<i>Otros</i>	2.7	13.4	84.6	18.5	3.0
<i>Desconocidos</i>	0.2	0.5	1.9	0.3	55.0

Fuente: Censo estonio, 2000. Statistics Estonia

De acuerdo con autores como Park, desde un punto de vista formal, no puede considerarse que la política de ciudadanía de Estonia se elaborase en base a criterios étnicos discriminatorios. Sin embargo, los requisitos lingüísticos exigidos para obtener la ciudadanía estonia atendiendo a los datos poblacionales sobre los ciudadanos de etnia rusa y su dominio de la lengua estonia abren la puerta a una interpretación basada en términos étnicos. Además, el alto porcentaje de rusos étnicos con pasaporte gris refleja la no integración total de la minoría rusa en Estonia. En este sentido, cabe destacar que la única ley existente en defensa de los derechos de las minorías es la Ley de Autonomía Cultural de las Minorías Nacionales (1993), en la que se define como minoría nacional a aquellos *“ciudadanos estonios que residan en el territorio de Estonia, tengan un vínculo con Estonia, difieran con los estonianos en su pertenencia étnica, características culturales, religión y lenguaje...”* (Artículo I). Esto significa que, debido al criterio de ciudadanía, la mayoría de los étnicamente no-estonios están oficialmente excluidos de la definición, aunque puedan participar en algunas actividades culturales (Poleshchuk, 2006).

De acuerdo con esta visión, analistas como Francisco J. Ruiz González (2010) asocian las estrictas medidas de asimilación e integración de la principal minoría del país al intento por parte de Estonia de retrotraer el proceso de rusificación que siguió a la Segunda Guerra Mundial y que diluyó la identidad cultural de Estonia. También Galbreth y Lasas proponen esta relación en su tesis:

“Cerca de un millón de migrantes soviéticos (trabajadores y soldados) fueron utilizados como un método de control político durante la época soviética. No es por tanto de extrañar que esas minorías no fuesen (y no sean) prima facie consideradas de fiar hasta que demuestren lo contrario. En el mismo sentido, es normal que las comunidades que nacieron en las repúblicas bálticas considerasen inaceptable esta desconfianza” (2013:209, traducción propia).

Según los autores, como consecuencia de estas diferencias, el problema de las minorías se convirtió en el epicentro de las relaciones entre Estonia y Rusia. De hecho, desde la independencia de las Repúblicas Bálticas la Federación Rusa anunció su intención de velar por las minorías rusófonas de las ex repúblicas soviéticas. En 1993, cuando el parlamento

estonio aprobó un proyecto ley sobre el estatuto de los extranjeros que contemplaba la posibilidad de extraditar a aquellos sin ciudadanía, Boris Yeltsin se expresó en los siguientes términos: *“Es como si los líderes estonios hubiesen olvidado algunas realidades geopolíticas y demográficas. El papel de rusia es recordárselas”* (citado en González, 2000).

En el ámbito bilateral Rusia ligó el resto de sus políticas en materia de asuntos exteriores a la cuestión de las minorías: primero postergando la retirada de las tropas y desmantelamiento militar y luego con la demarcación de las fronteras. A nivel internacional, empleó herramientas diplomáticas para atraer la atención de Occidente sobre la cuestión de las minorías. En 1992, el Soviet Supremo aprobó una resolución en la que se acusaba a Estonia de violar los derechos humanos y el tratado de cooperación de 1991. Una acusación que repitió ante Naciones Unidas, el Consejo de Europa (CdE) y la Organización para la Seguridad y la Cooperación en Europa (OSCE) como herramienta de presión.

En general, las principales organizaciones y gobiernos occidentales se mostraron neutrales o favorables a las normativas estonias. En 1993, un informe de la OSCE determinaba las políticas de ciudadanía estonia *“acordes a la normativa internacional”*. Sin embargo, otras entidades internacionales ejercieron presión en dirección contraria: entre 1992 y 1993 las organizaciones de derechos humanos Freedom House y Helsinki Watch publicaron informes desfavorables a las políticas estonias (Park, 1994). Este mix de presiones internacionales llevaron a una dulcificación de las políticas de ciudadanía por parte de Estonia en 1994 y a una rebaja de las exigencias del Kremlin. Sin embargo, la legislación mantuvo su naturaleza restrictiva. En este sentido, la presencia de los ciudadanos rusos y el fuerte interés de Rusia por velar por sus intereses durante la segunda mitad de la década de los 90 incrementó en Estonia la sensación de inseguridad nacional y, a su vez, provocó que Estonia mantuviese férrea su posición sobre la cuestión de las minorías (Galbreath y Lasas, 2013).

3.2 Relaciones bilaterales tras la adhesión de Estonia a la UE y la OTAN

La retirada de las tropas de suelo estonio fue la única cuestión a nivel bilateral resuelta antes de la adhesión de Estonia a la Unión Europea y la Organización del Tratado del Atlántico.

En relación al contencioso fronterizo, Estonia entró a formar parte de ambas instituciones con un acuerdo fronterizo preparado en 1999 pero sin firmar, ya que Rusia postergó la validación como método de presión para mejorar la situación de las minorías. En 2005 ambos países firmaron el acuerdo pero Rusia se negó a ratificarlo después de que Estonia añadiese en el preámbulo una mención al Tratado de Tartu de 1920. En este sentido, la falta de fronteras definitivas supone para la Unión Europea un problema jurídico internacional (González, 2000). Sobre la cuestión de las minorías, Rusia siguió presionando a nivel internacional para la regulación de la situación de los rusos étnicos fuera de sus fronteras. Sin embargo, no se registró ningún enfrentamiento directo efectivo más allá de las acusaciones verbales entre dirigentes de ambos países durante la primera mitad de la década de los 2000.

De acuerdo con Galbreath y Lasas (2013), con el doble ingreso Estonia cumplió con sus principales objetivos de política exterior tras la independencia. Principalmente porque la UE se presentaba la puerta a un futuro social y económico más próspero, mientras que la OTAN era considerada por las élites bálticas como herramienta esencial para garantizar su seguridad frente a Rusia (Mamedov, 2004). En este sentido, Viktorova (2006) define el acceso de Estonia a la UE y la OTAN como una reafirmación de la identidad Occidental/Europea de Estonia, así como una garantía para su seguridad y soberanía ante la amenaza de Rusia.

Cabía considerar que en este escenario las relaciones de Estonia con la Federación rusa tenderían a normalizarse. Además, porque Estonia y las otras dos repúblicas bálticas utilizaron su ubicación geopolítica como herramienta de negociación con la UE y la OTAN y Rusia. Sin embargo, lejos de atenuarse, el nuevo ámbito de tensión en las

relaciones ruso-estonias viene influido, aunque no determinado, por el proceso de ampliación de la OTAN hacia la región báltica.

De acuerdo con la doctrina militar rusa de 1993, las antiguas repúblicas soviéticas quedan definidas como el “extranjero próximo”, una nueva zona de influencia post soviética donde Rusia contempla el uso de la fuerza militar para defender los derechos de las minorías. En esta línea, en su ensayo *Historia Mínima de Rusia*, Matos Franco (2017) describe la percepción de Rusia sobre la ampliación en los siguientes términos:

“Rusia no solo colindaba ya con una OTAN que había garantizado a Moscú en 1990 que no habría ninguna ampliación hacia el este, sino que perdió influencia en países que fueron parte de la URSS y donde habita un enorme porcentaje de ciudadanos rusos”.

En este aspecto, las relaciones bilaterales tras el doble ingreso de Estonia pueden incluirse dentro del marco de relación OTAN-Rusia. Por un lado, Estonia considera a Rusia su principal amenaza por su interés de influir sobre todo en las zonas de mayoría rusa, ubicadas geográficamente en las fronteras, mientras que Rusia ve a Estonia como una amenaza a su seguridad nacional en cuanto a su membresía a la OTAN.

Aunque a través del programa *Peace for Partnership* la Alianza preparó a la región del báltico para su incorporación, desde el final de la Guerra Fría, también ha reforzado la cooperación con Rusia para demostrarle, sin éxito, que no representa una amenaza para su Seguridad Nacional a través de tres mecanismos:

- El Acta Fundacional de Relaciones Mutuas, aunque no vinculante jurídicamente
- Cooperación y seguridad entre Rusia y OTAN (1997)
- Consejo Permanente Rusia-OTAN

En el marco europeo, en 2005 Rusia, los países bálticos y otros estados miembros iniciaron una serie de negociaciones para tratar diversas cuestiones de las relaciones ruso-bálticas dentro del contexto europeo. El objetivo era facilitar el diálogo, aliviar tensiones y “permitir que los países bálticos se beneficiasen de la cooperación dentro del marco de las

relaciones EU-Rusia” (Buhbe, 2007:3). Este objetivo cobró especial relevancia en base al interés de Rusia y de la Unión Europea de renovar el marco regulatorio de cooperación Partnership and Cooperation Agreement (PCA) que vencía en diciembre de 2007.

Sin embargo, el diálogo entre Rusia-UE no puede ser contemplado desde una dimensión únicamente comunitaria, sino que los acercamientos que ambos consiguieron ese año y que quedaron plasmados en una hoja de ruta para incrementar su cooperación en los Cuatro Espacios Comunes definidos en la Cumbre de San Petersburgo de 2003 – Económico; de Libertad, Seguridad y Justicia; de Seguridad Exterior; de Investigación y Educación, y Aspectos Culturales– se vieron influenciados por las relaciones báltico-rusas (De la Cámara, 2008). Tanto es así que uno de los puntos esenciales de la iniciativa europea, la cooperación en seguridad y fronteriza en la que se incluían las peticiones de Rusia de obtener el visado de viaje para sus ciudadanos, quedó estancada tras la no ratificación de las fronteras con Estonia por parte de Rusia ese mismo año.

Las relaciones ruso-bálticas tocaron fondo en abril de 2007, “a medida que el legado del pasado soviético se intensificó dentro de las relaciones europeas contemporáneas” (Ibíd.,3). El estallido de la conocida como “crisis del soldado de bronce”, que se desarrollará a continuación, tensó a su vez la relación entre Rusia y la Unión Europea.

4. RELACIONES RUSIA-OTAN

En este capítulo se analizarán las relaciones Rusia-OTAN en un marco temporal definido desde la disolución de la Unión Soviética hasta 2007, fecha de los ciberataques. No obstante es preciso recordar que la Alianza Atlántica fue creada mediante el Tratado de Washington de 1949 para hacer frente a la posibilidad de un ataque soviético y proveer seguridad colectiva a sus países miembros. Sin embargo, tras la caída del Muro de Berlín y la caída de la URSS, la OTAN no fue disuelta: se mantuvo adaptándose al nuevo entorno estratégico. En este contexto, y derivado también de proclamación de Rusia como heredera de la URSS, Javier Morales Hernández (2010) sostiene que tanto Rusia como la OTAN tuvieron que redefinir sus identidades y su papel en el tablero internacional.

Según el autor, a lo largo de la posguerra fría, *“la Alianza se va reconstruyendo a partir de la diferencia frente al otro, en este caso, frente a los países «no occidentales» y/o «no democráticos»”*(Ibid., 203). En este aspecto, Morales Hernández defiende la reorientación de la OTAN hacia una “comunidad de democracias”: *“Lo que se pretende proteger ahora –en lugar de la tradicional soberanía e independencia del Estado frente a una agresión armada– pasa a ser de forma creciente la identidad de los aliados como comunidad política, resumida en el concepto de democracia”*. Cabe por tanto comprender bajo este prisma la ampliación de la OTAN como un mecanismo de inclusividad en un contexto en el que se diluye el concepto de defensa y se refuerza el de seguridad. No obstante, su extensión hacia Europa Central y Oriental sería la ratificación de *“la preservación de Rusia como el principal ‘otro’ frente al que se constituye la identidad de la Alianza”*.

En el caso de Rusia, autores como Fojón Lagoa (1999) coinciden con Morales Hernández, en que la percepción de Rusia sobre la OTAN viene definida a raíz de la Cumbre de Bruselas de enero de 1994, orientada a estrechar vínculos entre la Alianza y los países no miembros pertenecientes al Consejo de Cooperación Nord Atlántico (CCNA) y se crea el *Partnership for Peace* (PfP) para reforzar la cooperación militar. En esa cumbre se da así, la oportunidad a los miembros efectivos de reafirmar que la organización está abierta a la incorporación de nuevos miembros. *“A partir de ese momento, el tema de la expansión de la OTAN domina las relaciones con Rusia. Siempre que se han referido a este asunto, los*

rusos lo han tratado como una amenaza a sus intereses de seguridad” (Ibid., 152). Asimismo, el autor alude también al componente psicológico como uno de los principales argumentos rusos para mostrar su reticencia a la ampliación de la OTAN:

“Los dirigentes de la Federación Rusa también han alegado la sensación de amenaza que produce en el ciudadano ruso la aproximación a sus fronteras de una poderosa organización militar que incluye a su enemigo en ambas Guerras Mundiales y a sus adversarios en la Guerra Fría y que también integrará a alguno, o quizás a todos, sus antiguos aliados”.

Ruiz González (2010) añade en este punto las negociaciones que tuvieron lugar entre OTAN y la URSS para la reunificación de Alemania. A pesar de que no existen pruebas escritas sobre las negociaciones, la Federación Rusa refiere al compromiso que adoptaron (e incumplieron según la narrativa rusa) entonces los mandatarios norteamericanos de que la OTAN no se expandiría hacia el este. De acuerdo con el autor, la posición de Rusia ante el imparable avance de la Alianza hacia el este fue estrechar sus lazos de cooperación para *“evitar su aislamiento y de tener un cierto grado de influencia en las principales cuestiones de seguridad en el continente”*. Destaca así dos movimientos:

- La participación de Rusia en las fuerzas de implementación de la OTAN tras los Acuerdos de Dayton de 1995, que pusieron fin de la guerra en Bosnia-Herzegovina
- La firma de 1997 del *Acta Fundacional sobre las relaciones mutuas, cooperación y seguridad entre la OTAN y la Federación Rusa* (no vinculante) que daría lugar a la creación del Consejo Conjunto Permanente OTAN-Rusia

Si bien Ruiz González (2010) identifica en estos acuerdos una clara intención por parte de Rusia de mantener su oposición a la ampliación a la vez de intentar influir todo lo posible para minimizar sus consecuencias, Fojón Lagoa (1999) los define como un *“intento de dar seguridad a Rusia”* y facilitar así la desactivación de las posibles medidas reaccionarias de Moscú ante la ampliación. En la línea de este último autor, el entonces Secretario General de la OTAN describe el proceso de la siguiente manera:

“Había que plantearse un paso más y abrirles la puerta [a los antiguos países del Pacto de Varsovia] para entrar en la Alianza. No tenía ningún sentido que se quedaran fuera. Ni ellos querían, al contrario. Pero había que hacerlo de una manera tal que no provocara una reacción negativa de Rusia. Entonces nos planteamos una operación brillante que era intentar, antes de que se produjera la decisión formal de la ampliación, llegar a un gran acuerdo previo con Rusia sobre los términos de sus relaciones con la Alianza” (Entrevista de Lluís Bassets a Javier Solana, 2010).

No obstante, la ratificación de la percepción rusa de la OTAN como amenaza a sus intereses vitales puede verse reflejada en las Doctrinas Militares y Conceptos Estratégicos de la Federación de los años 90. Concretamente, en el Concepto Estratégico de 1999, en el que se volvió a considerar a la Alianza como una amenaza contra la seguridad de la nación (Yturriaga Barberán, 2011). Esta modificación fue realizada tras la crisis de Kosovo, en la que los Aliados bombardearon (en marzo de 1999) a la República Federal de Yugoslavia, históricamente aliada de Rusia, que acusó a la OTAN de realizar la operación sin consultar al Consejo Conjunto Permanente. Días antes, República Checa, Hungría y Polonia entraron a formar parte de la Alianza.

Coincidiendo con la elección de Vladimir Putin como presidente ruso, las relaciones entre OTAN y Rusia entraron el siglo XXI marcadas por una profunda desconfianza causadas por la crisis de Kosovo y la ampliación de 1999. Y aunque estas mejoraron puntualmente inmediatamente después de los ataques del 11S por el respaldo de Putin a Washington –se impulsó el Consejo OTAN-Rusia– (Palacios y Arana, 2002), de acuerdo con el amplio de los estudios en la materia mencionados, las relaciones se deterioraron a partir de 2003-2004 por la intención de la OTAN de integrar a los países bálticos, Ucrania y Georgia, y por a la voluntad de EE. UU de instalar un sistema de defensa antimisiles en Europa Oriental. Según expone Yturriaga Barberán (2011), *“Rusia empezó a sufrir un sentimiento de cerco y acoso, lo que Rafael Calduch ha calificado de ‘telón de acero a la inversa’”*.

La entrada en la OTAN en marzo de 2004 de las tres Repúblicas Bálticas supuso un nuevo punto de tensión. Ya en 1995, el Consejo de Política Exterior y Defensa ruso preparó un

informe –Rusia y OTAN– en el que señalaba que “la posible incorporación de los Estados Bálticos y Ucrania a la OTAN convertiría las regiones en una zona de rivalidad estratégica” (citado en Gorskii, 2001). Hasta entonces Rusia había considerado históricamente estas regiones como parte de su “exterior próximo” y donde, como se ha mostrado en el capítulo anterior, había una gran porcentaje de ciudadanos rusos.

En este aspecto, cabe considerar que para Rusia la ampliación de la Alianza, no sólo suponía una amenaza en términos territoriales de acercamiento de la organización militar a sus fronteras, sino que implicaría también una pérdida de influencia en las antiguas repúblicas soviéticas (Matos Franco, 2017).

Cabe destacar, que a pesar de las presiones por parte de las Repúblicas Bálticas a la OTAN para el desarrollo de un plan de contingencia específico desde su adhesión, no fue hasta 2010 que la OTAN desarrolló el plan regional específico –Eagle Guardian– ideado para defender a los países bálticos y a Estonia. Esta demora en la creación de un programa específico es visto por algunos autores como símbolo de la voluntad de la Alianza por mantener unas buenas relaciones con Rusia. Según se expone en el Concepto de Seguridad Nacional de Estonia de 2004, la incorporación del país reduce la probabilidad de los ataques armados en Estonia, aunque no excluye la posibilidad del resurgir de esa amenaza que dependerá, según se desprende del documento, de la capacidad de desarrollo de planes de defensa específicos para el territorio en cooperación con los organismos internacionales.

5. DESARROLLO DEL CONFLICTO

5.1 Crisis del Soldado de Bronce de Tallin

La reubicación en 2007 de una estatua de la Segunda Guerra Mundial –El Soldado de Bronce– situada en el centro de Tallin fue el detonante de una crisis diplomática entre Estonia y Rusia reforzada a su vez por los ciberataques contra Estonia que siguieron al conflicto. Previo al análisis de los hechos acontecidos ese año cabe repasar la preparación legislativa que favoreció el desmantelamiento de la estatua, así como las diferentes interpretaciones simbólicas asociadas a la estatua.

El 10 de enero de 2007 el parlamento de Estonia (Riigikogu, en estonio) aprobó la proyecto de Ley sobre Protección de Tumbas de Guerra –con 66 votos a favor y 6 en contra–. En el preámbulo del documento se explicita que *“el entierro de personas que murieron en actos de guerra en lugares inadecuados está en discordancia con la cultura europea y la tradición de homenajear los restos, según el Artículo 34 del Protocolo Adicional de las Convenciones de Ginebra del 12 de agosto de 1949”* (Riigikogu, 2007). En consecuencia, en el Artículo 8 del Capítulo 3 se otorga al Gobierno estonio la capacidad de *“reubicar las tumbas y restos de fallecidos en guerra en base al interés público”*.

Tras la aprobación de la mencionada Acta, el 15 de febrero el parlamento pasó la Ley de Construcciones Prohibidas. Esta regla propuesta por el Partido Reforma y aprobada por 46 votos a favor frente a los 44 votos en contra, prohibía los monumentos y los símbolos que glorificasen tanto el nazismo como la ocupación soviética. En una de las cláusulas del documento se especificaba que el Gobierno estaba obligado a retirar el Soldado de Bronce de Tallin de la céntrica zona de Tõnismäe no más tarde de 30 días después de la entrada en vigor de la legislación.

Se trataba de un monumento originalmente conocido como Monumento a los Libertadores de Tallin, instalado en 1947 para conmemorar a los soldados soviéticos caídos durante la Segunda Guerra Mundial. Desde inicios de siglo XX este había sido lugar de celebración de la minoría rusa del país durante fechas señaladas como el Día de la Victoria, celebrado

el 9 de mayo. Cabe pues mencionar las diferentes interpretaciones simbólicas de la estatua así como los precedentes al conflicto relacionados con ella.

De acuerdo con Ehala (2009:144), se pueden extraer hasta cuatro fases diferentes de interpretación simbólica del monumento. Primero, representaba la caída de los nazis durante la Segunda Guerra Mundial, lo que explicaría que se mantuviese en la localización original 16 años después de la independencia estonia. Posteriormente pasó a simbolizar la victoria soviética, lo que la convertía en un lugar que conecta a la minoría rusa de Estonia con Rusia. En tercer lugar simbolizó la liberación de Estonia de los nazis y, por último, los nacionalistas estonios la consideraron un símbolo de la ocupación soviética. Cabe pues destacar la materialización de las diferentes narrativas históricas en la figura del soldado de bronce: mientras para unos era un opresor, para otros un libertador.

La movilización de la estatua a un cementerio a las afueras de la ciudad (a 1 km de su ubicación original) vino precedida por una secuencia de actos vandálicos sobre la estatua. La madrugada del 9 de mayo de 2005, celebración del Día de la Victoria de Rusia, la estatua apareció manchada con pintadas rojas. Esa misma efeméride en 2006, dos nacionalistas estonios irrumpieron en la celebración rusa portando la bandera estonia y fueron expulsados por la policía. *“El incidente que fue retransmitido por la televisión nacional fue considerado como una humillación para los estonios y la élite política prometió desmantelar la estatua”* (Ibid.:145, traducción propia). Autores como Ganuza Artilles (2010) sitúan este hecho como un agravante de las tensiones sociales: *“La sociedad estonia se fue polarizando cada vez más y el soldado de bronce se convirtió en el punto de encuentro de manifestantes extremistas, cada vez más con mayor agitación. El debate en la sociedad estonia estaba servido”* (citado en Joyanes Aguilar, 2010).

Tras estos acontecimientos, la retirada del Soldado de Bronce se convirtió en una promesa electoral de cara a las elecciones parlamentarias de 2007. Los principales partidos que lo incluyeron en su campaña fueron el ultraconservador Pro Patria and Res Publica Union y el liberal Partido Reforma liderado por Andrus Ansip (antiguo miembro de la junta directiva del PCUS regional antes de la disolución de la URSS). De acuerdo con diversos analistas, Ansip utilizó la estatua y la fractura social entre ciudadanos de nacionalidad

estonia y los de nacionalidad rusas como elemento central de su campaña (Brüggemann & Kasekamp, 2008).

En las elecciones generales del 4 de marzo de 2007 el Partido Reforma resultó vencedor, con 31 escaños, a los que se le suman los 29 de su compañero de coalición, el Partido Central; frente a la oposición conservadora, la Unión de la Res Pública y Pro-Patria (IRL por sus siglas en estonio) que fueron el partido más votado en 2003 Ansip fue reelegido como primer ministro y tras la preparación legislativa necesaria se dispuso a dismantelar y trasladar el monumento soviético de la Segunda Guerra Mundial, cumplir así con una de sus principales propuestas electorales y evitar una escalada de tensión antes del 9 de mayo similar a las anteriores (Cohen y Radin, 2019).

El anuncio sobre los preparativos para trasladar la estatua se dio a principios de abril. A nivel diplomático, el ministro de Asuntos Exteriores de Rusia, Sergei Lavrov, declaró que la reubicación “*violaría los principios elementales de la moral humana*”, sería “*un intento de reescribir la historia*”. A su vez, el viceprimer ministro, Sergei Ivanov, hizo un llamamiento a los ciudadanos rusos a boicotear bienes y servicios estonios. Como respuesta, el ministro de Asuntos Exteriores de Estonia calificó las acusaciones de Rusia de ser una calumnia. Por su parte, la Unión Europea defendió la visión de Estonia de que se trataba de un cuestión política nacional y no internacional (Mijinsen, 2014).

La mañana del día 26 de abril la policía acordonó la zona para comenzar con las excavaciones que permitirían desanclar la estatua y desenterrar los restos de ex soldados soviéticos que se encontraban en los alrededores. Esa misma mañana cuando la estatua fue retirada y oculta en un lugar desconocido —aunque existen diversas versiones sobre el momento exacto del desplazamiento—, un grupo de manifestantes pacíficos se congregaron en la plaza.

Por la tarde se unieron grupos violentos de nacionalistas rusos que fueron protagonistas de graves disturbios por toda la ciudad. Según diversos medios nacionales, se registraron manifestaciones también en las ciudades de Johvi y Kohtla-Jarve, de mayoría rusa. Se trata de un episodio sin precedentes desde la independencia de Estonia por su violencia.

Según medios como la BBC y la CNN, la policía local lanzó gases lacrimógenos y utilizó cañones de agua para detener a los manifestantes que cometieron múltiples actos vandálicos, como el destrozo de escaparates (Tanner; BBC; Fernández, 2007).

El enfrentamiento se extendió desde la tarde del 26 hasta el día 27, cuando la policía restableció la calma. Según datos ofrecidos por las autoridades estonias, hubo 1.300 arrestados, cientos de heridos y un fallecido (Ganuzo, 2010). Finalmente la estatua y los restos fueron trasladados al cementerio militar de las Fuerzas de Defensa Estonias, situado a las afueras de la capital, tras el fin de las protestas. El investigador Robert Kasier lo engloba como un acto de “reterritorialización”:

“Despojada del monumento de su época soviética y de los cuerpos de los soldados del Ejército Rojo, la plaza se reconvirtió en un lugar des-sovietizado, des-rusianizado y recientemente Europeizado que se replanteó con flores de los colores de la UE y desplazó en el espacio-tiempo a la URSS y a Rusia, convirtiéndola en una Estonia postsoviética y Europea.” (Kaiser, 2011: 1053)

Paralelamente a los disturbios en Tallin la tensión se trasladó hasta Moscú, donde hubo movilizaciones para protestar por la reubicación del monumento. Uno de los episodios más destacables fue el asedio a la embajada de Estonia en Rusia por parte de la organización Nashi (*Los Nuestros*, en español), que aglutinaba a jóvenes afines a Putin y que se auto definía como “Movimiento Juvenil Democrática Antifascista”. Cerca de 150 activistas bloquearon las entradas y salidas del recinto del 27 de abril al 1 de mayo. El grupo exigía una disculpa de la embajadora estonia, Marina Kaljurand y la restauración de la estatua (BBC, 2007). Cuando se puso fin al asedio del edificio, el entonces jefe del Comité de la Juventud de Rusia, Vasili Yakimenko, anunció en los medios de comunicación que comenzaría a recoger firmas para trasladar la Embajada estonia a las afueras de Moscú (Manaut, 2007).

5.1.1 Reacciones diplomáticas a las protestas

Las relaciones diplomáticas entre Estonia y Rusia pendían de un hilo la mañana del 28 de abril. El conflicto relacionado con el traslado de la estatua del Soldado de Bronce provocó reacciones por parte de Rusia. El Ministro de Exteriores ruso, Sergei Lavrov denunció un “*exceso del uso de la fuerza por las autoridades estonias*”, calificó la acción de “*blasfemia contra quienes lucharon contra el nazismo*” y anunció que “*habría serias consecuencias en las relaciones con Estonia*” (Myers, 2007).

Por su parte, algunas agencias de noticias rusas matizan que Lavrov declaró que “*se debía reaccionar sin histeria, pero también dar pasos serios que demostrarán nuestra auténtica actitud ante esta acción inhumana*”. Otras incluso aseguran que el Consejo de la Federación Rusa reclamó a Putin que rompiese relaciones con el país báltico. Cabe aquí destacar que no se han encontrado evidencias de estas declaraciones más allá que reproducciones de dichas instituciones rusas.

Por su parte, el primer ministro estonio, Andrus Ansip, aseguró que no era necesario entrar en discusiones con las autoridades de Moscú porque eran “*asuntos internos del país*” (Pons, 2017). En declaraciones públicas, el presidente de Estonia Toomas Hendrik Ilves defendió que el altercado no tenía nada que ver con la violación de tumbas o con la memoria de los caídos en la Segunda Guerra Mundial. Por el contrario, declaró que “*el denominador común de los criminales de la noche de protestas no era la nacionalidad, sino sus ganas de alboroto y de saquear*” (Ibid.).

5.2 Los ciberataques de 2007

5.2.1 Desarrollo, naturaleza y alcance nacional de los ciberataques

De manera simultánea a los enfrentamientos del 27 de abril comenzaron los ciberataques a las infraestructuras estonias. De acuerdo con el *think tank* estonio de defensa y seguridad, el International Centre of Defence Studies, los ciberataques variaron “en volumen y objetivo” del 27 de abril hasta el 18 de mayo.

En su análisis sobre la situación de la ciberseguridad en el ámbito internacional y en la OTAN, el teniente coronel Néstor Ganuza, jefe de Adiestramiento y Doctrina del Centro de Ciberdefensa de la OTAN distingue los ciberataques en dos fases principales.

La primera (del 27 al 29 de abril) caracterizada por unos ataques rudimentarios, de carácter técnico y organizativo sencillo y *“sin capacidad de convocar a un número de atacantes lo suficientemente grande como para causar daños serios y poner en una situación de crisis o indefensión a Estonia”*. El objetivo principal de los ataques fueron las páginas web de las instituciones públicas estonias, como la web del Gobierno, de sus ministerios y de los partidos políticos que registraron fallos masivos en la conexión. De hecho, el primer signo registrado fue que la imagen del primer ministro Andrus Ansip desapareció de la página web oficial del Partido Reformista. Al mismo tiempo, los servidores empezaron a recibir enormes cantidades de mensajes *Spam* hasta bloquearse (International Center for Defense and Security, 2007).

Los equipos de seguridad y defensa de Estonia alertaron ese mismo día de que no se trataban de fallos técnicos, sino que estaban siendo blanco de un ciberataque. El 28 de abril el Gobierno convocó un equipo especial para la crisis compuesto por miembros de los ministerios de Comercio, Comunicación, Defensa, los servicios de inteligencia y el Equipo Nacional de Respuesta ante Incidentes Informáticos (CERT, de sus siglas en inglés). Contó además con apoyo técnico de expertos de la OTAN. De acuerdo con Néstor Ganuza, *“este fue un gran triunfo de Estonia: identificar la gravedad del asunto con celeridad y organizar inmediatamente un equipo de respuesta multidisciplinar e investirse de la autoridad necesaria”*. El autor identifica tres elementos que fueron claves para el éxito del desarrollo de la respuesta: la rápida identificación de que se trataba de un ciberataque masivo, la rápida formación de un equipo multifuncional para coordinar la respuesta y el reconocimiento internacional de que estaban siendo atacados.

En la fase dos, del 30 de abril al 18 mayo, los ataques comenzaron a sofisticarse y se volvieron más complejos desde un punto de vista técnico (Kash, 2008). De acuerdo con el autor, los ciberataques *“reflejaban un mayor conocimiento de las herramientas de ciberguerra, y de una coordinación y organización más minuciosa”*.

Durante esta fase diversos medios de comunicación nacionales, como el Eesti Päevaleht o el Baltic News, informaron de que los ciudadanos no podían sacar dinero de los cajeros, ni los medios de comunicación difundir o retransmitir información. Según los datos del CERT, las infraestructuras críticas de información del país báltico, como los servicios e-banking de los bancos nacionales *Hansapank* y *SEB Eeesti Uhispank* y los proveedores de servicios de información nacionales como el periódico electrónico *Postimees* se vieron bloqueadas parcialmente. En este aspecto se pueden definir los siguientes objetivos de los ciberataques: instituciones gubernamentales y personajes políticos, medios de comunicación y bancos.

En cuanto al tipo de ciberataques registrados por el CERT, estos fueron en su mayoría:

- **Ataques Distribuidos de Denegación de Servicio (DDoS)** realizados a través de botnets y basados en el envío masivo y continuado de solicitudes a los servidores hasta colapsar la web. El objetivo eran las webs de instituciones gubernamentales e infraestructuras críticas.
- **Ataques de desfiguración de sitios web (*web site defacement*)**, por el que se puede modificar el aspecto visual de una web. En su mayoría, se registraron en las páginas web y perfiles sociales de los personajes políticos.
- **Ataques a servidores de sistemas a través de botnets**
- **Envío masivo de correo basura (spam)** a direcciones IP públicas y privadas de entidades y políticos, provocando la caída de los servidores.

En relación al alcance nacional, es preciso destacar que en 2007 Estonia era un país que tenía una gran dependencia del espacio cibernético a raíz de estrategia de desarrollo de la primera Estrategia para la Sociedad de la Información de 1994 (*The Estonian Way to the Information Society*), actualizada en 2004 y orientada al desarrollo digital de los servicios públicos y privados (Kalvet, 2007). Numerosos rankings internacionales, a saber el *UN Global e-Government Readiness Report 2005* y el *e-Readiness Ranking de Economist Intelligence Unit de 2006*, situaron a Estonia entre los primeros países del mundo más desarrollados en infraestructuras de la información.

Según expone el Gobierno estonio en su página web, desde el año 2000, los ciudadanos estonios pueden pagar impuestos a través de internet y desde 2002 cuentan con firma electrónica para la realización de trámites administrativos. Asimismo, en las elecciones municipales de 2005 el país se convirtió en el primero del mundo en utilizar el sistema de voto por internet. También en las elecciones legislativas de 2007 fue pionero en utilizar el sistema de voto electrónico a nivel nacional.

En la misma línea, desde el 2000 la actividad política (sesiones de gobierno y consejos de ministros) se realizan a través de internet, evitando la burocracia por papel. Su desarrollo político y social en el ámbito del ciberespacio suponen que *“un ataque con éxito a las redes que controlan dicha actividad provoca de inmediato una crisis de comunicación política”* (Ganuzá, 2010). Se pueden observar sus esfuerzos del desarrollo público de las TIC en el siguiente cronograma:

Figura 5. Evolución de la sociedad digital de Estonia 1994-2007



Fuente: e-estonia <https://e-estonia.com/>

Según autores como Ganuza, el desarrollo de estonio en este campo responde a una estrategia de defensa. El propio Gobierno justifica en su página web la creación del borrador de Principios de la política de información de Estonia (1994) como una solución estratégica a “tiempos políticamente turbulentos” y establece así la destinación del 1% del PIB a fondos estatales estables para las TIC. Es notable que el gasto militar de Estonia ese mismo año no fuese superior, sino que según datos del Instituto Internacional de Investigación para la Paz de Estocolmo (SIPRI), este era del también del 1% del PIB, uno de los más bajos a nivel europeo.

5.2.2 Reacciones diplomáticas a los ciberataques

Aunque oficialmente no se ha podido demostrar que el Kremlin estuvo detrás del asedio, el 5 de mayo de 2007, la edición alemana *The Financial Times* filtró una conversación telefónica mantenida por el Ministro de Asuntos Exteriores de la Federación Rusa Yevgeny Primakov y su homólogo alemán Frank-Walter Steinmeier, en la que el ministro ruso admitía que la Federación rusa se aseguraría de que la policía consiguiera acabar con el bloqueo si la embajada Estonia abandonaba Moscú. Esta indicaba la presunta implicación de Rusia con las movilizaciones.

Precisamente, una de las cuestiones que Ganuza (2011) destaca en su estudio es la evidente relación entre la situación política y los ciberataques. En este aspecto, resalta los datos ofrecidos por el analista en ciberamenazas y miembro de Arbor Networks, José Nazario, que recogen cómo el 8 de mayo a las 11 horas, cuando se inició la celebración del 9 de mayo en Moscú, el número de ciberataques se incrementaron en un 150%. En concreto, el 9 de mayo se registraron 58 ataques DDoS en comparación con los 21 registrados el 3 de mayo.

Tras los ataques, hubo acusaciones oficiales y no oficiales de Estonia de la posible implicación del Gobierno ruso. El CERT, como declaró posteriormente el Ministro de Asuntos Exteriores estonio del momento, Urmas Paet, identificó que los ciberataques, codificados en lengua rusa, procedían en su mayoría “*de IPs [o direcciones] de ordenadores de miembros de los órganos del gobierno ruso e incluso, de las*

administraciones del presidente de la Federación Rusa” (Ruus, 2008). Aunque también se registraron ataques procedentes de Egipto, Vietnam y Perú. En este aspecto, cabe destacar que las direcciones IP bien podrían ser las atacantes o direcciones IP asociadas a la red de ordenadores ‘zombi’ incluidas en la ruta del ataque pero no en su origen (Ganuza, 2011:193).

Rusia, por su parte, negó la autoría. En base a las declaraciones posteriores de los representantes de ambos países recogidas en las tablas 10 y 11 podemos resumir las diferentes narrativas diplomáticas sobre los ataques de la siguiente manera.

Para Estonia:

- El soldado de bronce representaba la ocupación soviética y había sido objeto de múltiples ataques, por lo que su traslado rebajaría la tensión entre habitantes rusos y estonios y favorecería la unidad nacional.
- Los ciberataques significaron una agresión contra la soberanía nacional de Estonia y también contra la soberanía de la Unión Europea.
- El ataque es percibido como una agresión contra la OTAN.

Tabla 10: Reacciones diplomáticas de Estonia a los ciberataques en 2007

<i>Representante</i>	<i>Declaración</i>	<i>Fuente</i>
Urmas Paet , ministro de Asuntos Exteriores 1 mayo	<i>“El ataque es virtual, psicológico y real al mismo tiempo. Las direcciones de IP han ayudado a identificar que los ciberataques terroristas contra las páginas web del Gobierno Estonio y la Oficina del Presidente tienen su origen en ordenadores y personas concretas de las agencias gubernamentales del Gobierno ruso, incluyendo la Administración del Presidente de la Federación Rusa”</i>	(Gobierno Estonia, 2007)
Andrus Ansip , primer ministro 2 mayo	<i>“Un ataque físico contra la embajadora de Estonia en Moscú (...) seguido de una serie de ciberataques procedentes de servidores de las autoridades rusas, de la retirada de la bandera estonia de nuestra embajada y de unas declaraciones de la delegación de la Duma de Rusia exigiendo el cambio de Gobierno en nuestro país indica que nuestro estado soberano está bajo un grave ataque. Todos estos eventos evidencian que no estamos tratando un problema doméstico, sino que es</i>	(Gobierno de Estonia, 2007b)

	<i>una intervención flagrante y coordinada relacionada con asuntos exteriores”</i>	
Toomas Hendrik Ilves , presidente 18 junio	<i>“Los ciberataques fueron algo más que una actividad criminal normal. Alguien pagó mucho dinero para costear el servicio de esos criminales. Cuando miras la evolución de los ataques, estos se paralizan a medianoche. Pregunté al CERT qué significaba y me dijeron: «Es lo que le hayan pagado al atacante ese día. Esto significa que están organizados. No sabemos quién está detrás, pero sabemos que desde hace tres años, cualquier proveedor de internet en Rusia debe, por ley, conectar sus cables con el Servicio Federal de Seguridad. El FSB contral internet allí”</i>	(Frankfurter Allgemeine Zeitung, 2007)
Ene Ergma , presidenta del Parlamento estonio 21 agosto	<i>“Estonia es un país de la OTAN. Atacarnos a nosotros es una manera de comprobar la capacidad de defensa de la Alianza, que puede medir su capacidad de reacción en función de la respuesta dada a las protestas de la estatua de bronce”</i>	(Citado en Joshua Davis, 2007)

Fuente: <https://www.stratcomcoe.org/>, traducción propia

Para Rusia:

- El traslado de bronce suponía un desprecio hacia la historia soviética y un ataque contra la minoría rusa del país.
- Su traslado implicaría serias consecuencias en el ámbito de las relaciones bilaterales.
- Niegan toda relación con los ciberataques.

Tabla 11: Reacciones diplomáticas de Rusia a los ciberataques en 2007

Representante	Declaración	Fuente
Putín , presidente de Rusia 9 mayo	<i>Durante la celebración del Día de la Victoria: “Aquellos que intentan hoy desmantelar las estatuas de héroes de guerra están insultando a sus propios ciudadanos, sembrando discordia y desconfianza entre personas y estados”</i>	(Kremlin, 2007)
Dimitri Peskov , jefe de prensa del presidente 17 mayo	<i>“De ninguna manera el estado de Rusia está implicado en el ciberterrorismo (...) Cuando se observan las direcciones IP estas muestran que los ataques proceden de una gran variedad de países de todo el mundo. Esto no significa que los estados extranjeros estén detrás de esos ataques. Además, como probablemente sabrán, las direcciones IP pueden ser falsas”</i>	(BBC, 2007)

Fuente: <https://www.stratcomcoe.org/>, traducción propia

6. IMPLICACIONES EN EL MARCO DE LA OTAN Y DESARROLLO DE LA CIBERSEGURIDAD

6.1 Alcance de los ciberataques en el marco de la OTAN

Durante los ciberataques, la OTAN proporcionó asistencia técnica a Estonia y envió a expertos al país para colaborar con el CERT. Esta es considerada la primera vez que un país miembro de la Alianza solicita apoyo para contrarrestar un ataque a sus infraestructuras digitales. Es también la primera vez que se registra una agresión cibernética contra todo un Estado. En su solicitud de apoyo a la OTAN, el ministro de Defensa estonio, Jaak Aavikso, constató que los ataques estaban dirigidos a las infraestructuras electrónicas esenciales y que era la *“primera vez que un botnet amenazaba la seguridad de una nación entera”* (citado en Joubert, 2012). En base a las declaraciones abajo recogidas (véase Tabla 11), la OTAN consideró los ciberataques contra Estonia como una amenaza a la seguridad de la Alianza y aunque no se aventuraron a acusar a Rusia, mostraron su apoyo a la versión estonia sobre la autoría.

Tabla 12: Reacciones diplomáticas de la OTAN en los ciberataques en 2007

<i>Representante</i>	<i>Declaración</i>	<i>Fuente</i>
James Appathurai , portavoz de la OTAN 23 mayo	<i>“Creo que es bastante claro que este tipo de ataques son muy difíciles de rastrear de manera definitiva, lo que supone uno de los mayores desafíos en materia de ciberdefensa. No puedo hablar del origen, pero los estonios ya han hablado de dónde creen que proceden.”</i>	(OTAN, 2007)
Jaap de Hoop Scheffer , secretario general de la OTAN 25 mayo	<i>“Estos ciberataques tienen una dimensión de seguridad sin ninguna duda. Ese es el motivo por el que un experto de la OTAN ha sido enviado a Estonia para ver qué se puede hacer. ¿Tiene esto una implicación en materia de seguridad? Sí, tiene una implicación en seguridad. ¿Es relevante para la OTAN? Sí, es relevante para la OTAN. Es un asunto que temo que estará presente en la agenda política de los tiempos que vienen.”</i>	(DW, 2007)

Fuente: <https://www.stratcomcoe.org/>, traducción propia

Según se expone en la página web de la OTAN, la organización ha defendido sus sistemas de comunicación e información desde que en 2002, en la Cumbre de Praga se incluyese la ciberdefensa en la agenda política de la Alianza. La voluntad de reforzar la protección de estas infraestructuras fue ratificada en la Cumbre de Riga de 2006. Hasta 2007 la única estructura en materia de ciberseguridad y defensa era el Computer Incident Response Capability (NCIRC), creado en 2004 y cuya función es proteger y defender las infraestructuras digitales de la OTAN. La protección de las infraestructuras nacionales corría a manos de los países miembros. La página web recoge también cómo derivado de los ciberataques contra Estonia, los ministerios de defensa de los países miembros consensuaron que se necesitaba reforzar la defensa en el ciberespacio.

En su revisión sobre las lecciones aprendidas por la OTAN cinco años después de los ciberataques de Estonia, Vincent Joubert (2012) expone que los ciberataques fueron un verdadero despertar para la Alianza:

“Ofrecieron una demostración práctica de cómo los ciberataques pueden desestabilizar una nación entera con fuerte dependencia de las TIC. Esto supone una nueva amenaza para los miembros de la OTAN, así como para la integridad y la eficiencia de los sistemas de información, vitales para la tarea principal de la organización de defensa colectiva y cooperación de crisis”.

Cabe pues destacar que los ciberataques de 2007 pusieron de manifiesto cómo los ataques cibernéticos no se limitaban a ser una amenaza para las instituciones, sino que podían ser una amenaza para la seguridad nacional. De acuerdo con el autor, estos evidenciaron vulnerabilidades en el sistema de ciberseguridad de la Alianza desde tres perspectivas:

- A) Legal.** Desde una perspectiva legal, el Artículo 4 del Tratado del Atlántico Norte (1949) permitía a Estonia requerir una consulta formal con el resto de estados de la OTAN, puesto que los ciberataques amenazaban la seguridad nacional y la independencia política. No obstante, no pudo ser aplicado el Artículo 5 del Tratado, que establece la cláusula de defensa colectiva frente

a un ataque armado. Este determina que: “*las partes acuerdan que un ataque armado contra una o más de ellas, tenga lugar en Europa o en América, debe ser considerado como un ataque dirigido contra todas ellas y, en consecuencia (...) acuerdan tomar las medidas necesarias*”, no pudo ser aplicado al no considerar los ciberataques como una acción militar. Según apunta el autor, en este aspecto, las diferentes concepciones sobre los ciberataques y el ciberespacio (véase Capítulo 2) dificultan el consenso sobre si responder o no a un ataque cibernético. Caben además plantearse otras cuestiones como: ¿Qué se considera un ataque armado? Dado la volatilidad de los atacantes, ¿contra quién se debe responder?

B) Operacional. Joubert expone que la solicitud de Estonia a la OTAN ponía de manifiesto la necesidad de la Alianza de extender sus capacidades en materia de ciberdefensa más allá de la protección de las infraestructuras internas. Sobre todo, ante la incapacidad de determinar la autoría y de prevenir los ataques. En este sentido, el autor apunta a que la Alianza tomó consciencia de la necesidad de ayudar a los Aliados a defender sus Infraestructuras Críticas de Comunicación.

C) Estratégico. Desde un punto de vista estratégico, la defensa del ciberespacio supuso un gran desafío para la OTAN puesto que las hasta entonces empleadas doctrinas y estrategias no podían ser extrapoladas al dominio cibernético debido a su compleja naturaleza (véase Subcapítulo 2.2).

A raíz de una revisión de estas cuestiones, en 2008 la OTAN reforzó sus esfuerzos en materia de ciberseguridad. En 2008 se estableció:

- La aprobación de la primera Política de Ciberdefensa de la OTAN (*NATO Policy on Cyber Defense*).

- Acuerdo sobre el Concepto de Ciberdefensa de la OTAN (*NATO Cyber Defence Concept*) a comienzos del año 2008, en el que se recogía la principal respuesta frente a un ciberataque y se ampliaba el objetivo de defensa a la ciberseguridad de los Aliados (Caro Bejarano, 2011).

En este sentido, cabe también destacar que en 2010 se revisó el Concepto Estratégico de la OTAN de 1999 y se consideraron los ciberataques como una de las nuevas amenazas a las que la Alianza debía hacer frente. Se cita que:

“Los ciberataques están siendo más frecuentes, más organizados y más costosos en el daño que infligen en las administraciones gubernamentales, los negocios, economías y potencialmente en las redes de transporte y abastecimiento y otras ICI; pueden alcanzar un nivel tal que amenace la prosperidad, seguridad y estabilidad nacional y euro-atlántica”.

Asimismo, en 2008 también desarrollaron nuevas estructuras organizativas para implementar tanto la política de ciberdefensa y complementar así las funciones del NCIRC. Estas son:

- La Autoridad de Gestión de la Ciberdefensa de la OTAN (*NATO Cyber Defence Management Authority, NCDMA*)
- El Centro de Excelencia Cooperativa de Ciberdefensa en Estonia (*Cooperative Cyber Defence Centre of Excellence, CCDCOE*)

6.2 Desarrollo de la Ciberseguridad Estonia-OTAN

Como se ha expuesto anteriormente, los ciberataques vulneraron las principales Infraestructuras Críticas de Información (ICI) de Estonia, aunque estas no llegaron a interrumpirse ni a quedar inutilizadas (Ganuza, 2011). En este aspecto es importante resaltar que las normativas desarrolladas a partir de los ciberataques en el campo de la

ciberseguridad estuvieron orientadas a proteger, a la vez que impulsar, dichas infraestructuras.

Inmediatamente después de los ciberataques, el Gobierno estonio aprobó el Plan de Acción para Contrarrestar Ciberataques (julio) orientado a mejorar los procesos de preparación para emergencias en caso de ciberataques y a preparar unas bases legales para combatir el cibercrimen. En septiembre se aprobó el Plan de Implementación 2007-2008 de la Estrategia de la Sociedad Digital Estonia, que concretaba que debían desarrollarse las ICI en base a su capacidad para responder en situaciones de emergencia (Ficha técnica Joinup, Comisión Europea, 2015).

En 2008, se adoptó la Estrategia de Ciberseguridad, elaborada por un comité multidisciplinar compuesto por el Ministerio de Defensa, el de Economía, de Comunicaciones, de Defensa, de Interior, de Justicia y de Asuntos Exteriores, así como agencias y representantes del sector privado.

De acuerdo con el análisis elaborado por Czosseck, Ottis y Talihärm (2011), expertos del Centro de Excelencia Cooperativa de Ciberdefensa en Estonia, la Estrategia considera “*la ciberseguridad como un esfuerzo nacional que responde a la amenaza asimétrica que presentan los ciberataques*” (Czosseck et.al., 2011:58). El documento está creado en un contexto posterior a los ataques e identifica cuatro objetivos estratégicos:

1. La aplicación gradual de las medidas de sistemas de seguridad en Estonia
2. Desarrollo de las competencias en ciberseguridad y promoción del conocimiento de la seguridad de la información
3. Desarrollo de un marco regulatorio y legal para apoyar la seguridad de la operabilidad de los sistemas de información
4. Promoción de la cooperación internacional y refuerzo de la ciberseguridad global

En relación al objetivo 4 cabe destacar que los principales esfuerzos de cooperación internacional se hicieron en el marco de la UE y la OTAN y de los Estados miembros de ambas instituciones. La percepción de Estonia como un país con una gran capacidad de reacción durante y tras los ciberataques (Ganuza, 2011), así como la toma de conciencia por parte de la OTAN de la naturaleza transnacional de los ciberataques y su consecuente necesidad de reforzar sus estrategias de ciberdefensa más allá de la Alianza (Joubert, 2012), derivó en un refuerzo de la cooperación entre Estonia y la Alianza Atlántica en el campo de la ciberseguridad.

Se puede tomar como ejemplo la creación del Centro de Excelencia Cooperativa de Ciberdefensa (CCDCOE) establecido en Tallin y acreditado por la OTAN en 2008. Según se expone en la página web del Centro, su misión es *“apoyar a nuestros países miembros y a la OTAN con una experiencia interdisciplinaria única en el campo de la investigación, la capacitación y los ejercicios de defensa cibernética que cubren las áreas de enfoque de tecnología, estrategia y derecho”*.

Ante la falta de legislación sobre las nuevas guerras en el ciberespacio, el CCDCOE convocó tras los ciberataques al Grupo Internacional de Expertos (GIE) en defensa, ciberseguridad y Derecho internacional para que elaboraran una suerte de equivalente al Derecho Internacional Humanitario pero aplicado al nuevo dominio (Reguera, 2015). De esta reunión surgió entre 2009 y 2012, el Manual de Tallin, dirigido por el Profesor de la US Naval War College, Michael Schmitt, y en el que se analiza la aplicación del derecho internacional a las operaciones cibernéticas. Este parte de la base de que *“la guerra no deja de ser una guerra porque se desarrolle en el ciberespacio”* (Ibid.).

7. CONCLUSIONES

7.1 Determinación de la validez de la hipótesis

Tras un análisis exhaustivo de las relaciones entre Rusia y Estonia en el ámbito bilateral, así como dentro del marco de relación Rusia-OTAN, podemos dar como válida la hipótesis general de que “las tensiones acumuladas en las relaciones ruso-estonias motivaron un ciberataque masivo que ha impulsado el desarrollo de Estonia y la OTAN en materia de ciberseguridad”.

El recorrido histórico a través de análisis existentes previos nos ha permitido identificar la naturaleza de las relaciones entre ambos países más allá de los puntos de tensión concretos, como lo son el conflicto ya resuelto del desmantelamiento de las instalaciones militares, el conflicto sobre la demarcación de las fronteras y la cuestión de las minorías étnicas. En este sentido, los dilemas de seguridad alimentados por las diferentes (y antagónicas) narrativas históricas se presentan como una constante a lo largo de la evolución de las relaciones.

Asimismo, como se ha constatado, estas vienen definidas por dos procesos de construcción de identidad nacional: en el caso de Estonia como contraposición al “otro” y acercamiento a Occidente y, en el caso de Rusia como ratificación de su percepción de “gran potencia” en el contexto postsoviético y protección de su pasado soviético de la que es heredera. Este último proceso puede verse reflejado en el interés ruso de influir en el territorio báltico inmiscuyéndose en problemas que Estonia considera de carácter doméstico como las restricciones de la Ley de Ciudadanía o la retirada de la estatua del Soldado de Bronce de Tallin. Esta dinámica se percibe también después de la adhesión a la OTAN y la UE, por lo que podemos constatar que sigue caracterizando las relaciones bilaterales de manera independiente al estado de las relaciones Rusia-OTAN e incluso Rusia-UE.

Aunque no existen pruebas concluyentes sobre la autoría de los ciberataques, las reacciones estudiadas en ambos sentidos apuntan a que la crispación entre ambos países continuó, o más bien se acentuó, durante y después de los ciberataques. En este sentido, los

ciberataques suponen, cuando menos, un punto de inflexión en las relaciones bilaterales entre Rusia y Estonia, que alcanzaron su máximo grado de tensión en 2007.

Siguiendo las principales teorías expuestas, como la de Viktorova (2006) y la de Galbreath y Lasas (2013), crisis diplomática que estalló a lo largo de 2007 puede ser entendida también como un choque de identidades que trascienden incluso la cuestión migratoria. Los diferentes simbolismos y representaciones de la estatua reflejan la disonancia entre ambas comunidades, lo que se puede extrapolar al nivel internacional. En este sentido, cobra relevancia la propuesta de Viktorova (2006) de que *“Rusia y Estonia articulan percepciones del otro como una amenaza fundamental para la percepción de la propia identidad”*.

Esta lógica nos remite a las hipótesis secundarias de este trabajo. En relación a la exclusión de la evolución de las tensiones OTAN-Rusia como detonante de los ciberataques, el estudio realizado deja la puerta abierta a matices. Si bien las relaciones entre la organización militar y la potencia rusa no estaban en su mejor momento debido a la ampliación de la OTAN hacia el Este en 2004, no ha sido posible recoger suficientes evidencias sobre la intencionalidad de Rusia de atacar directamente a la Alianza como respuesta a una escalada de desconfianza mutua, puesto que la última tensión registrada fue con la incorporación de los países bálticos.

En contraste, el espacio utilizado para el ataque (el ciberespacio) deja abierto el debate sobre si los ataques fueron o no una “prueba” de la capacidad de respuesta de la OTAN ante una amenaza cibernética. Esto también puede ser comprendido como un intento de impedir precisamente la intervención de la Alianza en la operación contra Estonia, al no considerarse en el Tratado de Washington los ciberataques como un “ataque armado”, susceptible de ser respondido con una operación conjunta de los miembros de la organización.

En cuanto a las hipótesis sobre el desarrollo de la ciberseguridad estonia de manera independiente y dentro de la OTAN, como respuesta a una necesidad de protección frente a Rusia, esta ha sido analizada dentro del marco de las relaciones entre Estonia y Rusia, y

Rusia y OTAN. En el primer caso, las percepciones sobre las amenazas a su seguridad llevaron a Estonia a desarrollar un avanzado sistema administrativo y político basado en el refuerzo de las TIC justo después de su independencia en 1994, momento de gran tensión con Rusia por las negociaciones sobre la retirada de las tropas y la delimitación de las fronteras. Su refuerzo en este campo contrasta con el poco gasto militar del país, por lo en un ataque convencional sus capacidad de respuesta sería muy probablemente menor que la que demostraron tener en la gestión de los ciberataques.

El marco de las relaciones OTAN-Rusia, caracterizado tras la disolución de la URSS en la mejorar de las relaciones entre las dos partes y la reconstrucción de la identidad de la Alianza presuponen por tanto una actitud inicial conciliadora, al menos sobre papel, reflejada en los esfuerzos expuestos como el Consejo Permanente OTAN-RUSIA o el Acta Fundacional. Las reticencias iniciales de la organización al desarrollo de un plan de contingencia específico para las Repúblicas Bálticas puede ser comprendido dentro de esta dinámica. No obstante, los ciberataques de 2007 supusieron un punto de inflexión para la Alianza, demostrando el carácter transnacional del ciberespacio y su capacidad de suponer una amenaza para la seguridad nacional de los países miembros. Esta seguridad es una de las principales áreas de defensa a las que se compromete la OTAN y un ataque en ellas supone a su vez un desafío para su propia integridad.

En este contexto, y en base a la hipótesis secundaria sobre cómo el desarrollo de la ciberseguridad mejora la posición de Estonia dentro de la OTAN, podemos concluir que el desarrollo de la cooperación entre ambos en el marco de la ciberseguridad inmediatamente posterior (como la creación del Centro de Excelencia de la Defensa Cibernética Cooperativa de la OTAN) describen un refuerzo de la seguridad en un sentido bidireccional. Sale, eso sí, reforzada Estonia con poco capacidad militar y hasta 2010 carente de un plan de defensa específico avalado por la OTAN.

7.2 Cumplimiento del objetivo y objetivos secundarios de la investigación

En cuanto al cumplimiento del objetivo de la investigación, que consiste en “definir el peso de las relaciones bilaterales entre Rusia y Estonia en los ciberataques de 2007”, podemos concluir que este ha sido alcanzado. Se ha realizado un estudio atendiendo a una separación entre antes y después de la ampliación de la OTAN. Sin embargo, ha quedado demostrado que estas no alteran su naturaleza contenciosa con la incorporación de la ex república báltica a la Alianza. Para llevar a cabo este objetivo se han atendido los asuntos político-militares (principales conflictos), las realidades demográficas (presencia de minorías rusas en Estonia) y la importancia de cada uno de los actores dentro de las relaciones entre ellos, y entre cada uno y la OTAN.

Asimismo, se han alcanzado también los siguientes objetivos secundarios:

- En cuanto a la evaluación de la naturaleza de las relaciones bilaterales entre Rusia y Estonia, estas han quedado definidas en base a tres elementos: dilemas de seguridad, divergencia de la narrativa histórica y el proceso de construcción de identidad nacional como oposición al otro.
- Sobre la concreción de los principales puntos de tensión entre ambos países, se han establecido tres cuestiones principales durante el período 1991-2004: el desmantelamiento militar, que fue resuelto antes de la entrada en el siglo XXI, la cuestión fronteriza, latente hasta después de la ampliación de la OTAN y la cuestión de las minorías rusas, un problema todavía sin solventar y principal punto de discordia. En un segundo período definido de entre 2004 y 2007 se ha concretado como principal punto de tensión la incorporación de Estonia a las organizaciones occidentales y la dificultad de Rusia de ejercer su histórica influencia en la zona.
- Se ha descrito también cómo la evolución y naturaleza de las relaciones entre la OTAN y Rusia también han influido en la crisis de los ciberataques. No obstante, su implicación puede ser definida de manera indirecta, ya que su conexión viene

determinada por la forma (puesto que el Artículo 5 del Tratado Atlántico no contempla los ciberataques como ataque armado) y no tanto por su conexión con la crisis del Soldado de Bronce.

- Respecto al análisis de la implicación de los ciberataque en el desarrollo de un marco de seguridad en Estonia y en la OTAN estos han supuesto una apertura al desarrollo de los sistemas de ciberseguridad nacionales, así como al desarrollo de la la cooperación internacional en este ámbito.

BIBLIOGRAFÍA

1. TEXTOS DOCUMENTALES Y LEGALES

1.1 TEXTOS DOCUMENTALES

Gorskii, V. (2001): *Problems and Prospects of NATO-Russia Relationship: the Russian Debat Report*, Moscú, NATO Euro-Atlantic Partnership Council Fellowships Programme 1999-2001

Klimburg, A. (2012): *National Cyber Security Framework Manual*, OTAN CCD COE Publication: Tallinn

OTAN (2013): *Tallinn Manual of the International Law applicable to Ciberwarfare*. Cambridge University Press.

Pellerin, C. (2010): *Lynn: Cyberspace is the New Domain of Warfare*, Washington, American Forces Press Service.

Stang, G. (2013): *Global commons: Between cooperation and competition*, Comisión Europea. Disponible en: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_17.pdf (Último acceso el 12 abril 2020).

Zaaiman, J. & Leenan, L. (2015) *Proceedings of the International Conference on Information Warfare and Security*, Academic Conferences Limited.

1.2 LEYES Y TRATADOS

Congreso de Estados Unidos (1992): *Freedom Support Act*, 1992-1991. Disponible en <https://www.congress.gov/bill/102nd-congress/senate-bill/2532> (Último acceso el 15 de junio 2020)

OTAN (1949): *Tratado del Atlántico Norte*, Washington, 4 abril 1949. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es (Último acceso el 24 de mayo 2020)

Riigikogu (1992): *Constitución de la República de Estonia*, Gobierno de Estonia.

Riigikogu (1992): *Ley de Ciudadanía 1992*, Gobierno de Estonia.

Riigikogu (1993): *Ley de Autonomía Cultural de las Minorías Nacionales*, Gobierno de Estonia.

Riigikogu (2007): *Ley sobre Protección de Tumbas de Guerra*, Gobierno de Estonia.

1.3 INFORMES

CCN-CERT (2015): *Guía de Seguridad (CCN-STIC-401) Glosario y Abreviaturas*.

Disponible en:

<https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html>

CCN-CERT (2019): *Informe de Ciberamenazas y Tendencias 2019*, Ministerio de Defensa del Gobierno de España.

Comisión Europea/ Joinup (2015): *Ficha técnica. E-Government in Estonia*. Enero de 2015, N.17

Helsinki Watch (1992): *Human Rights World Report, 1992*. Disponible en:

<https://www.hrw.org/reports/1992/WR92/index.htm> (Último acceso el 24 de mayo de 2020)

Naciones Unidas (2005): *UN Global e-Government Readiness Report 2005*, department of Economic and Social Affairs Division for Public Administration and Development Management

The Economist (2006): *The 2006 e-readiness rankings*, The IBM Institute for Business Value y The Economist Intelligence Unit

World Economic Forum (2012): *Global Risk Report 2012*, Suiza

World Economic Forum (2020): *Global Risk Report 2020*, Suiza

1.4 BANCOS DE DATOS

Instituto Internacional de Investigación para la Paz de Estocolmo (SIPRI) (1991-1995): *Gasto militar en Estonia*. Disponible en:

<https://datos.bancomundial.org/indicador/MS.MIL.XPND.GD.ZS> (Último acceso el 15 de marzo 2020)

Statistics Estonia (2000): *Population and Housing Census 2000*, Statistical database.
Disponible en: <https://www.stat.ee/population-census-2000> (Último acceso el 17 de mayo de 2020)

2. LIBROS Y CAPÍTULOS DE LIBROS:

2.1 OBRAS GENERALES

Arp, B. (2008): *International Norms and Standards for the Protection of National Minorities: Bilateral and Multilateral Texts With Commentary*. Brill.

Calduch Cervera, R. (2014): *Métodos y técnicas de investigación internacional*, Madrid, Universidad Complutense de Madrid.

Choucri, N. (2012): *Cyberpolitics in international relations*, Cambridge, Massachusetts; London, England: The MIT Press.

Cohen, R., & Radin, A. (2019): *Russia's Hostile Measures in Europe: Understanding the Threat*. Rand Corporation.

Cucó, A. (1998): *El despertar de las naciones: La ruptura de la Unión Soviética y la cuestión nacional*, Universitat de València.

Eberhardt P, Owsinski J. (2015): *Ethnic Groups and Population Changes in Twentieth Century Eastern Europe*. ME Sharpe

Falkenrath, A. (1995): *Shaping Europe's Military Order: The Origins and Consequences of the CFE Treaty*. s.l MIT Press N.6, V.6.

Galbreath, D. (2005): *Nation-Building and Minority Politics in Post-Socialist States: Interests, Influence and Identities in Estonia and Latvia. Soviet and Post-Soviet Politics and Society* 8, Ibidem Verlag, Stuttgart.

Gibson, W. (1901): *Neuromante*, Minotauro

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, P. (2010): *Metodología de la investigación*, México DF: McGraw Hill .

Matos Franco, F. (2017): *Historia mínima de Rusia*, Turner.

Mijnssen, I. (2014): *The Quest for an Ideal Youth in Putin's Russia I: Back to Our Future! History, Modernity, and Patriotism according to Nashi, 2005-2013*, Volume 114 of Soviet and Post-Soviet Politics and Society, Columbia University Press.

Starr S.F, Dawisha, K. (2016): *The International Politics of Eurasia: State Building and Military Power in Russia and the New States of Eurasia*, Routledge

2.2 LIBROS ELECTRÓNICOS

Brüggemann, K. y Kasekamp, A. (2008): *The Politics of History and the “War of Monuments” in Estonia*, Nationalities Papers V.36

Buhbe, M. (2017): "Introducción", En: *Russia, the EU and the Baltic States The Future of Partnership and Cooperation: Interests, Concepts, Implementation* . Moscú/Vilnius.
Disponible en: <https://library.fes.de/pdf-files/id/04875.pdf>

Kramer, F; Staar, S. y Wentz, L. (2009): *Cyberpower and National Security*. Disponible en: www.jstor.org/stable/j.ctt1djmhj1 (Último acceso el 18 marzo de 2020)

Schwartau, W. (1994): *Information Warfare: Chaos on the Electronic Superhighway*. pp, 16-17 Disponible en: <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=150670> (Último acceso el 16 de enero 2020)

2.3 CAPÍTULOS DE LIBROS

Candau Romero, J. (2011): “Estrategias nacionales de ciberseguridad. Ciberterrorismo”. En *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*. Madrid: n/s. pp. 259-261

Caro Bejarano, M. J. (2010): “Alcance y ámbito de la seguridad nacional en el ciberespacio”. En: I. E. d. E. Estratégicos, ed. *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*.

Feliu Ortega, L. (2012): "La ciberseguridad y la ciberdefensa". Enmprenta del Ministerio de Defensa, *El ciberespacio. Nuevo Escenario de Confrontación*. s.l.:Imprenta del Ministerio de Defensa.

Galbreath, J. y Lañas, A. (2013) “10: Estonia, Latvia and Lithuania”. En David, M., Gower, J. y Haukkala, H., 2013, *National Perspectives on Russia. European Foreign Policy in the making?* Routledge Advances in European Politics

Ganuza, A. (2010): “La situación de ciberseguridad en el ámbito internacional y en la OTAN” En Instituto de Estudios Estratégicos, ed., *Ciberseguridad. Retos y amenazas de la seguridad nacional en el ciberespacio*, pp.167-214

Joyanes Aguilar, L. (2010): “Estado del arte de la ciberseguridad”. En Ministerio de Defensa, ed., *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, Cuadernos de Estrategia, pp. 14-20.

T. Kuehl, D (2009): “Capítulo II. Defining the Problem”. En Kramer, F; Staar, S. y Wentz, L. *Cyberpower and National Security*. Disponible en: www.jstor.org/stable/j.ctt1djmhj1 (Accesible última vez el 18 marzo de 2020)

3. ARTÍCULOS

3.1. ARTÍCULOS DE REVISTAS CIENTÍFICAS

Czosseck, C.; Ottis, R. y Talihärm, A.M. (2011): “Estonia after the 2007 cyberattacks”, *International Journal of Cyber Warfare and Terrorism* 1(1)

Dunlop, J. (1993): “Russia: Confronting a Loss of Empire, 1987-1991”, *Political Science Quarterly*, N.108, V. 4., pp 603-634.

Ehala, M. (2009): “The Bronze Soldier: Identity Threat and Maintenance in Estonia”, *Journal of Baltic Studies*, 40:1,139 Disponible en : https://www.researchgate.net/publication/233167347_The_Bronze_Soldier_Identity_Threat_and_Maintenance_in_Estonia (Último acceso el 17 de marzo de 2020)

Flournoy, M. y Sulmeyer, M. (2018): “Batterfield Internet”, *Foreign Affairs*, septiembre/octubre, N. 97, V. 5, pp. 40-46.

Fojón Lagoa, J.A., (1999): “La relación OTAN-Rusia, percepciones mutuas”. *Cuadernos de Estrategia* N°101

González, Á. (2000): “Minorías rusas en la antigua URSS”, *Revista CIDOB D'Afers Internacionals*, N. 51/52, pp. 25-43. Disponible en: www.jstor.org/stable/40585837 (Último acceso del 16 de mayo de 2020)

Herz, J. H. (1950): “Idealist Internationalism and the Security Dilemma,” *World Politics*, Cambridge University Press, N.2, V. 2, pp. 157–180.

Herzog, S. (2011): “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses”, *Journal of Strategic Security* 4, no. 2 Disponible en: <https://scholarcommons.usf.edu/jss/vol4/iss2/4> (Último acceso el 15 de marzo de 2020)

Joubert, V. (2012): “Five Years after Estonia’s Cyber Attacks: Lessons Learned for NATO?” *NATO Defense College*. Disponible en: www.jstor.org/stable/resrep10366 (Último acceso el 12 de febrero de 2020)

Kalvet, T. (2007): “The Estonian Information Society Developments Since the 1990s”. *Praxis working paper* N.29, Praxis Center for Policy Studies and Tallin University of Technology. Disponible en PDF: <https://pdfs.semanticscholar.org/87db/19146355206e5c97881074c9b8b9db13c32d.pdf>

Kara-Murza, V. (2015): “Russia and the Baltics: once friends, now foe”, *World Affairs*, N.177, V,5. Pp.,16-23. Disponible en: www.jstor.org/stable/43555420 (Último acceso el 28 de marzo 2020)

Morales Hernández, J (2010): “El futuro de la OTAN y Rusia. Identidades y exclusión en la seguridad europea”, *Revista CIDOB d’Afers Internacionals*, núm. 89-90, pp.199-210

Palacios, J.M., Arana P. (2002): “Doctrina militar rusa: herencia soviética, realidades postsoviéticas, perspectiva europea”, *Revista CIDOB d’Afers Internacionals*, núm. 59, p. 81-103.

Park, A. (1994): “Ethnicity and Independence: The Case of Estonia in Comparative Perspective”, *Europe-Asia Studies*, 46(1), 69-87. Disponible en: www.jstor.org/stable/153031 (Último acceso el 13 de marzo 2020)

Park, A. (1995): “Russia and Estonian Security Dilemmas”, *Europe-Asia Studies*, 47(1), 27-45. Disponible en: www.jstor.org/stable/153192 (Último acceso el 15 de marzo 2020)

Ruus, K. (2008): “Cyber War I: Estonia Attacked from Russia”, *European Affairs*., 9(1-2).

Theiler, O. (2011): “Nuevas amenazas: el ciberespacio”. *La Revista de la OTAN*. Disponible en <https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm>. Último acceso el 14 de mayo 2020

Viktorova, J. (2006): “Transformation or Escalation? The Estonian-Russian Border Conflict and European Integration”, *Working Papers Series in EU Border Conflict Studies*, Agosto, Número 21. Disponible en:
<https://www.birmingham.ac.uk/Documents/college-social-sciences/government-society/polsis/research/2006/eu-border-conflict/wp21-estonian-russian-border-conflict-and-european-integration.pdf> (Último acceso en enero de 2020)

3.2 ARTÍCULOS DE OPINIÓN

De la Cámara, M. (2008): “Las relaciones entre la Unión Europea y Rusia”, *UNISCI* enero, N. 16. Disponible en
<https://ucm.es/data/cont/media/www/pag-72513/UNISCI%20DP%2016%20-%20De%201a%20Camara.pdf> (Último acceso el 3 abril 2020)

Gómez de Ágreda, Á. (2010): “Global Commons en la era de la incertidumbre”, en J. Ureña, F. (2015) *Ciberataques, la mayor amenaza actual*. Cuadernos de opinión del IEEE. Disponible en:
http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf (Último acceso el 26 de diciembre de 2019)

J. Ureña, F. (2015): “Ciberataques, la mayor amenaza actual”. *Cuadernos de opinión del IEEE*. Disponible en:
http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf
(Último acceso el 3 abril 2020)

Robles Carrillo, M. (2015): “El ciberespacio y la ciberseguridad: consideraciones sobre la necesidad d un modelo jurídico”, *Cuadernos de opinión del IEEE*. Disponible en:
http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO124-2015_Ciberespacio-Ciberseguridad_Margarita-Robles.pdf (Último acceso el 26 de diciembre de 2019)

3.3 ARTÍCULOS DE MEDIOS DE COMUNICACIÓN

El País (2008): “Putin considera una "amenaza directa" la ampliación de la OTAN”, *El País*, 4 de abril.

Manaut, L. B. (2007): “Los cachorros de Vladimir Putin: jóvenes para defender Rusia”, *Deutsche Welle*, 26 de Julio. Disponible en:
<https://www.dw.com/es/los-cachorros-de-vladimir-putin-j%C3%B3venes-para-defender-ru>

sia/a-2707937). Obtenido de <https://www.dw.com/es/actualidad/s-30684>. (Último acceso el 18 de noviembre 2019)

Myers, S. L. (2007): “Russia Rebukes Estonia for Moving Soviet Statue”, *The New York Times*, 27 de abril.

Pons, R. L.-G. (2017): “La batalla del Soldado de Bronce: lecciones del primer episodio de ciberguerra con Rusia”, *El Confidencial*, 2 de octubre.

The Baltic Times (2007): “Forbidden structures”, *The Baltic Times*, 14 de febrero.

4. ARTÍCULOS Y DOCUMENTOS ONLINE

González, A. (2018): “Las Repúblicas Bálticas cumplen 100 años”, *Instituto Español de Estudios Estratégicos, Documento de análisis*.

Mamedov, E. (2004): “Los países bálticos ante su adhesión a la Unión Europea”. *Boletín Elcano* 46:5, ISSN 1696-3326

Revista de la OTAN (1999): “Concepto Estratégico de la OTAN”, Otoño 1999. Disponible en PDF: <https://www.nato.int/docu/rev-pdf/sp/9903-sp.pdf>

Ruiz González, F (2010): “Las relaciones OTAN-Rusia desde la caída del muro de Berlín: La Cumbre de Lisboa”. *Documento de Análisis del IIEE* nº 16/2010. Diciembre, pp.,2.

Stoicescu, K. (2020): “The Tartu Peace Treaty and Estonia’s Eastern Border”, *Diplomaatia*. Disponible en: <https://icds.ee/icds/about/> (Último acceso el 20 marzo 2020)

Yturriaga Barberán, J.A. (2011): “Relaciones entre Rusia y la OTAN: Cumbre de Lisboa. Documento Marco”, *Instituto Español de Estudios Estratégicos*. Disponible en PDF: http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM15-2011Relaciones_Rusia-OTAN_CumbreLisboa_JAYturriaga.pdf

5. ENTREVISTAS

Kash, W. (13 de junio de 2008). Entrevista a Lauri Almann: Lessons from the cyberattacks on Estonia. GCN, Disponible en: <https://gcn.com/articles/2008/06/13/lauri-almann--lessons-from-the-cyberattacks-on-estonia.aspx> (Último acceso el 13 de mayo de 2020)

Bassets, L. (2010): Conversaciones con Javier Solana. Reivindicación de la política, veinte años de relaciones internacionales, Debate.

6. TRABAJOS ACADÉMICOS

Kaiser, R. (2011): *Reassembling the event: Estonia's 'Bronze Night'*. University of Wisconsin–Madison, Geografía. Environment and Planning D: Society and Space 2012.

Kauppara, L. (1999): *The Baltic Puzzle: Russia's Policy towards Estonia and Latvia 1992-1997*. Tesis en Historia Política, Departamento de Ciencias Sociales, Universidad de Helsinki.

Mälkso, L. (2005): *Which Continuity: The Tartu Peace Treaty of 2 February 1920, the Estonian-Russian Border Treaties of 18 May 2005, and the Legal Debate about Estonia's Statue in the International Law*. Análisis académico, *Juridica Int'l*.

Reguera, J. (2015): *Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario*. Grupo de Estudios en Seguridad Internacional, Análisis GESI, 7/2015, Universidad de Granada.

7. PÁGINAS WEB

Council on Foreign Relations. *Cyber Operations Tracker*. Disponible en: <https://www.cfr.org/interactive/cyber-operations> (Último acceso el 12 abril 2020).

e-estonia: Disponible en: <https://e-estonia.com/> (Último acceso el 18 de junio 2020)

NATO Cooperative Cyber Defence Centre of Excellence. Disponible en: <https://ccdcoe.org/> (Último acceso el 12 abril 2020).

NATO Stratcomcoe. Disponible en: <https://www.stratcomcoe.org> (Último acceso el 12 abril 2020).

Página final en blanco