PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS SOCIALES

Conflictos entre la gobernabilidad y la soberanía en organizaciones multilaterales: estudio de la implementación de políticas de seguridad informática entre los años 2004 – 2016 en la Unión Europea.

Tesis para optar el Título de Licenciado en Ciencia Política y Gobierno que presenta:

Oscar Miguel Escalante Terán

Asesor:

Mg. Oscar Vidarte Arévalo

2018

ÍNDICE

RESUMEN

El presente trabajo estudia y analiza las causas de la inexistencia de políticas públicas comunitarias en la Unión Europea que garanticen de manera eficaz la seguridad y gobernabilidad informática tanto de los países miembros como de la organización comunitaria en sí.

Los espacios cibernéticos e informáticos y sus aplicaciones en nuestra vida diaria van en continuo progreso y aumento, cada vez más espacios de nuestra vida cotidiana y, por ende, ciudadana se ven penetrados por el desarrollo tecnológico, cibernético e informático. Esto también supone la participación del Estado como usuario y regulador en su contexto nacional como en el espacio internacional.

El fenómeno tecnológico y su impacto en la política viene siendo analizado en espacios académicos focalizados y la bibliografía especializada en la materia, escaza aún, por ejemplo, ya analiza el uso de herramientas de inteligencia artificial para la definición de la política exterior de los Estados a la par de que actualmente se vienen creando unidades especializadas en las fuerzas armadas de diferentes países ya que se considera al ciberespacio como un área de desarrollo militar como ya lo son el aire, mar y tierra.

En ese contexto, en el que se vienen trasladando temas propios del denominado “high politics” al ciberespacio y sus implicancias, ¿por qué la Unión Europea no ha podido diseñar e implementar políticas públicas comunitarias y eficaces que garanticen la seguridad y gobernabilidad informática?

La presente tesis hace un breve recuento del estado de la cuestión en la materia, así como una revisión cualitativa de los planes y regulaciones comunitarias existentes, así como del estado de avance y desarrollo de la materia en los países hegemónicos y relevantes en el proceso de toma de decisiones en la Unión Europea (Alemania, Francia y Reino Unido).

Los resultados principales obtenidos en la presente investigación, a la luz de la tradición realista de las relaciones internacionales, muestran que la interacción de los intereses nacionales de los países impide un desarrollo comunitario en la materia y, paradójicamente, los expone a mayores vulnerabilidades. Estos intereses se basan en las diferentes concepciones de seguridad que tengan los países como en variables identitarias que tienen un rol trascendente en la determinación de políticas e intereses nacionales y en el cómo se armonizan o no con las políticas e intereses comunitarios.

INTRODUCCIÓN

En años recientes, el creciente acceso a servicios de conexión vía internet en los países desarrollados y en vías de desarrollo, ha generado que diversos aspectos de la vida humana se vean impactados y dinámicas tan como comunes como las relaciones humanas se trasladen a espacios cibernéticos.

La evolución del porcentaje de la población mundial con acceso a internet es una muestra de cuan vertiginoso y profundo ha sido y será este impacto, ya que en 1995 solo el 0.4% de la población mundial tenía acceso a espacios cibernéticos lo que notablemente contrasta con el 51.7% que tiene el mismo acceso en junio de 2017.

Figura elaborada según los datos proporcionador por Internet World Stats

Para el caso europeo, materia de análisis en la presente investigación, podemos evidenciar que el acceso a la red entre el 2010 al 2015 ha tenido un incremento desde el 71% hasta el 80.3%.

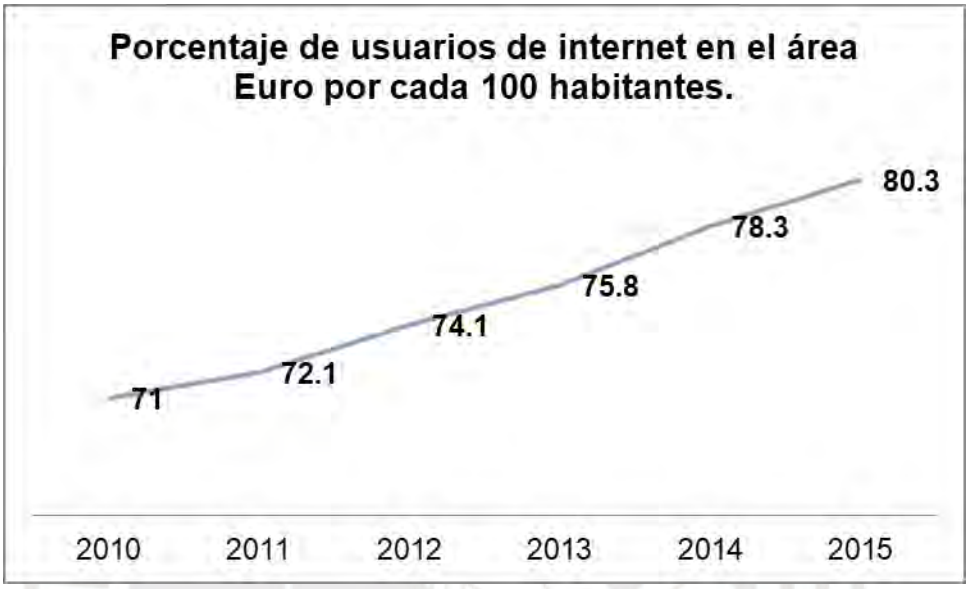

Figura elaborada según los datos proporcionador por UN Data

Es decir, aunque queda pendiente una brecha por cerrar que, conforme se van dando adelantos tecnológicos se puede prever un mayor impacto en la vida de las personas, de la sociedad en su conjunto y, por consiguiente, del Estado, así como de las relaciones persona – sociedad – Estado.

Por ello, no es de extrañar que los Estados, también, se hayan visto influenciados por este fenómeno y, naturalmente, diversos temas tales como la implementación de políticas públicas, la comunicación con los ciudadanos, los procesos de accountability e incluso las interacciones propias de los temas

correspondientes al “high politics”[1] se vienen concretando y estudiando en espacios cibernéticos.

Así, el elemento tecnológico aparece como un escenario en el que se gestan nuevos retos para el Estado y la comunidad internacional en su conjunto ya que se enfrentan nuevas amenazas a la seguridad internacional y la soberanía estatal, diferentes tipos de disturbios en el orden internacional, retos a la gobernabilidad, oportunidades de nuevas formas de integración, entre otros.

Por ello, el internet ofrece una nueva arena para el estudio de las Relaciones Internacionales que la literatura académica al respecto no asume, en totalidad, una perspectiva Estado - céntrica sino que se comienza a propugnar que en el estudio de las interacciones internacionales se debe considerar, también, el análisis de las acciones humanas, individuales y colectivas, con respuestas dinámicas e interconexiones en un sistema social cada vez más complejo en el que se exiten mayores recursos de poder, más espacios de influencia, posibilita una mayor interdependencia económica entre los Estados, pero ofrece a los individuos nuevas formas de asociarse y relacionarse entre sí y con el Estado.

[1] Los términos de "high politics" y "low politics" se enmarcan en el paradigma realista para definir las acciones del Estado en el ámbito internacional. Así, aquello que se corresponde con la supervivencia del Estado (asuntos militares, diplomáticos, seguridad internacional, adquisición de armas, declaración de la guerra, entre otros) reciben la denominación de "high politics" y aquello que no compromete la supervivencia del Estado (como las diplomacia cultural, el comercio exterior, entre otros) les corresponde la categoría de "low politics".

En suma, la aparición de esta nueva arena supone reconocer que existen para las Relaciones Internacionales nuevas oportunidades de competencia, contención y conflicto, por lo que diversos Estados han dictado y/o han intentado planificar e implementar políticas públicas con el objetivo de reducir amenazas, según sus propios intereses. La Unión Europea (UE), por su parte, tampoco ha sido ajena a este proceso.

Si bien la UE, a nivel comunitario, cuenta, desde el 2004, con la European Network and Information Security Agency (ENISA), los diversos Estados miembros han declarado y especificado su propia estrategia a nivel nacional, por lo que cabe preguntarse ¿Por qué, en un escenario que se pretende crear una UE abierta y segura informáticamente, desde el 2004, solo se cuenta con una sola política pública comunitaria en la materia? ¿Por qué, luego de las deficiencias en el diseño institucional evidenciadas en los últimos años, en la ENISA se propone crear una nueva 'Agencia Europea de Ciberseguridad'?

En ese sentido, en la presente investigación observaremos que la inexistencia de políticas públicas comunitarias en la materia se debe, fundamentalmente, a la existencia de conflictos producidos por el ejercicio de la soberanía estatal y la consecuente búsqueda de satisfacción de los propios intereses nacionales, principalmente entre Reino Unido, Francia y Alemania.

Por ello, la investigación parte cuestionando: ¿Cómo funcionan las políticas públicas de soberanía y gobernabilidad informática en la Unión Europea desde el 2004? Y, posteriormente, buscamos responder ¿Cuáles son

las causas de la existencia de estas políticas públicas? ¿Cuáles son sus características? ¿Qué actores están involucrados? ¿Cómo se definen estas políticas en los espacios comunitarios - supranacionales?

Estos cuestionamientos buscan, principalmente, comprender las interacciones entre el libre ejercicio de la soberanía estatal y su impacto en la gobernabilidad informática desde el 2004 en la UE.

Paralelamente, esperamos ofrecer una explicación sobre las causas de la existencia de políticas públicas se seguridad y defensa informática; así como, una descripción de sus características y una identificación de los actores involucrados en los procesos de toma de decisiones de estas políticas (los que toman decisiones, los que influyen en ese proceso y los que son regulados/afectados una vez implementada la política pública).

Las políticas públicas que buscan la seguridad informática de los países son de reciente y constante promulgación, y tienen por objeto ofrecer seguridad frente a la existencia de armas de destrucción masiva, interferencia económica, nuevos crímenes transfronterizos, entre otros.

La paradoja que emerge nos lleva a cuestionar si es que estas políticas públicas buscan generar verdaderamente espacios más seguros, ya que en el caso de la Unión Europea podrían estar suscitándose posibles efectos no buscados y, tal vez, hasta podrían estar produciendo afectaciones a la gobernabilidad comunitaria.

En el desarrollo de la investigación encontramos que el impacto de las innovaciones tecnológicas y su influencia en las interacciones políticas es un tema que se viene estudiando, mayoritariamente, desde casos de acciones ciudadanas y movimientos sociales; sin embargo, la investigación sobre cómo el Estado ha respondido a nuevos retos, por medio de políticas públicas, es aún escaza.

La complementariedad de políticas públicas (en materia de soberanía, seguridad y gobernabilidad democrática) comunitarias y estatales en el espacio geográfico de la Unión Europea permitirá apreciar las relaciones entre los Estados miembros y los órganos comunitarios; es decir, se abordará cómo las relaciones entre los diferentes Estados, en un escenario en el que ninguno desea dejar de lado sus propios intereses, afectan de manera importante el funcionamiento de las organizaciones supranacionales y comunitarias.

Nuestras exploraciones comprobaran que el origen de estas políticas públicas son variadas pero deben resaltarse, en primer lugar, las relaciones de competencia, conflicto y contención entre países; así como las amenazas sociales a la legitimidad de la autoridad difundidas en espacios cibernéticos, y que son identificadas como tales por los Estados; y, finalmente, las conductas antisociales o delitos que pueden darse en estos espacios.

En el transcurso de la investigación encontramos que las políticas públicas analizadas se direccionan según la amenaza a enfrentar, por lo que, y en ese sentido, mientras estas sean de origen estatal se busca competir, defender y proteger, pero en caso las amenazas tengan un origen no estatal se

opta por el control o la regulación de acciones individuales o colectivas en espacios cibernéticos, siendo esto muy frecuente.

Al momento de intentar identificar a los actores involucrados en las políticas públicas de soberanía y gobernabilidad informática, se piensa en los Estados y en los sistemas formales de la UE, pero se olvidan a los proveedores de servicios internet, a los delincuentes transnacionales, a los movimientos sociales/ciudadanos que interactúan constantemente en las redes sociales, entre otros.

El diseño del sistema supranacional de elaboración de políticas públicas en la materia favorece la pugna de los intereses nacionales y la consecuente imposición de aquellos que cuentan con mayores recursos de poder. Estas pugnas, en el caso de estudio, han obstaculizado la concreción pronta y eficaz de políticas públicas y estamos frente a una UE a la deriva en lo referente a seguridad y defensa informática.

Partimos revisando estudios sobre el rol de Europa y el proceso de integración europeo en la configuración de un nuevo orden mundial, siendo una conclusión contemporánea en esta literatura que el modelo de integración de la UE se encuentra fuertemente cuestionado, con muchos actores que señalan su derrota y que presuntamente solo habría servido para que determinados países puedan imponer sus intereses particulares (Torreblanca 2008: 88).

Y es que luego del proceso, conocido popularmente como Brexit, por el cuál se definió, vía referéndum, la salida de Reino Unido de la Unión Europea ha quedado en evidencia de que la UE vive una crisis existencial en sus

diversos alcances. Esta crisis cuestiona profundamente la posibilidad de que, en el marco de la globalización, los países europeos encuentren un método de cooperación que, reconociendo la interdependencia, compagine las diferentes visiones o intereses naciones - estatales (Booth 2016:14).

En materia de seguridad internacional, por su parte, tenemos que la introducción de nuevas amenazas se basa en el traspaso de las fronteras clásicas de la visión Estado - céntrica y la información es un instrumento de guerra por su capacidad de flujo y efecto homogeneizador y se genera un concepto multiforme de seguridad internacional que favorecen agendas de cooperación multilareal (Agozino 2005: 32 - 35 ; De Castro 2008: 56).

Esta agenda multilateral de cooperación se basaría, principalmente, en la búsqueda de una nueva fuente de legitimidad política en tanto la lógica amigo - enemigo no sería suficiente. Por ello, diversos autores mencionan que esta nueva agenda debe basarse en un acuerdo cosmopolita en el marco del derecho internacional usando elementos civiless como complementario a los militares (Kaldor 2010: 283 - 284).

En este escenario, el reconocimiento del ciberespacio como un elemento que permite la transmisión de información a gran escala abre la posibilidad de ver a las herramientas informáticas como un nuevo escenario de interacción estatal, humana, etc.

Por ello, cabe exponer que los elementos informáticos tienen un espacio ganado en la definición de los temas de high politics (a saber: intereses,

valores, seguridad de la información, entre otros) debido a la apertura de espacios para obtener recursos de poder, la proyección de influencias, oportunidades de creación de mercados y la transmisión de información (Choucri, 2012).

Estudios recientes establecen que la apertura de estos escenarios ha llevado que los Estados traten de regularlos por medio de políticas públicas que reduzcan su fragilidad y potencien su capacidad de contener y competir, así como regular y controlar las actividades civiles - ciudadanas en la materia (Choucri 2012: 9 - 10).

En lo referente a las características y actores de las políticas públicas en materia de soberanía informática, segundo tema eje del presente trabajo, tenemos que las políticas públicas en materia de soberanía y gobernabilidad informática se definen por tres tipos de interacciones: el conflicto, la competencia y la contención (Choucri 2012: 5).

El conflicto se refiere a casos de lo que podríamos llama violencia cibernética directa entedidos como ataques digitales dirigidos a Estados, entidades de interés público o usuarios por parte de otros Estados o grupos no estatales. La competencia se vincula a la creación de nuevas fuentes de poder digital para ampliar los espacios de influencia o de soporte para determinados intereses. Finalmente, la contención se refiere de manera directa a la determinación de quién obtiene qué, cuándo y cómo, y aquellos habilitados por los usos del espacio virtual.

Sobre los intereses relevantes e identificables en la elaboración de políticas públicas en materia de soberanía y gobernabilidad informática en la UE, tenemos que los estudios de cooperación internacional demarcan dos tipos de niveles: el nacional y el supranacional. Lo que ha conllevado a la coexistencia de intereses, roles e identidades en los procesos de elaboración de políticas (Lewis 2002: 2 - 3).

Esto, según la literatura estudiada, se da produce porque el diseo institucional ha determinado cómo se han estructurado los debates políticos resultando que las instituciones, incluídas aquellas que se consideran "apolíticas" o "técnicas", generan sus propios interses, agendas y prioridades a pesar de estar controlados por actores políticos como Estados (Peterson y Shackleton 2011: 13- 14).

Así, se producen intereses comunitarios que difieren de las prioridades políticas de los Estados (de todos o algunos) y los debates de políticas, por ello, se reducen a debates entre actores nacionales que persiguen intereses nacionales.

En gran medida, la literatura revisada expone que esta realidad a determinado que las instituciones comunitarias hagan poco por conciliar o integrar los diversos intereses existentes en la Unión Europea sino que determinan políticas según la consideración de cómo los Estados de la UE ayudan u obstaculizan el desarrollo de sus actividades (Peterson y Shackleton 2011:20).

La literatura también señala la naturalidad de que en los procesos de toma de decisiones comunitarios los gobiernos deseen influenciar a la medida de sus intereses. Todos los países miembros han cedido soberanía en favor de los órganos supranacionales correspondientes, pero asumen el costo debido a que los tomadores de decisión y/o amplios sectores poblaciones respaldan el supuesto de que parte de las políticas nacionales comprenden la participación en la elaboración de las comunes (Nugent 2006: 392 - 393).

En ese contexto, desde 1998 se expone un aumento de la cooperación en temas de seguridad, aumento de la capacidad militar de la UE, así como mayor autonomía civil y militar en la resolución de crisis internacionales. Cambios que se dan en el marco del establecimiento de una estrategia europea de cooperación y la creación de la primera fuera militar europea (Wallace 2005).

Wallace (2005) también reporta que desde la firma del Tratado de Ámsterdam, Gran Bretaña y Francia han asumido un notorio liderazgo, al que se suma Alemania desde 1999, lo que les ha facultado orientar sus intereses y políticas supranacionales en casos como los de Kosovo, las relaciones con la OTAN y las guerras de Irak y Afganistán.

En el caso británico, inicialmente se describe un política reticente a la UE, debido, básicamente, a una resistencia a la europeización de Gran Bretaña. Visión que cambia en tanto Blair preconizó que Gran Bretaña podría haber sido la bisagra entre la UE y EE.UU. y que, por tanto, debió jugar un rol importante en la elaboración de políticas de defensa europea (White, 2013).

La visión impulsada por Blair ha sido cuestionada en los últimos años por la frustación que han generado los conflictos entre el funcionamiento de la Unión Europea como espacio comunitario y el ejercicio de la soberanía británica para temas como inmigración, trabajo, entre otros. Esta coyuntura fortaleció a sector euroescépticos del Partido Conservador y conllevaron, por situaciones particulares que se dieron durante la gestión del ex Primer Ministro Cameron, al referéndum por el que se aprobó la salida de Reino Unido de la UE (Torreblanca, 2016).

Francia por su lado siempre ha tenido las pretensiones de ejercer un rol exterior desproporcional a su capacidad y tamaño, por ello habría hecho hincapié en su política y estrategia militar, incluyendo una política nuclear caracterizada por algunos como muy propia de la Guerra Fría. Francia juega un rol importante en las políticas de defensa europeas en tanto es un país que ha buscado influenciar en las operaciones de la OTAN y es parte de su interés nacional influir en los procesos deliberativos supranacionales según los mismos intereses (Treacher 2013).

Desde la reunificación, Alemania ha buscado y es parte de su interés nacional propiciar intervenciones de carácter humanitario además de ser un hegemón natural de Europa central y, por tanto, ha buscado proyectar sus intereses de seguridad y defensa para maximizar su poder institucional al interior de la UE (Harnisch, 2013).

En suma, la literatura estudiada concluiría que los tres países mencionados ejercen de manera directa influencia en las políticas de seguridad

y defensa, según sus propios intereses y ello, como se observará en el desarrollo de la tesis, nos sirve para entender por qué no se han concretado políticas públicas comunitarias eficaces en materia de seguridad y defensa informática.

Nuestro estudio de caso sirve, a su vez, como una comprobación practica de lo expuesto por la tradición realista de las relaciones internacionales y, en consecuencia, usamos este enfoque como un instrumento que nos ayuda comprender por qué la UE no cuenta aún con políticas de seguridad y defensa informática totalmente implementadas.

La tradición realista es útil en la narrativa explicativa de la presente investigación ya que permite explicar por qué los Estados europeos miembros de la UE teniendo una relación de horizontalidad formal, es decir compartiendo la misma estructura (el sistema comunitario), carecen de políticas públicas comunitarias que garaticen la soberanía y gobernabilidad informática por la interacción de los intereses nacionales de los países hegemónicos. Por ello, evaluaremos desde el realismo estructural si es que podríamos augurar un cambio en el sistema de seguridad y defensa europeo.

Cabe recalcar que Waltz también expuso que la interdependencia entre Estados a nivel de una institución internacional si bien generaba condiciones para la paz debido a que multiplicaba los contactos entre ellos, también multiplicaba las ocasiones y circunstancias que incitan a la guerra. Asimismo, el autor expone que mientras mayor interdependencia exista,

menor grado de maniobra tiene un país sin afectar a su socio y, adicionalmente, teoriza que un Estado relativamente independiente tiene mayor fuerza que uno con mayor grado relativo de dependencia (Waltz: 2005: 171 – 173).

Por ello, siguiendo a Waltz, podríamos afirmar que los países bajo el ámbito de acción comunitario viven en condiciones de paz y difícilmente vayan a ir a la guerra entre ellos, pero si se han dado mayor cantidad de conflictos.

Estos conflictos podemos entender que parten desde una visión crítica de la globalización y debates culturales contemporáneos en torno a la inmigración, el sentido de la libertad, la democracia, entre otros, que definen la vida política de cada nación y en los que desde los espacios comunitarios ha tratado de imponerse una visión común.

A la par del concepto de la interdependencia, recogemos lo expuesto por Waltz sobre las organizaciones internacionales en tanto expone que éstas se encuentran limitadas a regular los intereses de sus entidades fundadoras (países impulsores), por lo que tienen escaso efecto independiente (Waltz: 2005: 178).

Es decir, los organismos internacionales están subordinados a los objetivos nacionales de los países fundadores y las funciones de estas organizaciones cambian según sus estructuras originales y a pesar de la estructura burocrática que tengan, son los Estados quienes determinan soberanamente su destino (Waltz: 2005: 179 - 182).

Por ello, en el caso de análisis, se cumple lo expuesto por Waltz en tanto las organizaciones internacionales no responden a fines / objetivos internacionales, sino a los intereses nacionales de los Estados más fuertes (Waltz: 2005: 184).

Stanley Hoffman expuso claramente estas dinámicas definiendo en la década de los sesenta que los procedimientos europeos con intergubernamentales y supranacionales, debido a que el poder real lo detentan los gobiernos de las tres grandes potencias europeas (Alemania, Francia y Reino Unido) en el marco de institucionales centralizadas y amparadas en el derecho comunitario (Salomón 2002: 19).

En resumen, la presente investigación expone y desarrolla, desde la tradición realista con aportes del intergubernamentalismo, que la Unión Europea se encuentra en una situación de indefensión en materia de seguridad y gobernabilida informática debido a las interacciones de los intereses nacionales de los hegemones que impiden el diseño e implementación de una política pública comunitaria en la Unión Europea.

Siendo así, en el primer capítulo revisaremos la importancia que los espacios digitales vienen adquiriendo no solo como síntoma de progreso tecnlógico sino como una nueva fuente de problemas políticos e internacionales que deben ser abordados por la academia con mayor ahinco.

En la segunda parte del presente trabajo analizaremos el estado de las políticas que buscan garantizar la seguridad y soberanía informática en la UE: cómo se diseñan y cuáles son sus alcances y limitaciones.

Finalmente, abordaremos la narrativa explicativa de la hipótesis del presente trabajo exponiendo los planes de seguridad de los grades hegemones europeos (Francia, Alemania y Reino Unido) y el impacto de las interacciones de los diversos intereses nacionales en la posibilidad de diseñar e implementar políticas públicas de seguridad y defensa informática en el marco de posibles cuestionamientos a la legitimidad de la UE en tanto muchas de sus decisiones se entienden como contrarias a la tradición y esencia de la Occidental, sobre la que asienta la cultura europea.

CAPÍTULO 1: LA IMPORTANCIA DE LA SEGURIDAD Y DEFENSA INFORMÁTICA EN MUNDO DE HOY

1.1. Ciberespacio y seguridad informática: una revisión de conceptos.

La presente investigación nos cuestiona sobre la existencia de problemas en la gobernabilidad de la Unión Europea (UE) ocasionados por conflictos resultantes del ejercicio de la soberanía estatal de sus países miembros, principalmente Reino Unido, Francia y Alemania, en materia de políticas de seguridad y defensa informática.

Por ello, es necesario exponer y desarrollar los conceptos que ayuden a una mejor definición e internalización de la naturaleza de la seguridad y defensa informática y las políticas públicas que regulan esta materia; así como, reconocer la existencia de nuevas amenazas a los intereses nacionales producto del contexto en el que se vienen intentando diseñar e implementar este tipo de políticas públicas: la aparición de nuevas tecnologías y las herramientas virtuales.

Entender la correspondencia que existe entre las nuevas amenazas y el contexto señalado permitirá apreciar la relación causal que estos componentes de análisis tienen con el comportamiento final de los países y el organismo internacional en el caso de estudio.

Referirnos a los sistemas informáticos pone en relevancia la existencia de un “espacio físico no real” de almacenamiento de la información, es decir, ya no son grandes bibliotecas o archivos físicos los que sirven para almacenar las cuentas nacionales de los Estados, el posicionamiento de tropas, los registros civiles, entre otros datos, sino que

reconocemos y trabajamos sobre una realidad virtual, no física, que por lo expuesto es vulnerable ante determinadas y, a la vez, múltiples amenazas.

Esto es lo que diferentes autores denominan como "ciberespacio" (Cabero: 1995):

> "*el espacio físico no real en el cual se tiende a desarrollar nuestras interacciones (…) un espacio de comunicación caracterizado por una red de canales de información, que se encuentran organizados de tal forma que toda la información acumulada en cada uno los puntos, se encuentra a disposición de todos los puntos de la red"*

Definimos este concepto debido a que el ciberespacio es el escenario en el cual cobra sentido la seguridad de los sistemas informáticos: es el espacio a regular, es decir, es la nueva arena sobre la cual el Estado va a dictaminar políticas públicas, debido a que aquí se encuentra almacenada toda la información relevante para la satisfacción de los intereses nacionales.

De ahí que la importancia de las políticas públicas de seguridad informática resida en la salvaguarda de la información y del sistema informático, es decir son políticas que abarcan al *"conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que puedan afectar al mismo"* (García-Cervigón y Alegre Ramos 2011: 2).

Por otro lado, la seguridad puede entenderse como la defensa la integridad y privacidad de la información contenida en el sistema informático, garantizar la salvaguarda de los equipos físicos y la seguridad de los usuarios del sistema informático (García-Cervigón y Alegre Ramos

2011: 10); asimismo, puede clasificarse como activa, cuando se intenta detectar amenazas y proveer soluciones a problemas concretas, como los antivirus; y pasiva cuando se toman medidas necesarias para aminorar el impacto de una afectación ya producida a la seguridad de un sistema informático (García-Cervigón y Alegre Ramos 2011: 3,5).

Estas amenazas, fundamentalmente, pueden clasificarse en tres tipos para entender el sentido de las políticas públicas (García-Cervigón y Alegre Ramos 2011: 11):

a. Las amenazas de software como virus, espías troyanos, gusanos, ataques variados vinculados a la existencia de software malintencionado.
b. Las amenazas físicas que abarcan todas las posibles acciones que podrían incurrir en daños causados al sistema informático por razones físicas. Así tendríamos el robo e incendio de equipos, por ejemplo.
c. La amenaza humana correspondiente a usuarios intrusos o no autorizados del sistema informático y a las fallas propias de los usuarios del sistema informático.

La revisión de los conceptos expuestos ayuda a una mejor comprensión de cuáles son los nuevos espacios de regulación por parte del Estado para la disminución de las amenazas y la satisfacción de los intereses nacionales. Los espacios informáticos suponen un nuevo espacio de interacción no físico usado deliberadamente por los Estados en la implementación de su política exterior.

1.2. El Estado frente a la seguridad informática.

El ciberespacio, visto desde las políticas públicas, por tanto, resulta un sistema contingente y jerárquico compuesto por la infraestructura física, los bloques logísticos que soportan el elemento físico, la información almacenada, procesada y transmitida, y los actores que participan de las interacciones propias de este espacio (Choucri 2012: 8).

Es decir, para el Estado resulta un escenario de alto riesgo, debido a factores como la competencia de estándares tecnológicos, la posibilidad de captar recursos humanos capacitados y la constante renovación de las características de las amenazas.

Esta peculiaridad contingente del ciberespacio, a nivel europeo, fue reconocido en la Cumbre de Lisboa de la Organización del Tratado del Atlántico Norte (OTAN), en el 2010, y se acordó incluir a los ciberataques dentro de las preocupaciones estatales y comunitarias en el marco de lo establecido por las Políticas de Seguridad y Defensa de la Unión Europea (Ministerio de Defensa de España 2010: 9).

Ante estos nuevos riesgos, el Estado considera al ciberespacio como un *"quinto dominio de la guerra junto a la tierra, mar, aire y espacio"* (Ministerio de Defensa de España 2010: 13), con lo que la regulación y el cómo se atiende la materia se enmarcan en la preocupación estatal de la seguridad y la defensa.

En el transcurso de la investigación, hemos encontrado que los países diseñan e implementan este tipo de políticas públicas para competir y contenerse mutuamente en escenarios de conflicto; para responder ante

situaciones de amenaza que puedan cuestionar la legitimidad y estabilidad social y política vigente en determinado momento; y para regular conductas antisociales de origen ciudadano, principalmente las correspondiente a los denominados “delitos cibernéticos”.

Paralelamente, los bajos costes de acceso a herramientas tecnológicas y redes de internet, suponen que los individuos, ciudadanos, interactúen de manera mucho más natural, constante y permanente en este quinto dominio de la guerra que se constituye el ciberespacio.

Es por ello, que en materia de derechos humanos, y debido a que *“en el ciberespacio, dichas acciones cobran un cierto carácter de invisibilidad frente al escrutinio público y, por tanto, la aparente inmaterialidad e invisibilidad de los ataques precisa nuevas formas de análisis”* (Bustamante 2010) hoy se intenta teorizar sobre una cuarta generación de derechos humanos que deben ser reconocidos por el Estado y que impactan en la forma cómo se pretende regular esta nueva arena de interacción.

En suma, el Estado pretende y debe regular el ciberespacio en el marco de la seguridad y la defensa, en este caso informática, con el marco jurídico, referente a derechos humanos, que va surgiendo y esquematizándose. Podríamos decir que el ciberespacio supone una materia de regulación en el que la libertad de los sujetos puede verse en entre dicho debido a la respuesta, o regulación, que deben ofrecer los Estados, institución que tutela por las libertades y su ejercicio por parte de los ciudadanos.

Las regulaciones o intervenciones estatales en el ciberespacio se pueden ver de manera gráfica luego de que empresas como Google, Yahoo y Microsoft reportarán, por ejemplo, que entre el 2012 y 2013 el gobierno norteamericano solicitó información de más de 50 mil cuentas o usuarios registrados en sus portales por investigaciones vinculadas a la inteligencia y terrorismo (Prigg 2014).

Existe un nuevo espacio en el que los ciudadanos, personalmente u organizados, interactúan entre sí y con el Estado con capacidad de afectar intereses estatales - gubernamentales de diversa naturaleza y por lo que existe una justificación y legitimidad de la acción estatal en salvaguarda del interés nacional.

1.3. Relaciones Internacionales y seguridad informática.

Por lo expuesto, Choucri identifica, como ya hemos ido adelantando, que el espacio informático o ciberespacio es una fuente de vulnerabilidad estatal constante, ya que posiciona potenciales amenazas a la seguridad nacional y puede producir disturbios en el orden internacional (2012: 1).

La existencia del ciberespacio supone la oportunidad para que ciudadanos, organizaciones, etc., de y en cualquier parte del mundo puedan acceder a bases de datos de Estados, organismos multilaterales, bancos, entre otros, de otra parte del globo.

Así como ciudadanos pueden acceder a datos, los Estados, usando computadoras e internet, pueden controlar remotamente, por ejemplo, aviones y capturar datos relevantes para servicios de inteligencia o atacar objetivos para la satisfacción de sus intereses. Sin embargo, estas

herramientas no son exclusivas para los Estados por lo que los ejércitos y sociedades se exponen a nuevos y mayores riesgos, vía ciberataques: al igual que con las armas convencionales los países occidentales han empezado, en teoría, a tomar medidas internacionales para reducir las probabilidades de ciberguerras (Ministerio de Defensa de España 2010: 15).

La ciberguerra consiste en la existencia de *"ciberataques a ciudadanos, organizaciones, empresas y, hasta, instalaciones críticas de países como plantas de energía química, centrales nucleares o fábricas de diferentes índoles"* (Ministerio de Defensa de España 2010: 15). Este tipo de hechos, se reportan diariamente y con mayor frecuencia en diferentes medios de comunicación[2].

Por ejemplo, por los medios de comunicación nos enteramos que la OTAN sufrió 60% más ataques en el 2016, lo que suponen 500 ataques por mes, de grupos muy activos provenientes de Rusia (Abellán 2017); también se reportaron ataques rusos a correos electrónicos de personal del Ministerio de Relaciones Exteriores de Italia y sus embajadas (Verdú 2017). Reportes periodísticos también nos informaron que Europa fue atacada masivamente siendo Ucrania la mayor afectada dado que su Banco Central advirtió a diversas empresas financieras que un virus estaba creando problemas con bancos y clientes (Pretoff 2017).

[2] Sobre el reporte de los medios de comunicación acerca de ciberataques en el mundo, recomendamos visitar el ranking de los 10 ciberataques más importantes del 2013 elaborado por América Económica. Visita en línea: <http://tecno.americaeconomia.com/noticias/10-ciberataques-que-han-marcado-el-2013>, 30 de Octubre de 2013.

Por todo ello no debe extrañarnos que, por ejemplo, en el 2013, en el Comité de Inteligencia del Senado norteamericano, el entonces jefe de la Oficina Nacional de Inteligencia exponga que la rapidez de los cambios tecnológicos suponen nuevos riesgos y amenazas a los que es cada vez más difícil responder por las nuevas tecnologías digitales (Saiz 2013).

Así, en el análisis de las interacciones entre el ciberespacio y las relaciones internacionales, se establece que nos encontramos frente a un fenómeno creciente, recurrente, muy reciente y de la literatura se deduce que, ante la ausencia de bastos estudios sobre la materia, lo producido puede servir para idear, sobre todo, lo que será el futuro.

Siendo esto expuesto, se reconoce que el ciberespacio, ha demostrado capacidades políticas poderosas porque no solo pone en tela de juicio la permeabilidad de las fronteras sino visibiliza la ambigüedad de los controles actuales sobre quién transmite información, qué tipo de información transmite, cuándo, cómo y qué efectos tiene esa transmisión. Ante la inexistencia de control, por tanto, se discute a nivel de políticas públicas sobre un espacio a regular que aún es considerado como un espacio libre limitado por los esfuerzos de los Estados para controlar, de sobremanera, los contenidos que se transmiten (Choucri 2012: 51).

Asimismo, para reconocer los impactos del ciberespacio en las relaciones internacionales se parte, en una primera instancia, por exponer qué países tienen mayores niveles de conectividad mundial y, para nuestro caso de estudio, la data sería la mostrada a continuación (Internet World Stats):

Usuarios conectados a internet en la Unión Europea				
Unión Europea – países	Población	Usuarios de internet	Penetración	% Usuarios respecto de la UE
	(2017 Est.)	2017	(2017 - % Population)	2017
Alemania	80636124	72290285	89.6	16.67
Austria	8592400	7273168	84.6	1.68
Bélgica	11443830	10060745	87.9	2.32
Bulgaria	7045259	4213065	59.8	0.97
Chipre	1187575	901369	75.9	0.21
Croacia	4209815	3133485	74.4	0.72
Dinamarca	5711837	5534770	96.9	1.28
Eslovaquia	5432157	4629641	85.2	1.07
Eslovenia	2071252	1563795	75.5	0.36
España	46070146	40148353	87.1	9.26
Estonia	1305755	1196521	91.6	0.28
Finlandia	5541274	5125678	92.5	1.18
Francia	64938716	56367330	86.8	13.00
Grecia	10892931	7525926	69.1	1.74
Hungría	9787905	7874733	80.5	1.82
Irlanda	4749153	4453436	93.8	1.03
Italia	59797978	51836798	86.7	11.95
Letonia	1944565	1663739	85.6	0.38
Lituania	2830582	2399678	84.8	0.55
Luxemburgo	584103	569442	97.5	0.13
Malta	420521	334056	79.4	0.08
Países Bajos	17032845	16143879	94.8	3.72
Polonia	38563573	28267099	73.3	6.52
Portugal	10264797	7430762	72.4	1.71
Reino Unido	65511098	62091419	94.8	14.32
República Checa	10555130	9323428	88.3	2.15
Rumania	19237513	12082186	62.8	2.79
Suecia	9920624	9216226	92.9	2.13
Total Unión Europea	506279458	433651012	85.7	

Cuadro elaborado según los datos proporcionados por Internet World Stats

Las estadísticas de conectividad a internet en los países de la Unión Europea confirman que los países que estudiaremos tienen los tres porcentajes más altos de usuarios conectados a internet, por ello tienen mayores intereses en regular y/o liderar los debates en torno a las regulaciones comunitarias en materia de seguridad informática.

Podemos afirmar que el proceso por el cual se han comenzado a ver temas de high politics en espacios cibernéticos reside en el incentivo que genera a los Estados el incremento de la cantidad de usuarios conectados para desplegar su soft power.

Asimismo, los escenarios cibernéticos constituyen una nueva arena de interacción que es fuente de conflicto, ventana de capacidad y oportunidad de negociación; también impulsan la necesidad de gestar mecanismos institucionales para controlar los flujos de información y control remoto de determinadas infraestructuras, etc.

Así, el ciberespacio es un escenario a estudiar para las relaciones internacionales porque su existencia constituye un elemento a tener en cuenta por los Estados para diseñar e implementar la política exterior y, además, sirve como herramienta para buscar la prevalencia de determinados intereses nacionales.

Los ataques cibernéticos de Estado a Estado; el espionaje electrónico; la difusión de información vital, relevante y considerada secreta para el interés nacional y de seguridad por determinados Estados; conlleva que en este nuevo escenario sea posible observar choques de poder,

relaciones de dependencia, entre otros, que revelan la necesidad de estudiar lo cibernético desde las relaciones internacionales.

Por ello, como bien sugiere Choucri, pareciese que los Estados están definiendo que en los espacios cibernéticos se encuentran ante amenazas que pueden ser individuales, económicas, etc., y, por ello, van incluyendo estas dimensiones en sus consideraciones de "amenazas del siglo XXI" (2012: 70).

1.4. Gobernabilidad y soberanía informática.

La discusión sobre gobernabilidad y soberanía informática la entendemos desde el debate en torno a una sociedad civil global, ya que se conceptualiza en el contexto de la globalización el rol preponderante que las nuevas tecnologías han adquirido en los procesos de integración y como esto ha generado tensiones para la soberanía de los Estados y la gobernanza global por las nuevas amenazas que ofrece (De Castro Sánchez 2010: 55 – 56).

La sociedad civil global es una concepción que surge en el marco de la interconexión contemporánea de los Estados y al aumento del flujo de personas, movimientos, grupos, redes, plataformas que se han involucrado en debates públicos de manera transnacional. Esto posibilita que, si bien el Estado mantenga la titularidad de la soberanía en las relaciones internacionales, existan nuevos actores globales que también tienen capacidad de decisión y presión sobre los Estados (Kaldor 2010: 207).

Así, podemos entender que la gobernabilidad no es un concepto nuevo. Comprende que *"los gobiernos cumplan mejor sus tareas de agregación y dirección"*, es decir, puede entenderse en la dirección de que los Estados

hagan más con menos, y el hacer más implica ofrecer servicios y garantizar su efectivo cumplimiento (Canales 2001:38).

La “gobernabilidad informática” supone, por tanto, que los Estados implementen de manera efectiva políticas públicas que resguarden la seguridad y defensa informática dentro de su jurisdicción. Esta visión la tomamos desde la Gobernanza de Tecnologías de Información que busca la gestión eficiente de recursos tecnológicos y la reducción de los riesgos inherentes a la tecnología informatica (Comín 2005: 14).

La “soberanía informática” se debe decir que corresponde al debate sobre el ejercicio del poder y control del Estado en la arena cibernética, ya que implica: manipular el acceso al sistema informático, regular contenidos, manejo de la información, regulación del acceso ciudadano, independencia de la infraestructura; en suma, tener un real dominio de lo cibernético en función de la protección de su propia información valiosa (Choucri 2012: 133 – 134).

Ambos conceptos son expuestos, mencionados y acoplados por los planes de seguridad de la UE, Reino Unido, Francia y Alemania. Pero, ¿cuál es el debate actual en torno a la gobernabilidad de la Unión Europea? ¿Estos debates ayudarían a entender más aún la naturaleza del problema? Nosotros creemos que sí, ya que a raíz de la crisis del euro, los debates en torno a la unidad de la UE apuntan a cómo lograr una unidad política, es decir avanzar a mayores niveles de integración comunitaria.

Como reconocen Nicolas Berggruen y Nathan Gardels, el debate en el escenario post crisis del euro, gira en torno a que *“ha llegado el momento de*

mirar más allá del horizonte inmediato y empezar a pensar en cómo podrían ser las nuevas instituciones de Gobierno de una unión política".

¿Qué implica para estos autores proyectar instituciones de Gobierno comunitario? Pues, *"la puesta en común de soberanía en una unión política debe centrarse en limitar el poder de un Gobierno federal europeo a la tarea de garantizar los bienes públicos europeos necesarios -como la coordinación macroeconómica, las infraestructuras comunes y los asuntos exteriores- y dejar la mayoría de las demás funciones, desde la educación y las políticas culturales hasta la flexibilidad a la hora de decidir los objetivos fiscales de cada Estado, a las naciones-estado soberanas"*.

El reconocimiento de estos autores y especialistas de considerar los asuntos exteriores y, en consecuencia, la seguridad como un bien público europeo sobre el cual se necesita mayor integración refuerza y valida nuestro punto de partida: la seguridad informática y sus aplicaciones internacionales no serán eficientes si no se avanza hacia mayores niveles de integración y coordinación comunitaria, es un reto para el futuro mediato de la Unión Europea.

Berggruen y Gardels, también han expuesto de manera importante que la evolución de la democracia supone, necesariamente, equilibrar el poder que otorga la difusión del uso ciudadano de las redes sociales y la autoridad legítima de gobierno (Berggruen y Gardels, 2012: 125).

Pero, ¿por qué confluir a este equilibrio? Principalmente, porque sin ningún tipo de esfuerzo en este sentido, la democracia directa que conllevan

las redes sociales, por si sola, no reforzaría la gobernanza sino que, por el contrario, la dificultaría (Berggruen y Gardels, 2012: 135).

La solución planteada por los autores es establecer un modelo de gobernanza en el que se reconozca la complejidad y diversificación de los participantes, pero generando estructuras para el ejercicio legítimo de la autoridad y espacios para la generación de debates y consensos públicos (Berggruen y Gardels, 2012: 141).

Con los conceptos expuestos, consideramos poner en relieve la nueva realidad a la que se enfrentan los Estados: el ciberespacio, conformado por la interconexión de sistemas informáticos. El cómo se ha regulado esto ha sido poco estudiado en la literatura académica y, más aún, su estudio como caso para explicar las tensiones en organizaciones internacionales es aún escaso y casi nulo.

Es innegable que la realidad informática actual supone retos para la sociedad democrática y, más aún, su regulación por parte de organizaciones supranacionales como la UE conlleva fricciones como las que describiremos en capítulos posteriores entre el multilateralismo y la soberanía de cada Estado.

Es necesaria mayor unidad política y de gobierno de la UE, ya que, como veremos en el desarrollo de capítulos subsiguientes, para establecer espacios multilaterales que garanticen la gobernabilidad y soberanía informática de los Estados se requiere mayor integración, coordinación y cooperación comunitaria.

CAPÍTULO 2: SEGURIDAD Y DEFENSA INFORMÁTICA EN LA UNIÓN EUROPEA (UE)

2.1. Intento de implementación de políticas: repaso histórico del tratamiento comunitario en la materia.

La regulación comunitaria en materia informática empieza en 1999, siendo el primer elemento de regulación comunitaria la firma electrónica mediante la Directiva 1999/93/CE. Los objetivos comunitarios de regulación de la firma electrónica eran comerciales.

Hacia 1999 se buscó una libre circulación de mercancías al interior de la UE y la regulación de la firma electrónica mediante la creación de servicios de certificación; esto suponía garantizar un espacio seguro de libre circulación comercial electrónico, reconociendo que el desarrollo del internet y demás herramientas informáticas desmontan las barreras geográficas para el libre tránsito de bienes y servicios (Directiva 1999/93/CE).

Un segundo hito de la regulación se enmarca en la Directiva 2000/31/CE que determinaba algunos aspectos jurídicos del comercio electrónico. Así, reconociendo el proceso de integración europeo, comunitariamente se declaraba que la ausencia de regulaciones jurídicas en la materia imposibilitaba el libre tránsito de bienes y servicios para el comercio electrónico en el mercado interno europeo.

Además, en estos años, no se buscaba sintetizar una legislación uniforme a nivel comunitario, sino que, por contrario, solo se buscaba armonizar criterios para que cada Estado dictaminara la legislación que considerará pertinente sobre la materia.

El año 2002 es el más fecundo en torno a la producción de regulaciones comunitarias en materia de seguridad y defensa informática. Así, se publicaron la Directiva 19/2002/CE, la Directiva 20/2002/CE, la Directiva 21/2002/CE, la Directiva 22/2002/CE y la Directiva 2002/58/CE.

Estas normas, a nuestro parecer, van abriendo camino en la búsqueda de regulaciones comunes y no solo hacia la armonización de criterios como se hizo hasta el 2000. Asimismo, estas directivas son la antesala a la creación de la Agencia Europea de Seguridad de las Redes y la Información (ENISA, por sus siglas en inglés) como agencia comunitaria para regular la materia en la UE.

La Directiva 19/2002/CE refiere a la interconexión de redes informáticas y también con un trasfondo comercial, ya que buscaba asegurar la interconexión de redes a nivel transfronterizo con el objetivo de garantizar la integración del mercado interno europeo sin impedimento a las empresas para negociar la interconexión de sus redes.

Por su parte, la Directiva 20/2002/CE buscaba establecer criterios para los servicios de autorización de redes y servicios de comunicaciones electrónicas en atención a la seguridad, salud y orden público, introduciendo de modo declarativo ya la necesidad de unificar medidas y regulaciones en la materia.

Posteriormente, la Directiva 21/2002/CE es la “Directiva Marco” para establecer un marco regulador común a los servicios de redes y comunicaciones electrónicas. La Directiva 22/2002/CE es una continuación y establece los derechos de usuarios de los servicios de redes y comunicaciones

electrónicas y, finalmente, la Directiva 2002/58/CE establece el marco regulatorio específico para la ordenación de la protección de datos personales en los servicios de redes y comunicaciones electrónicas.

Como se ha podido observar, las regulaciones comunitarias al ámbito informático han sido progresivas: empezaron con la búsqueda de establecer criterios comunes para que cada Estado establezca regulaciones propias, con un fundamento comercial, hacia el establecimiento de marcos regulatorios comunitarios que abrieron una ventana de oportunidad para establecer una agencia especializada en la materia.

Del trasfondo comercial se ha pasado a entender la regulación de lo cibernético desde una perspectiva de la seguridad y la defensa. Así se entiende la creación de una agencia comunitaria especializada: los intereses comerciales ya buscaban introducir garantías de seguridad al intercambio de bienes y servicios, es decir buscaba prevenir lo que hoy entendemos como delitos informáticos (suplantación de identidad, derechos de información personal, entre otros).

2.2. Creación de la Agencia Europea de Seguridad de las Redes y la Información (ENISA).

Por lo expuesto, entendemos que el ciberespacio y los sistemas informáticos se constituyen como un nuevo espacio de regulación para los Estados. Cada uno diseñará e implementará políticas públicas, en el sector de seguridad y defensa, para proteger sus sistemas informáticos.

Esto quiere decir que los Estados buscarán tanto proteger sus sistemas informáticos como obtener información de los sistemas de otros países con el

objetivo de concretizar sus intereses nacionales. Estos esfuerzos nacionales, en el caso europeo, suponen también que un organismo comunitario, como la Unión Europea (UE), regule, es decir diseñe e implemente políticas públicas de carácter comunitario (de aplicabilidad a los países miembros), para la seguridad y defensa informática comunitaria.

En ese sentido, en el año 2004, por medio del Reglamento (CE) No 460/2004, emitido por el Parlamento y Consejo Europeo, se creó la Agencia Europea de Seguridad de las Redes y la Información (ENISA).

La norma de creación de la ENISA, declara y reconoce que las redes y los sistemas informáticos se han convertido en un factor de desarrollo económico y social, y constituyen elementos vitales como los suministros de agua y electricidad, por lo que existe una preocupación comunitaria por la seguridad informática como un elemento adicional que define el bienestar del ciudadano europeo.

La ENISA, como agencia europea comunitaria, es la encargada de velar por la gestión de la seguridad de los sistemas informáticos y tiene como objetivo liderar el debate público para el diseño e implementación de políticas públicas comunitarias. Esto, debido a que, entre sus funciones tiene que proporcionar al Parlamento y la Comisión Europea, así como a los países de la UE, información sobre los riesgos informáticos existentes y prestarles asesoramiento en la materia facilitando la cooperación entre la Comisión Europea y los países miembros de la UE (Europa 2013).

Asimismo, la ENISA debe velar por los riesgos a los que están expuestos los usuarios europeos y buscar la cooperación entre el sector

público y privado para la gestión de esos riesgos y mantener espacios informáticos seguros (Europa 2013).

En tanto regulación, la UE, mediante el Reglamento (CE) No 1007/2008 y el Reglamento (UE) No 580/2011, modificó la duración de la ENISA, extendiéndola hasta Septiembre de 2013; por medio del Reglamento (UE) No 526/2013 se extiende la duración de la agencia hasta el 2020, fecha en la seria reemplazada por la Agencia Europea de Ciberseguridad, esta nueva entidad tendría como misión colaborar a los Estados miembro en la lucha contra ciberataques así como crear un régimen europeo de certificación para garantizar la seguridad de productos y servicios digitales (Comisión Europea 2017).

Asimismo, en el último Reglamento citado la UE redefine la agencia como una organización comunitaria que *"debe llevar a cabo las tareas que le confieren los actos jurídicos de la Unión en el ámbito de las comunicaciones electrónicas (para) contribuir a un elevado nivel de seguridad de las redes y de la información en la Unión (…)"* (Reglamento (UE) No 526/2013).

¿Por qué es importante tener presente a la ENISA? Porque su creación es la primera respuesta europea comunitaria para la regulación de los sistemas y redes informáticas. Como ya hemos observado, anterior a eso solo encontramos un conjunto de normas comunitarias declarativas, es decir que solo expresaban qué se buscaba y qué debía hacerse, o que regulaban aspectos comerciales, especificamente.

Se debe tener consideración que la creación de la ENISA es una política pública en sí misma: la UE responde así ante la necesidad de intervenir en

espacios cibernéticos garantizando la gobernabilidad comunitaria y las soberanías informáticas estatales.

A pesar de que la ENISA no haya contribuido a diseñar e implementar una política pública concreta a nivel comunitario europeo, ha ido generando estrategias. La de mayor impacto para nuestros días es la Estrategia Europea de Ciberseguridad del 2013 -2016, ya que ha dado origen a la primera normativa comunitaria de regulación del ciberespacio en europa dando mandato y plazo a los países para generar normativas nacionales e identificando puntos críticos, proveedores esenciales, entre otros alcances que serán detallados en el desarrollo de la presente sección.

2.3. Límites y alcances del sistema de seguridad y defensa informática.

Entender cómo funciona de manera formal la ENISA es parte medular de la presente investigación, ya que en el próximo capítulo veremos cómo los intereses nacionales han interactuado en la estructura formal de funcionamiento de la agencia encargada de producir el marco regulatorio comunitario a nivel de seguridad y defensa informática.

El Reglamento (UE) No 526/2013, en sus Secciones 2 y 3, establece el proceso de toma de decisiones de la ENISA. La agencia cuenta con un Consejo de Administración, un Director Ejecutivo y un Grupo Permanente de Partes Interesadas. Asimismo, el Consejo de Administración nombra a un Comité Ejecutivo para la eficiencia del funcionamiento de la ENISA.

El Consejo de Administración, compuesto por un representante con derecho a voto de cada país miembro de la UE, tiene como misión velar y garantizar que la agencia cumpla con los fines que se le han sido asignados

comunitariamente, aprobando sus planes anuales, plurianuales, los planes y programas, regulación de intereses, nombra al Director Ejecutivo de la agencia, entre otros.

El Comité Ejecutivo, nombrado por el Consejo de Administración, tiene como única función la implementación de los planes administrativos y presupuestarios aprobados por el Consejo. Los miembros del Comité Ejecutivo y del Consejo de Administración tienen un mandato de 4 años renovables en sus puestos.

La ENISA es gestionada por un Director Ejecutivo, nombrado por el Consejo de Administración; este Director está encargado de gestionar los planes presupuestarios de la agencia, la implementación de los planes de trabajo, pero también del seguimiento de las políticas de seguridad y defensa informática en los países europeos. Asimismo, la Dirección Ejecutiva debe garantizar la independencia de la ENISA frente a cualquier interés que no sea el comunitario.

El Grupo Permanente de Partes Interesadas es un reconocimiento formal de los actores relevantes para las políticas públicas de seguridad y defensa informática.

Este Grupo está compuesto por representantes de *"la industria de las TIC, proveedores de redes o servicios de comunicaciones electrónicas abiertos al público, grupos de consumidores y expertos académicos en seguridad de las redes y de la información, y representantes de las autoridades nacionales de regulación"* (Reglamento (UE) No 526/2013), tiene como función el asesoramiento a la agencia para la concreción de sus planes y medidas;

siendo el Consejo de Administración su mayor órgano de gobierno, con representación de todos los países y responsabilidad de nombrar al Director Ejecutivo.

A su vez, el Director Ejecutivo implementa y concreta los objetivos de la ENISA, y, por su parte, el Comité Ejecutivo se encarga de la gestión administrativa y presupuestaria de la agencia. Teniendo, además, un Grupo Permanente de Partes Interesadas como asesor a la agencia y representando a todos los actores relevantes e involucrados o afectados por las políticas públicas de seguridad y defensa informática.

La estructura organizativa de la ENISA comprueba que las organizaciones internacionales son poco independientes debido a que, como sostiene Waltz, son los países los que determinan lo que verdaderamente será regulado por un organismo internacional (Waltz: 2005: 178).

El Consejo de Administración está compuesto por un representante de cada país miembro, por lo que la incapacidad demostrada por la ENISA para proponer y liderar el debate público comunitario para diseñar e implementar políticas públicas de seguridad y defensa informática depende de los intereses de todos los países: la UE ha creado una agencia para regular lo cibernético pero los países miembros, por la interacción de sus intereses, hacen que este organismo no funcione como debe a cabalidad.

Es decir, la Unión Europea, en tanto organismo internacional, está supeditada a los intereses de los países miembros, estos determinan, por decisión o indecisión, si es que la ENISA cumple o no sus funciones (Waltz: 2005: 179 - 182) y, en nuestro caso, son los Estados miembros quienes vienen

soberanamente determinando políticas de seguridad y defensa informática, afectando la gobernabilidad comunitaria informática.

Se debe considerar también que la Agencia lleva a cabo sus actividades ajustándose a los planes anuales o multianuales aprobados por el Consejo de Administración, recayendo en el Director Ejecutivo, con apoyo del Comité Ejecutivo, la responsabilidad de proponer los contenidos de los planes al Consejo.

El Consejo de Administración aprueba los planes para la agencia luego de haber obtenido el visto bueno de la Comisión Europea y de haber verificado que cumplen con los objetivos de la agencia. Finalmente, es el Director Ejecutivo quien deberá exponer, una vez aprobado, el plan de trabajo de la agencia ante el Parlamento Europeo, el Consejo y Comisión Europeo y ante los Estados miembros que así lo requieran.

En materia de normativa comunitaria aprobada, se debe mencionar la Estrategia Europea de Ciberseguridad (EEC) emitida en el 2013, que estableció pilares claros de trabajo y desde la que se dio origen, tres años después, a la primera normativa comunitaria en nuestra materia de estudio: la Directiva (UE) 2016/1148, del 6 de Julio de 2016, denominada la “Directiva NIS”.

Los pilares de la EEC del 2013 (Comisión Europea 2013) y su satisfacción son cuestionables, y esa evaluación, creemos, contribuye a reforzar nuestra explicación en torno a los grados de indefensión de europa en materia de seguridad y gobernabilidad informática.

A saber, los pilares fueron: lograr ciberresilencia, reducción de la ciberdelincuencia, desarrollar estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD), el desarrollo de recursos industriales y tecnológicos de ciberseguridad y el establecimiento de una política internacional coherente del ciberespacio para la UE.

Para evaluar la tesis expuesta en la presente investigación, abordaremos la evaluación de algunos de los pilares expuesto, aquellos que permiten evidenciar claramente la lentitud o inacción o insatisfacción de la seguridad y gobernabilidad informática en la UE.

Siendo así, en torno a lograr la ciberresilencia o la administración de riesgos a través de la cooperación internacionales dado el carácter transfronterizo de las amenazas informáticas. El fundamento de este pilar era garantizar la seguridad del mercado interior y elevar los estándares de seguridad interna de la UE.

¿Se ha logrado ello? ¿Por qué no se ha dado? A pesar de que en el marco de este pilar estratégico se vienen desarrollando ejercicios conjuntos de contención de ciberamenazas (cada dos años y denominados “Ciber Europa”), y de que en el 2011 se desarrollo el primer ejercicio EE.UU. conjunto con la UE denominado “CiberAtlántico”, los índices y reportes de ciberataques han demostrado la vulnerabilidad europea en la materia cuestionando la efectividad del cumplimiento – satisfacción de este primer pilar.

Por ejemplo, España ha sido víctima de más de 100 mil ataques en el 2016, el doble de los registrados en el 2015 y cinco veces más que los del 2014. De los ataques registrados en este país europeo se tienen afectaciones a

los servicios de Telefónica y una multiplicación por siete a infraestructura críticas en los últimos dos años, es decir aquellas que proveen servicios ciudadanos y públicos y de las que pueden impactarse económicamente hasta llegar a la pérdida de vidas humanas (El País 2017; EFE 2017; Gálvez 2017). También se debe tener en cuenta, en este mismo punto, los 25 centros de salud que fueron afectados por ciberataques, de los cuales 16 fueron dejados sin funcionamiento, en Reino Unido (Muñoz 2017).

Es decir, en palabras de Luis Jiménez Muñoz, subdirector general del Centro Criptológico Nacional (CCN), organismo adscrito al Centro Nacional de Inteligencia (CNI) dedicado a la ciberdefensa en España: vivimos en una ciberguerra diaramente. Estos actos se corresponden con el robo de información, desestabilización, entre otras agresiones que pasan inadvertidas dado que suceden en un espacio intangible y que si se dieran en clásicos términos físicos desencadenarían conflictos internacionales constantes e impredecibles (Carretero 2017).

La ciberdelincuencia es otro factor que lleva a evidenciar la vulnerabilidad europea en torno a la seguridad informática, por ejemplo, el Informe sobre la lucha contra la ciberdelincuencia del 2017, expone que en el 2016 los ataques a los servidores de la Comisión aumentaron en un 20% respecto del año anterior (Parlamento Europeo 2017).

El último reporte de EUROPOL (2017) referido a los crímenes informáticos expone que:

> *"Europa del Este se identifica como una fuente clave de malware ATM (…) Europa también es un objetivo clave para los ciberataques y fraudes con motivación financiera. En segundo lugar, solo después de los EE.*

> *UU.. Reino Unido informa el mayor número de fraudes BEC (más del 9,5%). Francia y Noruega también ven una proporción notable de estos ataques, cada uno sufre más del 2% de los ataques globales. Alemania, Italia, los Países Bajos y el Reino Unido también representan una pequeña pero notable proporción de detecciones de ransomware globales (16% combinadas). Alemania y Rusia se identifican como objetivos clave para el malware bancario.*
> *El Reino Unido sufre la segunda mayor cantidad de infracciones de datos a nivel mundial, aunque distante segundo lugar de los EE.UU.. Alemania e Irlanda también figuran en una lista global de los 10 principales."* (EUROPOL 2017)

Es decir, si bien Europa se consigna como uno de los lugares en el que hay menos ataques a computadoras personales, está presente en los rankings (vía algunos países) de ocurrencia de algunos cibercrímenes.

Las estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD), así como al Plan de Acción Europeo de Defensa (PAED), contemplan intensificar progresivamente el desarrollo de políticas tendientes a la seguridad informática.

Esta progresividad se evidencia en que el PCSD contempla el desarrollo del elemento cibernético y expone que, actualmente, viene siendo más desarrollado en cooperación con la OTAN con el objeto de evitar la duplicación de esfuerzos. Por su parte el PAED contempla la creación de un fondo europeo para la defensa y desde ahí se establece la necesidad de innovación tecnológica y, uno de los elementos a desarrollar, es la ciberdefensa (UE – OTAN 2016; Legrand 2017; European Commission 2017, Comisión Europea 2017).

Sobre la base de este documento y sus respectivos pilares expuestos, es que en el 2016 se emitió la primera normativa comunitaria en torno a la seguridad informática dado que la inexistencia de una política para la

ciberseguridad o que este se encuentre fragmentada hace o mantiene vulnerables a todos los países de la UE; ante esto es que se promulgaría la Directiva 2016/1148 conocida como Directiva NIS - Network and Information Systems (Moret 2017).

La normativa busca establecer un régimen europeo de ciberseguridad a través del incremento de los niveles comunes de seguridad, haciendo que estos, a su vez sean acreditados. Se establece, asimismo, que los países miembros tienen 21 meses para adecuar sus normativas nacionales y seis meses para la identificación de los proveedores de servicios esenciales, reforzando la necesidad de alianzas público privadas para las políticas de seguridad informática (Moret 2017; DIRECTIVA (UE) 2016/1148).

Asimismo, se crea un Grupo de Cooperación coordinado por la ENISA para asesorar a los países en el desarrollo de sistemas y herramientas de ciberseguridad haciendo hincapié en la naturaleza transfronteriza de la seguridad informática para generar una cultura de seguridad fundamental para la economía y sociedad de cada país miembro de la UE (Mendoza 2016).

Esta normativa, al ser la primera de carácter comunitario y dictada 12 años después de creada la ENISA, en su forma y fondo perfila que el proceso formal para el establecimiento de políticas concernientes a la ciberseguridad están condicionadas a nivel interno por la interacción de los intereses nacionales, como veremos en el siguiente capítulo, haciéndolo lento en comparación con la velocidad en la que se producen ciberataques y con la que otros actores internacionales, que compiten con la UE, avanzan en la implementación de políticas que usen tecnológicas digitales.

Asimismo, se debe señalar que esta primera norma se emite en un contexto de grandes desafíos y afectaciones concretas a la seguridad y gobernabilidad informática de la UE: la urgencia de contar con espacios de seguridad informática ha desbordado lo importante, diseñar e implementar políticas comunitarias eficaces en la materia; estos son los primeros pasos en un contexto de cuestionamientos a la UE misma.

Por ello, creemos que la toma de decisiones en la ENISA expone a la organización a la indecisión y la no concreción de políticas públicas comunitarias y, en ese sentido, hace falta que posea mayor independencia respecto de sus fundadores y posea mayor capacidad de generar e imponer un interés europeo, comunitario, en la materia.

Con lo expuesto, hemos dilucidado los mecanismos formales por los cuales consideramos se imposibilita la toma de decisiones comunitarias en materia de seguridad y defensa informática, también evidenciamos la demora en el establecimiento de regulaciones comunitarias porque los Estados así lo desean, y, finalmente, exponemos la justificación del presente estudio: la correlación existente entre la interacción de intereses nacionales en el ámbito comunitario europeo para explicar lo descrito en las primeras líneas de este párrafo.

CAPÍTULO 3 LOS CONFLICTOS ESTATALES Y COMUNITARIOS EN ESCENA

Con la presente investigación hemos podido observar que ante un índice creciente de desarrollo en los países se evidencia un mayor uso de sistemas informáticos y comunicativos.

El uso de estos sistemas en el Estado y el consecuente almacenamiento de información estatal, crucial para la satisfacción de los intereses y objetivos estatales, conlleva la responsabilidad de los organismos públicos de protegerse ante cualquier tipo de intrusión, manipulación, interrupción de los sistemas, puesto que afectaría a millones de personas.

Sin embargo, los países no solo se han propuesto posiciones de defensa, sino que, también, tienen interés en proponer al sistema internacional cómo debe ser tratado esta materia, siempre respondiendo a sus intereses nacionales. Es decir, la comunidad internacional busca ordenar el caótico espacio cibernético y, en gran medida, ello pasa por implementar políticas de seguridad informática, pasiva y activa, con capacidad de armonizar la búsqueda soberana de la satisfacción de los intereses nacionales con la necesidad de cooperación para construir espacios de interacción política internacional seguros.

3.1. Planes de seguridad y defensa informática: casos de Reino Unido, Alemania y Francia.

En el recorrido de la investigación comprobamos que la ciberdefensa, enmarcada en las políticas de seguridad y defensa, es un tema de vital importancia para la seguridad nacional de los Estados. Esta, a su vez, se

compone por el conjunto de medidas que, respetando los derechos y libertades fundamentales, en coordinación entre el sector público y privado, tienen por objeto proteger los sistemas informáticos del Estado (Pastor, Pérez, Arnáiz y Taboso, 2009: 11 – 12).

Europa no ha sido ajena a esta realidad y, por ello, como hemos observado se vienen realizando esfuerzos para concretar medidas comunitarias para hacer frente a estas amenazas.

Asimismo, dentro del escenario europeo, Estonia ya ha sido, en el 2007, blanco de ciberataques (que conllevaron a la toma de medidas por parte de la OTAN) por parte de hackers rusos. Lo que conllevó a una basta reforma que apostaba por crear una política pública concreta, efectiva y considerada como modelo dentro de la UE y la OTAN; el ex Presidente Toomas Hendrik, resopnsable de la transformación digital del país es hoy académico de la Universidad de Stanford y del Foro Económico Mundial (O'Kuinghttons 2017).

También, a nivel de ciberataques ocurridos en Europa, en el conflicto armado entre Georgia y Rusia, hacia el 2008, se registraron ciberataques rusos, previos a la invasión terrestre, para debilitar las infraestructuras básicas de Georgia (Pastor, Pérez, Arnáiz y Taboso, 2009: 16).

Estos reportes se suman a los ya mencionados en secciones anteriores del presente trabajo: ataques en España, al servicio de salud británico, a los servicios digitales de la Cancillería Italiana, entre otros, y demuestran, por el caso de Estonia y la propuesta de creación de una milicia digital en España (Gómez 2017), que la respuesta es aislada y fracturada, lo que refuerza la vulnerabilidad.

Siendo esto así, es natural que las potencias europeas Reino Unido, Francia y Alemania hayan revelado sus preocupaciones en la materia denunciado ser víctimas de múltiples ciberataques chinos y que, más aun, el Ministerio de Defensa británico haya considerado que se debe idear la creación de una ciberfuerza como un cuarto Ejército (Pastor, Pérez, Arnáiz y Taboso, 2009: 14); todo esto sumado que existen temores europeos de que se sucedan incidentes, tal como se dieron ciberataques rusos en EE.UU. para incidir en la elección de Donald Trump, digitados desde Rusia para influir en las elecciones de los países europeos, principalmente de los hegemones (Verhofstadt 2017).

Francia, Alemania y Reino Unido son los países materia de estudio en nuestro caso de estudio debido a su trascendencia y hegemonía en los procesos de toma de decisiones, en materia de seguridad y defensa, en la Unión Europea; son los países que registran mayor nivel de conectividad a sistemas informáticos (medición vía cantidad de usuarios); por su importancia en la comunidad internacional y la posibilidad de acceso a información sobre la materia a investigar.

Debemos mencionar que luego del Brexit y su progresiva concreción, la interacción entre estos países se vera afectada y, por consiguiente, también, el resultado de las contingencias por la búsqueda de hegemonía al interior del espacio comunitario: al alterar el equilibrio de poder por la ausencia de Reino Unido, que siempre se ha posicionado en un punto medio entre Francia y Alemania, la hegemonía de este último será evidente ante la relativa debilidad francesa. Esto supone una pérdida de lo que algunos académicos consideran un pilar de la existencia del espacio comunitario europeo: evitar la hegemonía

alemana, lo que supondrían conflictos futuros entre el enfoque francés, el alemán y sus repercusiones prácticas en la dirección de la UE (Booth 2016:12).

3.1.1. Francia:

El componente cibernético en las políticas de seguridad y defensa francés toma relevancia en el Libro Blanco de la Defensa del 2008 y se profundiza en el correspondiente al 2013. Este documento contiene las premisas, para un determinado periodo de tiempo, que guían las acciones del Estado francés en seguridad y defensa.

La premisa de "protección" en ese documento defendía la "capacidad de recuperación" del Estado y la sociedad francesa ante las agresiones a su seguridad mediante la innovación en los instrumentos de gestión de crisis y reforma de estructuras y procedimientos internos, reforzándose las capacidades de guerra cibernética y de biodefensa (Tertrais).

Se introduce, en el 2008, la necesidad de mejorar las capacidades técnico militares francesas, la adquisición de una capacidad de defensa informática, mejorar la capacidad de respuesta partiendo del principio que para saber defenderse, es bueno saber atacar (Pastor, Pérez, Arnáiz y Taboso, 2009: 28).

El documento correspondiente al 2013 identifica que los ciberataques son amenazas de fuerza, cuyos riesgos son amplificados por la globalización, con capacidad de intensificarse de aquí al 2025. Conforme a ello, se establece un modelo de ejército con capacidades militares en cibernéticas (Embajada de Francia en España).

Asimismo, se establece la ciberdefensa como una nueva posición estratégica para Francia, ya que no bastaría con la sola protección sino que se hace necesario determinar el origen de los ataques; mantener una mirada ofensiva y procurar el fortalecimiento del recurso humano, militar y civil, capaz de dar respuesta; mejorar los sistemas informáticos del Estado y de los grandes operadores (Embajada de Francia en España).

En la Revisión de la Estrategia de la defensa y la seguridad nacional de Francia del 2017 se evidencia una mayor conciencia y avance en los temas correspondientes a la ciberseguridad: se expone la prioridad de la soberanía digital ante los rápidos avances de la tecnología digital en la que multiples actores operan bajo poca supervisión legal constituyéndose así en una nueva fuente de vulnerabilidad (République Francais 2017).

Los planteamiento de este último documento en materia de seguridad informática exponen las aspiraciones francesas de tener autonomía y capacidad para tomar acción en el dominio informático, ya que se lo reconoce como un espacio de competencia internacional sobre el que hay que tener control físico y virtual (République Francais 2017).

Para el investigador Félix Arteaga (2017), el último documento francés expone los deseos de ese país en tanto esperan que sus fuerzas armadas cubran un espectro amplio de misiones con mayor capacidad operativa, sin descartar contribuciones de terceros pero sin llegar a niveles de dependencia por la complejidad y velocidad de la toma de decisiones, lo que incluye a la UE. Buscan, en suma, liderar las configuraciones multilaterales que se articulen, esperan estar al mando directo de todo ello.

3.1.2. Alemania:

En un inicio, hacia el 2007 – 2008, los esfuerzos alemanes en la materia se han orientado a concebir los soportes informáticos como parte de las infraestructuras críticas del país e idear un Plan Nacional para la Protección de Infraestructuras de Información; este plan buscaba: proteger y prevenir, así como preparar respuestas a las amenazas informáticas y crear una iniciativa sostenible en el tiempo para mejorar las capacidades informáticas alemanas (Pastor, Pérez, Arnáiz y Taboso, 2009: 33).

Posteriormente, en el 2011, el Ministerio Federal del Interior de Alemania publica la "Cyber Security Strategy for Germany" en el que se ratifica la concepción alemana de los sistemas informáticos abordados como infraestructura crítica. La importancia de su protección radicaría en la conexión de éstas, vía internet, con otros sistemas informáticos (Federal Ministry of Interior: 4).

Por ello, Alemania considera necesario establecer reglas internacionales de conducta en esta materia, que incluye la cooperación de la UE, el Consejo Europeo, la OTAN, el G8 y la OSCE (Federal Ministry of interior: 5).

A nivel interno, Alemania ha considerado oportuno mejorar la protección de los sistemas informáticos usados en los negocios y por la ciudadanía; elevar los estándares de seguridad informática en la administración pública, especialmente en las redes de conexión federal; Crear un Centro Nacional de Ciber Respuesta con el objetivo de mejorar la coordinación estatal (Policía Federal, Atención a desastres civiles, entre otras) y mejorar la capacidad de respuesta a las agresiones informáticas; creación de un Consejo Nacional de

Ciberseguridad que congrega a los ministerios encargados de la economía, comercio, defensa, la política exterior, representantes de los Länder y negocios alemanes para concretar esfuerzos conjuntos entre el sector privado y público. Asimismo, se considera de vital importancia la efectividad del combate del cibercrimen; la mirada alemana, como parte de su política exterior, pasa por potenciar la ENISA y agendar en los organismos comunitarios de defensa como una prioridad las políticas de ciberdefensa (a nivel europeo), y por establecer cooperación internacional transatlántica por medio de la OTAN (Federal Ministry of interior: 3- 11).

Al 2016, Alemania cuenta con la Bundesamt für Sicherheit in ther Informationtechnik (BSI), agencia especializada para en la ciberseguridad alemana con un enfoque que relacione el Gobierno, la economía y la sociedad, que tiene como marco de acción la Estrategia de Ciberseguridad para Alemania del Ministerio Federal del Interio, la Agenda Digital del Ministerio de Relaciones Económicas y Energía, y la Estrategia Nacional de Gobierno Electrónico del Ministerio de Transportes e Infraestructura Digital.

Todos esos componentes definen el marco de acción actual de Alemania en torno a la ciberseguridad y definen los pilares de la Ciberestrategia al 2016: mantenimiento de la soberanía alemana en la era de la digitalización, beneficio del interés público en las potencialidades y beneficios de la digitalización, afianzar marcos de acción del gobierno federal alemán, colaboración entre economía – ciencia – sociedad, y cerrar una política europea e internacional de cooperación en la materia debido al carácter transfronterizo del ciberespacio (Rothenpieler 2017).

Los campos de acción expuestos en la ciberestrategia alemana son 4: Acción segura y autodeterminada en un entorno digitalizado, Esfuerzo conjunto del gobierno y la economía, Arquitectura de ciberestratégica potente y sostenible a nivel nacional y, finalmente, la que nos vincula en el presente trabajo, posicionamiento activo de Alemania en la discusión de política de la ciberestrategia europea e internacional. Sobre este último, que se vincula con nuestra materia de estudio, el país en cuestión busca definir la política europea en ciberseguridad, el mejoramiento de la política de defensa de la OTAN, la cooperación multilateral y el fortalecimiento de la ley internacional (Rothenpieler 2017; Federal Office for Information Security 2016: 58).

Esta postura alemana responde al conocimiento de su predominancia y hegemonía en el escenario comunitario, por lo que impulsar la integración comunitaria en la materia es un modo de construir un escenario en el que Alemania y, por consiguiente, sus intereses nacionales predominen en materia de seguridad y defensa informática, lo que podría haberlo logrado en tanto la Directiva NIS, primera norma comunitaria europea, y los programas y estrategias conjuntas europeas de seguridad y defensa, parecen corresponderse a la caracterización presentada en la Ciberestrategia al 2016: cooperación, soporte multilateral y apuntalamiento de la OTAN.

3.1.3. Reino Unido:

Reino Unido incluye la “The National Security Strategy of the United Kingdom” del 2008 la protección de los soportes de internet como parte de las infraestructuras críticas del país susceptibles de ser atacados por criminales, terroristas u otros Estados.

Para ello, se idearon las siguientes acciones básicas: a. creación de un el Centro para la Protección de Infraestructuras Nacionales (CPIN), con la meta de reducir las vulnerabilidades de las infraestructuras; b. el desarrollo de una Estrategia Nacional de Seguridad de la Información, implementando un plan de lucha contra el cibercrimen; y c. la adquisición de equipos para el Ministerio de Defensa con el objetivo de recolectar datos (redes, tráfico de información, entre otros) y defender las redes (ante intrusos, virus, entre otros) (Pastor, Pérez, Arnáiz y Taboso, 2009: 31 - 32).

El documento “A strong Britain in an Age of Uncertainty: The National Security Strategy of the United Kingdom” del 2010 define que los ciberataques pueden tener origen en grupos criminales, terroristas u otros Estados (espionaje hostil) (HM Government: 11-14) y los ubica dentro de las 4 amenazas prioritarias a responder en materia de seguridad y defensa (HM Government: 27).

Asimismo, debido a las oportunidades económicas que el soporte informático brinda, compromete la acción del Estado en favor de implicar al sector privado en la lucha contra los ciberataques (HM Government: 5) y dentro del Estado favorece la cooperación entre las dependencias ya creadas.

La renovación del plan de ciber seguridad y estrategia de Reino Unido, promulgado para el término de 2016 al 2021, determina que en la materia y el marco de acción internacional refuerza la proyección de trabajo en unitario para garantizar los intereses y properidad futura de Reino Unido en el ciberespacio. Asimismo, buscan afianzar su capacidad operativa, la defensa de las infraestructuras críticas, de los intereses británicos en el extranjero y,

llamativamente, la promulgación de normas de comportamiento de un Estado responsable y no vinculantes (HM Government 2016).

Este último alcance ayudará en el análisis del presente estudio, ya que la particularidad británica de estar en Europa sin verse afectados por la vincularidad de normas comunitarias, más aún en temas concernientes a la seguridad del Estado, es una característica de la definición del interés de Reino Unido en la materia y en el cómo ha interactuado con los demás intereses.

La particularidad británica en esta materia, consideramos, es una de las causas estructurales del Brexit: ante la interacción negativa de los intereses nacionales en el ámbito comunitario, se fortalece el euroescepticismo. Este fenómeno, con mayor o menor medida, se viene dando en otros países miembros en los que se aprecia un choque entre aquello que la Unión Europea propone o impulsa a nivel comunitario y con los intereses nacionales diversos, muchas veces definidos por la identidad cultural de los países.

A nuestro entender, pues, los tres países buscan disminuir y controlar las agresiones hacia sus sistemas informáticos pero de diferente formas. Francia propone una mirada más ofensiva y beligerante en la materia, Reino Unido el establecimiento de un espacio de actuación responsable mas no vinculante para la satisfacción de sus intereses, mientras que Alemania busca crear y/o reforzar las instituciones internacionales encargadas de proteger los sistemas informáticos.

Las diferencias, creemos, marcan el proceso de implementación de una política pública comunitaria en lo referente a seguridad y defensa informática.

Asimismo, deben entenderse en el cómo los Estados buscan interactuar en un espacio comunitario para satisfacer sus intereses nacionales.

3.2. La visión de los demás países.

En febrero de 2013 (Comisión Europea), la Comisión Europea exponía y anunciaba que era necesario y prioritario enfrentar las amenazas cibernéticas mundiales de manera comunitaria e ir, incluso, dando pasos hacia la colaboración en una regulación mundial a la materia.

Ello, debido a que una respuesta conjunta de la comunidad internacional contribuiría a hacer más resistentes las redes digitales y a reducir de manera más rápida y drástica la delincuencia cibernética y las afectaciones a los sistemas informáticos referentes a la seguridad pública y nacional.

Existe en esa declaración de la Comisión Europea una clara predominancia de la visión alemana de cómo se debe tratar la materia: reforzar la legislación, incidir en la cooperación internacional y entender que las redes son infraestructuras críticas.

A pesar de que tengamos la predominancia de la visión alemana en la Comisión Europea, debemos prestarle atención a lo que dicen los demás países sobre la implementación de políticas de seguridad informática, ello colabora en la capacidad de diferenciar el real impacto de las políticas comunitarias en el orden nacional – estatal.

Sin embargo, no todos los países cuentan con los presupuestos, intereses o la relevancia geopolítica necesaria para diseñar e implementar políticas públicas de seguridad informática.

España es un país que viene trabajando en la materia de manera incial; su interés en regular y proteger infraestructuras críticas sobreviene con los atentados de Madrid en el 2004 que conlleva a la creación de un Centro Nacional de Protección de Infraestructuras Críticas, con el objeto de proteger los sistemas de información de la administración pública, y con la participación del Ministerio de Defensa Español en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (Pastor, Pérez, Arnáiz y Taboso, 2009: 33 - 34).

Asimismo, como hemos detallado ya en acápites anteriores del presente trabajo, el Gobierno español viene implementando una serie de medidas nacionales para contener el incremento de los ciberataques y teniendo como proyección crear una fuerza de 'hackers' con ese objetivo.

En el caso italiano, por su parte, encontramos que el tema es más disperso y no posee, a nuestro parecer, una estructura o visión que busque ser proyectada hacia la comunidad internacional; así, se tiene que la agenda italiana en materia de seguridad informática pasa por asegurar la infraestructura digital necesaria para la administración pública, buscar la cooperación con los sectores privados, la detección de amenazas y la necesidad generar la capacidad de ofrecer respuestas a las afectaciones y amenazas (Calliviani, 2011).

En torno a los demás países resalta, como también ha sido señalado anteriormente, el caso de Estonia: Hacia el 2007, la remoción, a manos de ciudadanos de Estonia, de una estatua del Ejército Rojo, dejada tras la Segunda Guerra Mundial, ocasionó que fuese víctima de ataques cibernéticos rusos. Estos estuvieron dirigidos a su infraestructura militar, civil y de gobierno,

y conllevó a que 6 países europeos liderados por Alemania decidieran que Estonia deba mejorar sus capacidades y apoyaron que la OTAN colaboré durante esa situación (Panagiotis: 2013).

Así, luego de tener que ser socorrido por la OTAN ante ciberataques rusos, se ha convertido en la punta de lanza de políticas concretas y eficientes en la materia siendo considerados como un modelo por la misma OTAN.

Los demás países no cuentan con información relevante y accesible en la materia. La inexistencia de información disponible revela el desinterés existente por la materia en los demás países y ayuda en el entendimiento de porque recién el 2016, a 12 años de creación de la ENISA, se ha logrado emitir la primera normativa comunitaria vinculante, pero que consideramos aun insuficiente frente la velocidad con la que aumentan los retos y afectaciones digitales.

Este contexto de desinterés e incapacidad de los demás países genera un escenario que posibilita el empoderamiento de los tres países hegemones y es materia de estudio en esta investigación: no existen resistencias y, por el contrario, ellos lideran la capacidad de propuesta en los espacios comunitarios para la materia, aunque de manera infructuosa por la incompatibilidad de sus intereses.

3.3. Impacto de interacción de estos intereses en la Unión Europea.

El caso de la Unión Europea es paradójico y podría definirse como un caso de frustración sin desintegración (tomando uno de los subtítulos de “The institutions of the European Union” de John Peterson y Michael Shackleton), debido a que el apoyo de los ciudadanos europeos al proceso de integración

matiza con un conjunto de instituciones que no logran responder a las expectativas previstas.

Esto se refuerza con la intergubernamentalidad expuesta por Stanley Hoffman, ya que desde esta concepción se enfatiza en la importancia de los gobiernos nacionales y sus roles en la determinación de la esencia y procedimientos comunitarios europeos.

Hoffman expuso que los gobiernos nacionales siempre respaldarían sus intereses y evidenció la dicotomía entre low politics y high politics, a los que ya nos hemos referido en la presente tesis, correspondiendos los segundos con aquellas políticas en las que los gobiernos nacionales están menos dispuestos a transferir su autoridad a un organismo supranacional porque necesitan minimizar la incertidumbre y retener un control estricto sobre los procesos de decisión cuando se trata de intereses vitales (Moga 2009: 800 - 801).

Sostenemos que esta dinámica expuesta en la década de los sesenta no ha variado y la imposibilidad de contar con políticas comunitarias de seguridad informáticas creemos que expone a una mayor indefensión a la Unión Europea y sus miembros respecto de amenazas tecnológicas recientes.

Así, se caracteriza que, para muchos casos, los proyectos que logran consenso y salir adelante en la UE son aquellos que se caracterizan por ser apolíticos y no controversiales, y muchas veces sucede también que hay una competencia de instituciones comunitarias que limitan e incluso imposibilitan concretar políticas públicas comunitarias eficaces y con legitimidad (Peterson y Shackleton: 11), lo que, consideramos, no solo se produce en lo concerniente a la seguridad informáitca sino, también, a políticas de inmigración, cultura o de

regulaciones legales que definen el sentido de la libertad, los derechos, deberes y la democracia en los Estados.

La seguridad y defensa informática es un tema controversial, eminentemente político y que pone en competencia, ya no solo instituciones, sino también países que buscan predominar en un conjunto de diversos intereses nacionales. Hemos reconocido que dentro de todos los intereses nacionales europeos, incluso, tres son los más preponderantes o hegemónicos: los de Reino Unido, Alemania y Francia.

La caracterización expuesta por Peterson y Shackleton refuerzan, a su vez, la teoría de Waltz respecto de las organizaciones internacionales: los países europeos bloquean propuestas controversiales y políticas, ergo solo dejan concretar aquello que deciden y se ajuste a sus intereses (Waltz, 2005: 178).

Waltz, como expusimos en la introducción de la presente tesis, también sustenta que mientras mayor interdependencia exista, menor grado de maniobra tiene un país sin afectar a su socio y, adicionalmente, teoriza que un Estado relativamente independiente tiene mayor fuerza que uno con mayor grado relativo de dependencia (Waltz: 2005: 171 – 173).

Lo señalado por el autor consideramos introduce la caracterización de la frustación causada por el conflicto de Alemania, Francia y Reino Unido, para esto podemos recurrir a cuatro características principales expuestas por la literatura revisada para ello (Pollack, 2005: 37):

a. La interdependencia entre las organizaciones.
b. Interacciones continúas entre los miembros de la red.

c. Interacciones reguladas.

d. Un alto grado de autonomía respecto del Estado.

Analizando cada una de estas características, observamos que la interdependencia de los países es intrínseca a la naturaleza de la materia a regular: la conectividad cibernética. Alemania lo recoge de manera lúcida al otorgarle importancia a sus redes en tanto sirven para interconectarse con otras redes.

Esto debería favorecer la concreción de la política pública comunitaria de manera más pronta y acorde a la velocidad con la que se presentan retos y afectaciones a la soberanía digital, pero en nuestro caso de estudio podría haber servido para mantener la iniciativa en el lapso transcurrido aunque con inactividad.

Ahora corresponde ver cómo el nuevo equilibrio de poderes entre Francia y Alemania determinan la posibilidad de concretar y avanzar con políticas públicas en la materia, aunque, como hemos analizado, sus planes y perspectivas son disímiles entre sí, por lo que no preveemos un futuro esperanzador.

En segundo lugar, los países miembros, en esta materia, no han tenido interacciones continuas sino conflictos o matices que han imposibilitado las interacciones necesarias para favorecer la gobernabilidad informática y hacer eficaz la ENISA.

Las “interacciones” han sido reguladas puesto que se encuentran dentro de un marco comunitario, formal, que corresponde a la ENISA, pero el mismo

marco no prevé como decidir o concretar políticas públicas controversiales, respecto a este tema se ha dejado a libertad de comportamiento del agente.

En cuarto lugar, el diseño institucional de la ENISA, como es natural, no goza de alguna autonomía respecto de los Estados: si bien cuenta con órganos propios, estos no responden a instituciones comunitarias sino que están compuestos por representantes directos de cada país, cada uno de ellos con un interés diferente.

Ante lo expuesto, creemos que los matices expuestos en las características de las estrategias cibernéticas de cada uno de los países relevantes en el proceso de toma de decisiones predispone a un conflicto/contraste permanente que imposibilita concretar una política pública comunitaria en la materia; esta al no poder concretarse, afecta a los países miembros, que como Estonia, requieren directrices para asegurar sus propios soportes informáticos y concretar la gobernabilidad informática del espacio europeo.

Asimismo, ante la incapacidad de generar una respuesta comunitaria ante el conflicto de los intereses de estos tres países surge la presencia de la OTAN como un actor capaz de ejecutar y proponer medidas que son aceptadas por los países.

La visibilidad creciente del rol de la OTAN durante las afectaciones a Estonia en el 2007 comprueban que la incapacidad comunitaria refuerza su aparición y su participación/colaboración de la OTAN es promovida por Alemania, en concordancia con los planes y la visión alemana en materia de seguridad y defensa informática.

La OTAN tiene, a diferencia de la ENISA, la capacidad de generar sus propios conceptos en materia de ciber defensa y son aceptados por los países europeos sin mayor discusión.

¿Por qué? ¿Por qué ha sido más fácil tener espacios de acción concreta en una institución como la OTAN? Creemos que se debe a la no necesidad de generar consenso: mientras la ENISA tiene que llegar a votaciones y consensos, la OTAN ha generado un concepto de defensa informática válido, técnico y apolítico.

Para la OTAN las políticas en ciber seguridad y defensa deben partir del reconocimiento de la existencia de la alianza en un mundo globalizado e inseguro, lo que indefectiblemente supone la necesidad de implementar una visión de amenazas asimétricas en la materia (Panagiotis: 2013).

Asimismo, se debe tener en cuenta que la OTAN es un espacio internacional en el que los intereses norteamericanos tienen singular relevancia. Estados Unidos busca contener la presencia y proyección rusa en Europa, por lo que usa la OTAN para la contención, que incluye el fortalecimiento de la seguridad y defensa informática comunitaria.

Los conflictos estatales se dan en tanto los temas que se intentar regular sean controversiales y profundamente políticos. La seguridad y la vocación de compartir infraestructuras e información son temas completamente controversiales y políticos en tanto están profundamente ligados a la consecución de los intereses nacionales de cada Estado, por ello es más factible obtener resultados por medio de alianzas militares que a través de un órgano comunitario.

Para nuestro caso de estudio es importante resaltar los debates sobre los cuestionamientos a las acciones de la UE desde una perspectiva identitaria, sobretodo desde la posibilidad de contravenir la tradición política y esencia de la cultura Occidental.

Esto puede verse en las declaraciones de los diversos líderes, a los que se les ha etiquetado de populistas y eurófobos, que surgieron luego de la crisis del euro o en el marco de los lineamientos comunitarios frente a inmigración, y que reclaman limitaciones a los poderes de Bruselas en tanto consideran que sus países van perdiendo no solo soberanía sino también identidad.

Huntington (1993) se anticipaba a estos escenarios exponiendo que los bloques económicos regionales podrá arraigarse en una civilización común, en la que s refuerze la conciencia de esa civilización y, por ello, exponía que el éxito de la entonces "Comunidad Europera" *"descansa sobre el cimiento compartido de la cultura europea y el cristianismo occidental"*.

¿Es negativo que los pueblos definan su identidad en términos étnicos y religiosos? Creemos que no, dado que se contribuye a la generación de ideas e identidades colectivas que trascienden de intereses ideológicos (por ejemplo, el caso polaco y su enraizamiento cristiano es una variante explicativa de la caída del régimen comunista, lo que soporta la idea de que la identidad trasciende de poderes ideológicos).

La esencia de Occidente, para Huntington (1993), se enmarca en su legado de la cultura clásica, el cristianismo occiental (catolicismoy protestantismo), los idiomas europeos (lenguas romances y germánicos), la separación del poder temporal y espiritual (sin negar su dualidad), el imperiode

la ley, el pluralismo social, la existencia de organismos representativos y el sentido individualista de derechos, deberes y libertades.

Creemos que cuando diversos actores comunitarios consideran que esta identidad es afectada, desde el mismo espacio comunitario, se expande la imposibilidad de concertar y concretar políticas públicas, más aún en materia de seguridad y defensa. En tanto aquello que fundamenta la idea del “nosotros” se vea afectado, menor será la probabilidad de unirse para defensar contra diversas amenazas, de cualquier índole.

El mismo Hungtinton años después (1997) expone que la división de Occidente solo lo vuelve vulnerable ante los esfuerzos de los países no occidentales por explotar sus diferencias internas y dividirlos. Impulsar la cohesión de Occidente significa, por tanto, preservar la cultura occidental dentro del mismo Occidente.

Un ejemplo de éxito, consideramos en la presente tesis, de esto es la OTAN: surge en la posguerra fría como un elemento de seguridad de la cultura occidental frente a un enemigo común, ideoloógico, y que cuestiona la tradición y esecia de Occidente: el comunismo.

Por lo expuesto, consideramos que muchos de los intereses nacionales que impiden establecer políticas públicas comunitarias, en este caso de seguridad y defensa informática, se corresponden con la idea de determinadas sociedad y, por consiguiente, de sus Estados y gobiernos, de que deben preservar su identidad cultural.

Mientras no se entienda que la seguridad y gobernabilidad informática es el elemento para defender la cultura Occidental (el “nosotros” que fundamenta

la cultura europea) en el futuro (esto por el devenir natural del desarrollo científico y su impacto público) difícilmente se podrá avanzar para hacer frente de manera decidida y eficaz a las vulnerabilidades tecnológicas y científicas a los intereses estatales.

CONCLUSIONES

En el desarrollo de la presente investigación, consideramos, hemos llegado a probar que la Unión Europea se encuentra en un estado de vulnerabilidad respecto a su seguridad y gobernabilidad informática debido a la imposibilidad de armonizar los intereses nacionales exitentes, principalmente de los hegemones europeos (Reino Unido, Alemania y Francia).

Asimismo, la presente investigación partió con tres objetivos principales identificables: explicar las causas de la existencia de políticas públicas de seguridad y defensa informática; en segundo lugar, describir cómo ha sido tratada la materia en la Unión Europea (UE), a nivel formal. Y, finalmente, comprender cómo se determinan las políticas públicas de seguridad y defensa informática según el orden político interno de la UE.

Al terminar la presente, debemos hacer un balance de los logros, considerando estos tres objetivos iniciales. Así, tenemos que:

A. Las innovaciones tecnológicas han significado abrir un nuevo espacio de interacción política para los Estados pero, a su vez, han supuesto una redefinición de sus límites y capacidades físicas: la existencia de un espacio virtual, en el que interactúan los sujetos, conlleva la virtualización del Estado.
B. Las políticas públicas que buscan generar espacios virtuales seguros responden al uso que el Estado le ha dado a los sistemas informáticos para el almacenamiento de la información relevante para la consecución de sus intereses nacionales. Siendo así, se

debe considerar que la información, en sí misma, tiene un gran valor para la toma de decisiones del Estado.

C. La Unión Europea (UE) es una organización comunitaria supranacional que, a la luz de lo expuesto en la presente investigación, es incapaz de generar políticas de seguridad informática de aplicación en todo el espacio comunitario. Esto debido a las constantes fricciones que se producen entre los intereses nacionales de los países con capacidad de influir en los procesos de toma de decisiones: Alemania, Reino Unido y Francia.

D. Si bien los postulados de Waltz explican esta incapacidad, es decir, los organismos internacionales al tener Estados tan compenetrados entre sí, les ofrece poco margen de acción y ocasiona que los Estados con mayor independencia busquen dominar estas organizaciones imponiendo sus intereses e identidad; debe considerarse que una organización como la UE sería capaz de generar acuerdos e implementar políticas si convierte a la seguridad informática en un tema no controversial ni político sino técnico – militar: los intereses de los países que influyen de sobre los procesos de toma de decisiones (Reino Unido, Francia y Alemania) tienen una visión técnico – militar de esta materia, por lo que asumir ese enfoque podría suponer un incentivo para el consenso, el rol jugado por la alianza militar transoceánica de la OTAN respaldan esta conclusión.

E. La incapacidad de generar una política comunitaria afecta la gobernabilidad informática en la materia, esto se ve materializado los multiples ataques que han sido señalados en el presenta trabajo y que han ocurrido en los últimos años. La ENISA tiene años de existencia y ha sido incapaz de generar un espacio comunitario seguro, de protección eficaz de la información y esto conllevó a que la OTAN, una alianza militar independiente de la UE, asuma un rol protagónico en esta materia y escenario.

F. Es imprescindible para la seguridad y el futuro de la proyección internacional de la Unión Europea establecer un mecanismo de confluencia en el que se reconozca la hegemonía de Francia y Alemania en la materia. Es decir, se debe promover una instancia de coordinación y acuerdos previos entre los países hegemónicos que han quedado como partes del espacio comunitarios luego del Brexit.

Asimismo, es de vital importancia que la UE se conduzca hacia un espacio en el que la seguridad y las relaciones internacionales (política exterior) sean definidas de manera federal, tal como lo menciona la bibliografía consultada en la investigación, para poder concretar un espacio comunitario democrático, gobernable y eficaz en la gestión y control de la información cibernética.

G. No se pueden obviar los cuestionamientos de naturaleza cultural a las acciones implementadas por la UE: en tanto existan actores que las interpreten como contrarias a aquel fundamento que les permite

pensar en colectivo (“nosotros”) en la cultura europea, difícilmente podrán diseñarse e implementarse políticas efectivas y concretas en la árena de estudio que motiva la presente tesis.

BIBLIOGRAFÍA

ABELLÁN, Lucía

2017 *"Los ciberataques a la OTAN incrementan en un 60% en 2016"*. En: Diario El País. Visita en línea: <https://elpais.com/internacional/2017/03/13/actualidad/1489425600_231212.html>, Sabado 20 de Enero de 2018, 10:00 horas.

AGENCIA EFE

2017 *"Mega ataque cibernético afecto compañías en Europa"*. En: Cooperativa – Chile. Visto en línea: <http://www.cooperativa.cl/noticias/tecnologia/internet/seguridad/mega-ataque-cibernetico-afecto-a-companias-en-europa/2017-05-12/133138.html>, Domingo 28 de Enero, 22:00 horas.

AGOZINO, Adalberto

2005 *Megatendencias en seguridad internacional*, Buenos Aires: Editorial Ábaco de Rodolfo Depalma.

ARTEAGA, Félix

2017 *"La Revisión Estratégica de la defensa y la seguridad nacional de Francia en 2017"*. Real Instituto Elcano. Comentario Elcano 48/2017. 16 de Noviembre de 2017. Visto en línea: <http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-arteaga-revision-estrategica-defensa-y-seguridad-

nacional-francia-2017>, Domingo 28 de Enero de 2018, 22:45 horas.

BARBÉ, Eshter

1987 *"El papel del realismo en las relaciones internacionales – la teoría de la política internacional de Hans J. Morgenthau"*. En: Revista de Estudios Políticos (Nueva Época). Núm. 57, Julio – Setiembre

BERGGRUEN, Nicolás y Nathan GARDELS

2012 *Gobernanza inteligente para el siglo xxi. Una vía intermedia entre Occidente y Oriente.* Madrid: Editorial Taurus.

2012 *"¿Cómo podría ser una unión política europea?"*. En: Diario El País. Visita en línea: <http://internacional.elpais.com/internacional/2012/01/24/actualidad/1327406234_109035.html>. Miércoles 2 de abril de 2014, 15.00 horas.

BOOTH, Stephen

2016 *"El BREXIT: un desafío para todo el continente"*. En: Papeles FAES. Fundación para el Análisis y los Estudios Sociales. 14/03/2016, No 185, Madrid. Versión en línea: < http://www.fundacionfaes.org/file_upload/publication/pdf/20160310180423el_-brexit-_un_desafio_para_todo_el_continente.pdf>. Visita: Viernes 26 de Enero de 2018, 10:00 horas.

BUSTAMANTE DONAS, Javier.

2010 *"La Sociedad de la Información: Hacia una Cuarta Generación de los Derechos Humanos: repensando la condición humana en la sociedad tecnológica"*. Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación. Organización de Estados Iberoamericanos para la Educación, Ciencia y Cultura. Número 1, Septiembre – Diciembre 2010. Visita en línea: < http://www.oei.es/revistactsi/numero1/bustamante.htm>, Lunes 03 de Junio de 2013, 15.00 hrs.

CABERO ALMENARA, Julio.

1995 *"El ciberespacio: el no lugar como lugar comunicativo".* Universitat de les Illes Balears, 1995. En: Edutec – Materials. Visita en línea: <http://www.uib.es/depart/gte/cabero.html>, Jueves 30 de Mayo de 2013, 19.00 hrs.

CANALES ALLENDE, José Manuel.

2001 "Gobernabilidad y Gestión Pública". En: DE LIMA GETE, Blanca Olías Coord. *La Nueva Gestión Pública*. Prentice Hall: España, 2001. Pp. 38.

CARRETERO, Nacho

2017 "Entrevista a Luis Jiménez Muñoz". En Diario El País. Consulta: 20 de Enero de 2018. https://politica.elpais.com/politica/2017/08/07/actualidad/1502095850_940407.html

CAVALLINI, Matteo

2011 *Digital Agenda Assembly – Cybersecurity: barriers and incentives.* Ministerio DellÉconomia e delle Finanze (Italia), Bruselas.

COMÍN, Martha.

2005 *"Gobernar las TI: obtener el máximo valor de la tecnología"*. Computing e – business. PwC – IESE. 6 de abril de 2005.

COMISIÓN EUROPEA

2013 *Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro.* Bruselas, 7 de febrero de 2013. Visita en línea: <http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es>, Jueves 25 de Enero de 2018, 07:30 horas.

2017 *Comisión Europea: Comunicado de Prensa. Estado de la Unión 2017*. Bruselas, 19 de Setiembre de 2017. Visita en línea: <http://europa.eu/rapid/press-release_IP-17-3193_es.htm>, Martes 23 de Enero de 2018, 23:00 horas.

CHOUCRI, Nazli

2012 *Cyberpolitics in International Relations*. Cambridge: The MIT Press.

CHOUCRI, Nazly y Daniel GOLDSMITH.

2012 *"Lost in cyberspace: Harnessing the internet, internacional relation and global security".* En: Bulletin of the Atomic Scientists 68 (2). Pp. 70 – 77, 2012.

DE CASTRO SÁNCHEZ, Claribel.

2010 "Seguridad Internacional y nuevas amenazas en un mundo globalizado". En: GONZÁLEZ SÁNCHEZ, Víctor M. Coord. *Globalización: un enfoque multidisciplinar*. UNED – Tirant lo Blanch: Valencia, 2010.

DIARIO EL PAÍS

2017 *"Los ciberataques en España se duplican en un año: más de 105 000 en 2016"*. En: Diario El País. Visto en línea: <https://politica.elpais.com/politica/2017/03/14/actualidad/1489494011_520649.html>, Sabado 27 de Enero, 21 horas.

EUROPEAN COMMISSION

2017 *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.* Bruselas, 13 de Setiembre de 2017. Visto en línea: < http://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf >, Sabado 27 de Enero de 2018, 23:45 horas.

2017 *State of the Union 2017. Cybersecurity.* Visto en línea: < http://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf>, Domingo 28 de Enero de 2018, 00:30 horas.

2013 *COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro.* 7 de Febrero de 2013. Visto en línea: <http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es>, Sabado 20 de Enero, 23:00 horas.

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL)

2017 *Internet organised crime threat assessment.IOCTA 2017.* Netherlands.

FEDERAL MINISTRY OF THE INTERIOR

Cyber Security Strategy for Germany. Visto en línea: <http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile>. 15 de Noviembre de 2013.

FEDERAL OFFICE FOR INFORMATION SECURITY

2016 *The State of IT Security in Germany 2016.* Federal Office for Information Security (BSI), Frankfurt am Maim. Octubre 2016.

FRANCHINI, Roberto

2003 *La conducta estadounidense en cuanto a su política exterior: Una explicación Realista*. Universidad de las Américas, Puebla, México.

GÁLVEZ, J.J.

2017 "Los ciberataques a infraestructuras estratégicas se multiplican por siete en dos años". En: Diario El País. Visto en línea: <https://politica.elpais.com/politica/2017/05/24/actualidad/1495619175_136537.html>, Viernes 26 de Enero, 12:00 horas.

GARCÍA-CERBVIGÓN HURTADO, Alfonso y María del Pilar ALEGRE RAMOS.

2011 *Seguridad Informática*. Editorial Paraninfo: Madrid, 2011.

GÓMEZ, Rosario

2017 *"Escuadrones de 'hackers' contra los ciberataques".* En: Diario El País. Visto en línea: <https://elpais.com/elpais/2017/05/17/opinion/1495034241_299111.html>, Domingo 21 de Enero de 2018, 21:00 horas.

GONZÁLEZ, Ariel

2007 *"Análisis y evolución del balance de poder: hacia una conceptualización del tripolarismo".* En: Revista Intellector. Centro de Estudos em Geopolítica & Relações Internacionais. Ano III, Volume IV, No 7, Julho/Dezembro 2007, Rio de Janeiro. Versión en línea: < http://www.revistaintellector.cenegri.org.br/ed2007-07/arielgonzalez-site.pdf>. Visita: 03/07/2013

HM GOVERNMENT

2010 *A strong Britain in an Age of Uncertainty. The National Security Strategy.* Prime Minister of Great Britain.

2016 *Estrategia de Ciberseguridad Nacional 2016-2021*.

HUNTINGTON, Samuel

1993 *"¿Un choque de civilizaciones?".* Visto en línea: < http://www.mty.itesm.mx/dhcs/deptos/ri/ri95-801/lecturas/lec125.html>, 20 de Febrero de 2018, 22:00 horas.

1997 *"Occidente único, no universal"*. Revista Política Exterior. Enero – Febrero 1997. Visto en línea: < https://www.politicaexterior.com/articulos/politica-exterior/occidente-unico-no-universal/>. 21 de Febrero de 2018, 08:00 horas.

INTERNET WORLD STATS

"Internet Users in Europe". Visita en línea: <http://www.internetworldstats.com/stats4.htm>, Lunes 22 de Enero de 2018, 19.00 horas.

"Internet growth statistics". Visita en línea: <http://www.internetworldstats.com/emarketing.htm>, Domingo 28 de Enero de 2018, 12:31 horas.

KALDOR, Mary

2010 *El poder y la fuerza. La seguridad de la población civil en un mundo global*. España, Estudio Úlbeda.

KELLO, Lucas

2012 *Cyber Disordes: Rivalry & Conflict in a Global Information Age*. Science, Technology & Public Policy Program. International Security Program – Minerva Project (Harvard – MIT). Belfer Center, Harvard Kennedy School.

KEOHOANE, R. (ed.)

1986 *Neorealism and its Critics*. Nueva York: Columbia University Press.

LEGRAND, Jerome

2017 *La Política Común de Seguridad y Defensa*. Fichas técnicas sobre la Unión Europea. Setiembre de 2017. Vista en línea: < http://www.europarl.europa.eu/RegData/etudes/fiches_techniques/2017/N53899/04A_FT(2017)N53899_ES.pdf>, Domingo, 28 de Enero de 2018, 21:00 horas.

LEWIS, Jeffrey

2002 "National interests: coreper". En Peterson John y Michael Shackleton (Ed) *The institutions of European Union*. New York: Oxford University Press.

MENDOZA, Miguel Ángel

2016 *"NIS: ¿qué es y qué implica esta nueva legislación en seguridad?"*. En: We Live Security. Visto en línea: < https://www.welivesecurity.com/la-es/2016/07/22/nis-que-es-

nueva-legislacion-seguridad/>, Domingo 28 de Enero de 2018, 10:30 horas.

MINISTERIO DE DEFENSA DE ESPAÑA.

2010 *"Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio"*. Instituto Español de Estudios Estratégicos – Instituto Universitario "General Gutiérrez Mellado", Diciembre de 2010.

MOGA, Tedor Lucian

2009 *"The Contribution of the Neofunctionalist and Intergovernmentalist Theories to the Evolution of the European Integration Process"*. En: Journal of Alternative Perspectives in the Social Sciences (2009) Vol 1, No 3, 796-807.

MORET MILLÁS, Vicente

2017 *Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español*. Documento de Opinión. Instituto Español de Estudios Estratégicos. 3 de Marzo de 2017. http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO21-2017_DirectivaNIS_VicenteMoret.pdf

MORGENTHAU, Hans J.

1963 *La lucha por el poder y por la paz*. Editorial Sudamericana, Buenos Aires.

MUÑOZ, Alberto

2017 *"Los hospitales de Reino Unido, en alerta por un ciberataque".* En: Diario El Mundo. Visto en línea: <http://www.elmundo.es/tecnologia/2017/05/12/5915cb15e5fdea24788b4658.html>, Lunes 22 de Enero de 2018, 21:00 horas.

NUGENT, Neil

2006 *Government and politics of the European Union.* Durham: Duke University Press.

O'KUINGHTTONS, Úrsula

2017 *"Un caso de éxito: cómo Estonia se protegió contra los ciberataques"*. En: Diario El País. Visto en línea: <https://elpais.com/tecnologia/2017/05/13/actualidad/1494680920_206684.html>, Domingo 21 de Enero de 2018, 20:50 horas.

PANAGIOTIS EFTHYMIOPOULOS, Marios

Challenging NATO's Security Operations in Electronic Warfare: The Policy of Cyber-Defense: the Case of Greece. Visto en línea: <http://www.lse.ac.uk/europeanInstitute/research/hellenicObservatory/pdf/4th_%20Symposium/PAPERS_PPS/FOREIGN_SECURITY_POLICY/EFTHYMIOPOULOS.pdf>. 10 de Diciembre de 2013.

PARLAMENTO EUROPEO

2017 *Informe sobre la lucha contra la ciberdelincuencia. Comisión de Libertades Civiles, Justicia y Asuntos de Interior*. 25 de Julio de 2017.

PARLAMENTO EUROPEO Y CONCEJO EUROPEO

2016 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Consulta: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES

PASTOR ACOSTA, Oscar; PÉREZ RODRIGUEZ, José Antonio; ARNAIZ DE LA TORRE, Daniel y Pedro TABOSO BALLESTEROS.

2009 *Seguridad Nacional y Ciberdefensa.* Fundación Rogelio Segovia, España.

PETERSON, Jhon y Michael SHACKLETON

2011 *EU Institutions and Europe's Politics*. Wissenschaftszentrum für Sozialforschung.

PRETOFF, Alana

2017 *"Hackers lanzan ciberataque masivo contra empresas y agencias en Europa".* En: CNN Tecnología. Visita en línea: <http://cnnespanol.cnn.com/2017/06/27/hackers-lanzan-ciberataque-masivo-contra-empresas-y-agencias-en-europa/>, Viernes 19 de Enero de 2018, 21:30 horas.

PRIGG, Mark

2014 *"Technology giants reveal how often they are ordered to turn over information to the Government (and it's thousands of times a month)".* En: Daily Mail. Visita en línea:

<http://www.dailymail.co.uk/sciencetech/article-2551277/Technology-giants-reveal-ordered-turn-information-Government.html>. Viernes 26 de Enero de 2018, 10:00 horas.

RÉPUBLIQUE FRANCAIS

2017 *Strategic Review of Defenseand National Security 2017. Key points.* Para descarga de su versión en inglés: https://www.defense.gouv.fr/dgris/presentation/evenements/revue-strategique-de-defense-et-de-securite-nationale-2017

ROTHENPIELER, Samuel

2017 *National Cyber Security Strategy 2016* [Diapositiva]. Consulta: 15 de Enero de 2018. https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/170426-bsi-enisa-nlo-presentation-v2.pdf

SAIZ, Eva

2013 *"Los ciberataques sustituyen al terrorismo como primera amenaza para EE.UU.".* En: Diario El País. Visita en línea: <https://elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html>, Miércoles 10 de Enero, 08:30 horas.

SALOMÓN, Mónica

2002 "*La teoría de las relaciones internacionales en los albores del siglo XXI: diálogo, disidencia, aproximaciones"*. En: Revista Electrónica de Estudios Internacionales. 2002. Pp. 1 – 59.

SOWELL, Jesse H.

Documento de trabajo de la Oficina de Investigación Naval. Número N00014-09-1-0597.

TORREBLANCA, José Ignacio

2008 "*Francia y la Unión Europea: percepciones, sintonías, desajustes. España"*. En: Revista "Política exterior" No 122 - 2008. Pp. 81 – 92.

2016 "Las claves del Brexit". En: Revista Cambio 16. 23 de Abril de 2016. Visita en línea: <https://www.cambio16.com/reportajes/las-claves-del-bretix/>, Jueves 25 de Enero de 2018.

UN DATA: A WORLD OF INFORMATION

"Internet users (per 100 people)". Visita en línea: <http://data.un.org/Data.aspx?d=WDI&f=Indicator_Code%3AIT.NET.USER.P2>. Miércoles 24 de Enero de 2018, 09:00 horas.

UNIÓN EUROPEA – ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE

2016 *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. 8 de Julio de 2016.

VERDÚ, Daniel

2017 *"La red diplomática italiana, víctima de un ciberataque a sus correos".* En: Diario El País. Visita en línea:

<https://elpais.com/internacional/2017/02/10/actualidad/1486749643_133050.html>, Viernes 19 de Enero de 2018, 21:00 horas.

VERHOFSTADT, Guy

2017 *"La guerra híbrida de Rusia contra Occidente"*. En: Diario El Tiempo. Visto en línea: <http://www.eltiempo.com/mundo/europa/los-ataques-ciberneticos-de-rusia-podrian-llegar-a-europa-31133>, Miércoles 24 de Enero, 11:00 horas.

WALLACE, William

2005 "Foreign and Security Policy". En: Wallace, Helen; Wallace, William y Mark A. Pollack. *Policy-Making in the European Unión.* Nueva York, Oxford University Press.

WALTZ, Kenneth N.

2000 *"Structural Realism after the Cold War"*. En: International Security, Vol. 25, No. 1 (Summer 2000), MIT. Versión en línea: < http://teoriarelacionesinternacionales.files.wordpress.com/2009/07/neorrealismo_y_realismo_estructural.pdf>. Visita: 31/06/2013