UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

LA CIBERGUERRA Y LA CONFIGURACIÓN DE LAS AGENDAS DE CIBERSEGURIDAD EN RUSIA Y ESTADOS UNIDOS 2007-2020.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN
RELACIONES INTERNACIONALES

P R E S E N T A:

Mariana Corona Fragoso

DIRECTOR DE TESIS:
Mtro. Marco Antonio Lopátegui Torres

Tesis elaborada en el marco del Proyecto PAPIIT IN-309121

"Los Regionalismos Frente a los Retos y la Complejidad de las Amenazas a la Seguridad y Defensa Contemporáneas II"

Ciudad Universitaria, CDMX, 2023.

Agradecimientos

"Agradecer" es en mi opinión, una palabra que limita lo que siento por aquellas personas que me han acompañado en mi trayectoria académica (y personal) mucho antes de si quiera iniciar este trabajo de investigación. Su presencia es muestra invaluable de amor, y de confianza inquebrantable, algo que merece ser honrado y no solo agradecido.

Siempre y, sobre todo, primero honrar profundamente a la Dra. Virginia Fragoso Ruíz y al Ing. Jorge E. Corona González, o como yo les llamo "mamá y papá"; quienes han impreso en mi existencia todo su amor, confianza y valores que hacen de mí la profesionista y persona que soy. Su legado ha mantenido mis sueños, y sus enseñanzas, han fortalecido mis pasos. Sepan que cada triunfo es tan mío como suyo. Gracias por traerme hasta aquí. En ese mismo sentido, este trabajo no habría sido posible sin mi mano derecha, y amiga de vida, mi hermana Delia Corona; fuente de inspiración y del empuje necesario para cumplir sueños como este, de los cuales, espero que ella también cumpla los suyos, pero siempre y dónde sea, juntas de alguna manera.

A mis abuelitas Maura Ruíz y María de la Luz González, quienes, a su manera, sembraron en mí el ímpetu de salir adelante y expresar mis ideas, la gracia de sobrellevar las desavenencias, y siempre han tenido una linda palabra para sanarme el corazón. Abuelito Mauro, siempre te sentí cerca, siempre sentí tu cálido apretón de hombro durante el semestre de primavera, en Abril… ¿aún crees que seré embajadora desde allá arriba? Nana Rita, jamás dudes ni un momento que este logro se hizo posible por tu dedicación, cuidado y amor que me diste, al tener la fortuna de experimentar una infancia preciosa de tu mano.

Mis más profundos agradecimientos a la familia Ruíz Contreras por estar al tanto de mí, mucho antes de llegar a este mundo, por su consejo y cariño incondicional, los cuales han sostenido mi persona en el camino de descubrir en quién me quiero convertir.

A la Universidad Nacional Autónoma de México, que, con el firme compromiso de darle a nuestra nación, profesionistas críticos y libres que con sus aspiraciones forjen el rumbo de México a mejores escenarios, cumple la labor más noble que pueda realizar una institución; enseñar y darle a su sociedad el bien más preciado al que puede aspirar; el conocimiento y la cultura. Siempre con una deuda impagable que solo con la entrega y ética profesional a la que me debo como egresada podría, un día, ser saldada.

En esta línea, mi más humilde agradecimiento a Proyecto PAPIIT IN-309121 "Los Regionalismos frente a los retos y la complejidad de las amenazas a la seguridad y defensa contemporáneas II" así como a sus responsables el Dr. Alejandro Chanona y la Dra. Yadira Gálvez, quienes con su compromiso y fiel vocación a la formación de internacionalistas que busquen estar a la vanguardia de los acontecimientos en la escena internacional, apoyaron esta investigación desde su etapa más primaria en un contexto pandémico.

A su vez, agradezco a la Dra. Irene Zea y al Mtro. Irwing Rico por su asesoría y prestancia para lograr esta investigación; confrontar mis postulados para fortalecer mi conocimiento no solo ha sido un reto, sino también un honor. No podría faltar así, darle las gracias a mi asesor, el Mtro. Marco Antonio Lopátegui, quién en más de una ocasión ha creído en mí antes que yo misma; los resultados de este trabajo de investigación contienen la esencia, cariño, y fe que solo un mentor que va más allá del salón de clases puede tener; gracias por validar mis ideas, mis sentimientos y siempre estar en la disposición de brindar una mano amiga a quien se deje, y en este caso yo me dejé…

Un agradecimiento especial a la Dra. Arcelia Moreno y al Ing. Carlos Moreno, quienes hicieron posible que representara a la Universidad en República Dominicana y me mostraron un camino que, sin saberlo en ese momento, me llevaría a escoger la carrera que el día de hoy estoy culminando. Sepan que su nobleza trasciende en la historia de más de uno de nosotros.

La UNAM me ha llevado a conocer a otros universitarios a quienes puedo llamar amigos y a otros "jefe" o "jefa". Sin embargo, he tenido la fortuna de encontrar en una misma persona a ambos: tal es el caso del Dr. Francisco José Trigo, Coordinador de Relaciones y Asuntos Internacionales de esta casa de

estudios, la Mtra. Paola S. Mendieta y la Lic. Clarisa Vargas, quienes me han acompañado, enseñado y brindado su experiencia siempre con la intención de hacerme mejor internacionalista y persona. Por darme la oportunidad y su amistad, mil gracias.

Este trabajo solo es el resultado final de una etapa que estuvo enmarcada por quienes conocí a lo largo del camino, quienes vivieron a mi lado los mejores y lo peores momentos que cursar una carrera te da. Son personas cuyos sus ideales abrazaron los míos y me dieron el privilegio de vivir aventuras en el camino de convertirnos en profesionistas. Gracias eternas a Amalia Cabrera, Monserrat Gasca, Brenda Jarquín, Michelle Martínez, Mía Fuentes, Mariana Becerro, Abigail Hernández, Tania Cervantes, Salma Trueba, Ayary Sevilla, Andrea Jiménez, Lilia Leal, Andrea Isabel Guevara, Iván Martínez, Sergio Huesca, Arturo Álvarez, Misael Rivero, Roberto Mohar, Mariana P. Nicolau, Ana Jiménez, Ximena Ochoa, Adrián Suárez, Carolina Velasco, Javier Vieyra, Leslie S. Capetillo, Juan Carlos Mondragón, Astrid Sánchez, Marisol Venegas, Jocelyn Casagnon, Dulce Karina García y Sandra Hernández. Especialmente, a Luis Andrés González, quien en pandemia o en Corea del Sur siempre sostuvo mis ánimos y su fe, hizo palpable la mía.

A la persona que tiene mi corazón, Cristian Avila, gracias por mostrarme que puedo aspirar siempre a algo mejor, por contagiarme tu ánimo para seguir adelante, por enseñarme que hay muchos más caminos que recorrer, y que, si es juntos, es más bonito. Esta investigación nos lleva en cada página un paso más cerca de nuestras metas. Gracias por amarme cada día y comprenderme como pareja, amiga, universitaria, tesista y todo lo que soy.

Para poder tener un espectro más amplio a nivel internacional es necesario tener las herramientas para entender y comunicar; por ello el idioma inglés ha sido trascendental tanto para mi formación como para que este trabajo pueda contar con referencias bilingües y traducciones propias. Mtra. Reyna I. Huerta, gracias por hacer lo anterior posible, por abrirme un mundo de posibilidades y creer en que podría dominar la lengua inglesa a la perfección desde que me conoció a los 12 años, por las enseñanzas del idioma y de la vida, mil gracias Teacher.

La persona que mantuvo mis nervios en el bolsillo, y todo bajo control debería compartir créditos en este trabajo porque fue fundamental para que la ansiedad no me ganara. Por darme un oído amigo y un espacio seguro para mis más profundas reflexiones, quiero agradecer a la Psicól. Magda L. Rendón.

Aunque no estuvo aquí para ver el esfuerzo de cada madrugada materializado, quiero "darle la patita" a mi compañero de desveladas y trabajo, Whisky; él me acompañó al hacer tarea desde que tengo memoria, se iba a dormir hasta que yo lo hacía… siempre tendrá un lugar a un lado de mi escritorio (sé que aún me espera ahí). Terminamos nuestra "última gran tarea". Gracias por tu lealtad.

Lo más probable es que no hubiese sobrevivido a las desveladas, presión y estrés si no hubiese sido por las balsámicas letras de Taylor Swift a las 02:00 de la mañana; así que mil gracias TayTay porque esto es: "the end of a decate, but the start of an edge".

Finalmente, al amigo más incondicional y sincero que tengo, Dios, porque "ya me has escuchado, todo llegará".

-Mariana Corona
Otoño, 2023.

ÍNDICE

ÍNDICE DE FIGURAS Y TABLAS

Introducción

Las tecnologías de la información y comunicación en el siglo XXI han tenido un papel sustancial en la dinámica social, cultural, económica y política alrededor el mundo. El espacio cibernético se configura como un espacio que se compone de relaciones e interacciones que forman parte de la realidad material que nos rodea, en éste, la regulación y comprensión de los flujos de información y datos se vuelve prácticamente imposible de decodificar, pues repercute en la armonía o el conflicto entre los individuos y Estados a distintos niveles.

Como resultado de la hipertecnologización y los avances tecnológicos de la revolución industrial 4.0, así como de la incipiente regulación en materia de ciberseguridad, se observa de manera recurrente la existencia de distintas prácticas como el ciberespionaje, el robo de información a empresas, instituciones gubernamentales, y financieras, así como a las actividades de la sociedad civil, a través de la infiltración de *malwares* especializados, denegación de servicios, gusanos cibernéticos, entre otros, que amenazan la seguridad de los Estados y, por lo tanto, de la sociedad internacional en su conjunto

La ciberguerra emerge como una alternativa de confrontación entre actores estatales y no estatales. Los primeros se han caracterizado por infringir ataques de mayor magnitud, dirección y daño, lo cual se ha traducido en la necesidad de realizar estudios para comprender el elemento cibernético como parte sustantiva de la seguridad, de las modalidades de confrontación interestatal en el escenario internacional, y sobre todo, en las agendas de seguridad nacional de cada país.

Esta investigación tiene como objetivo general exponer un panorama sobre la configuración de la ciberguerra como nueva estrategia de confrontación interestatal, así como presentar los casos de ciberguerra entre Estados Unidos de América y la Federación Rusa, para ello se incluyen implicaciones y ejemplos suscitados en el período comprendido de 2007 a 2020. Finalmente, se pretende analizar a la ciberseguridad como un aspecto esencial de la agenda de seguridad internacional actual, ya que se erige como una necesidad que demanda el contexto tecnológico del que son parte.

En 2007 se suscitó en Estonia un ciberataque de gran magnitud, si bien en ese momento no se pudo comprobar que dicho ataque fuera directamente orquestado por el gobierno ruso, muchos teóricos y analistas, entre los que resalta el experto en los sucesos socio-cibernéticos; Richard Clarke, lo han afirmado conforme el caso se ha estudiado con mayor profundidad.

El caso de Estonia marcó la presencia de una forma peculiar de ataque: la ciberguerra, este concepto emergió de forma contundente no sólo por haber afectado a casi toda la población del país, sino también por todas las esferas sociales que trastocó. Por citar algunos ejemplos; las páginas web de bancos, medios de prensa y organismos gubernamentales colapsaron debido a niveles sin precedente de tráfico en la internet.[1] Este caso marcó un antes y un después para el análisis de las confrontaciones entre Estados, y del tema de la ciberdefensa. En este contexto, es que se considera a Estonia como el primer ataque orquestado a través del ciberespacio cuyas afectaciones fueron consideradas de gran escala.

Otro referente se encuentra en los ciberataques de procedencia internacional, como el caso de Kosovo (1999), Taiwán (2003), NASA (2006), y Stuxnet (2010). Sin embargo, el ataque a Estonia fue determinante por su carácter estatal y, más aún, por su carácter público ante la escala de los daños ocasionados. Los ciberataques coordinados, se realizaron contra instituciones gubernamentales, medios de comunicación, la banca, así como contra servidores y enrutadores específicos.

Los ataques cibernéticos de 2007 demostraron la situación de seguridad y ciberseguridad en Estonia, además de evidenciar un punto de inflexión en los esfuerzos de dicho país para aumentar su posición estratégica en la OTAN. A su vez, éstos hechos revelaron debilidades y desafíos que enfrenta la Alianza de la OTAN y abrieron la puerta a la discusión pública sobre la magnitud de los daños originados por los ataques, destacando la necesidad de cooperación internacional.

En este contexto, se reconoció el liderazgo de defensa cibernética de Estonia y junto con otras seis naciones (España, Alemania, Italia, Letonia, Lituania y Eslovaquia)

[1] Damien McGuinness, “Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país”, *BBC News Mundo*, Reino Unido, 6 de mayo 2017.

se estableció el Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN (CCDCOE) en Tallin.

En 2019 se planteó la Estrategia de Seguridad Cibernética, en la que se reconoció que, al menos para Estonia en ese momento, la guerra cibernética no significa proveer soluciones tecnológicas, sino proteger a la sociedad digital y la forma de vida en general. En este sentido, la evolución de los espacios bélicos se ha transformado por el desarrollo científico tecnológico y por el desarrollo de estrategias para enfrentarse en los dominios terrestre, naval, o aéreo y, en últimas instancias, espacial.

En el siglo XXI emerge una quinta dimensión: lo virtual, donde el ser humano ha sido capaz de trasladar esta práctica, reconfigurando la concepción de conflicto, soldado, arma y, ataque[2]. El espacio cibernético es una posibilidad latente para el conflicto moderno, y no solo significa que es un nuevo espacio para la confrontación dentro de toda la gama prexistente (terrestre, aéreo, marino, espacial), sino que también modifica el tipo de conflicto y sus dinámicas. A diferencia de los otros dominios, el ciberespacio se caracteriza por el anonimato, la velocidad para efectuar un daño a los sistemas de necesidades primarias de los Estados es sumamente barato y con pocos elementos requeridos para poder vulnerar, principalmente, por la discreción que comporta.

Al indagar el contexto de la nación rusa encontramos como antecedente especial lo acontecido en 2007. En ese año el país experimentaba una apertura urgente con el exterior; siguiendo la línea de Vladimir Putin sobre el tema del multilateralismo como parte característica de su campaña y administración. En dicho momento prevalecían problemas que enfrentaba en sus fronteras, como resultado de la caída de la Unión de Repúblicas Socialistas Soviéticas (URSS). En ese contexto, Rusia comenzó a suministrar recursos para el desarrollo armamentista nacional pero también con otros países como es el caso de Irán en cuestiones nucleares (acuerdo nuclear a largo plazo firmado por el Kremlin en 2001), y la venta de lanzadores de misiles S-300. Este hecho llamó la atención de la comunidad internacional, un ejemplo es que en este año las relaciones diplomáticas con Gran Bretaña y Alemania se deterioraron. En el área social existían protestas en Georgia y Estonia, principalmente, por la entrada del ejército ruso

[2] Andrés Gaitán Rodríguez, *Ciberguerra: La consolidación de un nuevo poder en las relaciones internacionales contemporáneas*. Bogotá, Universidad de Santo Tomás. 2018, p. 114.

en sus territorios, y con Bielorrusia por el corte de suministros de gasoductos. No obstante, muchos de los conflictos que vivían al exterior se debían al desarrollo de la tecnología, de la cual no se sabía con precisión la intención que tendría su uso[3].

En el contexto estadounidense, el país se recuperaba de la crisis económica de 2005, y aprovechando la estabilidad económica lograda, se acrecentó el desarrollo armamentista, no sólo bajo el marco de los conflictos en Medio Oriente y bajo las políticas bélicas puestas en marcha con la guerra en Afganistán; sino que paralelamente también hacia el perfeccionamiento de las tácticas militares y de las armas, como prioridad en el gobierno de George W. Bush.

En este sentido, es necesario destacar que la caída de la URSS y el fin de la Guerra Fría significaron un parteaguas en la historia universal. Sin embargo, el sentido de competencia entre Estados Unidos y Rusia no había finalizado pues se originó una nueva dinámica en el contexto de la ola tecnológica del siglo XXI.

Hoy en día, ambos países han desarrollado protocolos de seguridad cibernética para prevenir los ataques a sus bases de datos más importantes, sin embargo, son millones los ataques que se reciben a diario. Si bien, actualmente países como China, Israel, Irán y Corea del Norte han mostrado un incremento en su rivalidad con Estados Unidos en cuestiones de ciberataques/ciberguerra, Rusia es el país del cual no solo se originan dichos ciberataques a Estados Unidos, sino el único país que también los recibe de forma constante desde 2007, según datos recabados del *Digital Attack Map* de Arbor Networks (mapa interactivo que muestra los ciberataques en tiempo real y en años anteriores).

El impacto del contexto hipertecnologizado en la sociedad internacional, abre otro canal no antes considerado en el elevado riesgo para la seguridad nacional e internacional. Por ello es imperativo considerar la seguridad cibernética como eje fundamental para la conformación de las Agendas de Seguridad Nacional, no solo de Rusia y de Estados Unidos, sino de todos los países como una prioridad.

[3] Ria Novosti, “Diez acontecimientos internacionales más importantes para Rusia en 2007”, *Sputnik News Internacional*, Rusia, 2 de enero 2008.

En temas de seguridad cibernética y defensa, actualmente son pocos los países que dentro de su Agenda de Seguridad Nacional consideran la ciberguerra como un área de atención prioritaria. La última encuesta realizada por la Unión Internacional de Telecomunicaciones (UIT), clasifica a los países con base en cinco criterios, mismos que se mencionan a continuación: 1) aquellos que tienen la capacidad de enjuiciar a los *hackers*; 2) los que cuentan con la capacidad técnica para prevenir ataques cibernéticos; 3) los esfuerzos para cooperar en la materia con otros países; 4) la fortaleza que tiene la industria local en materia de ciberseguridad; y, por último, 5) la forma en que está organizada la agencia u organismo nacional dedicado a promover y lograr la seguridad cibernética gubernamental.

Estados Unidos posee una de las mejores infraestructuras de ciberseguridad en el mundo, situación que va de la mano con sus pilares de seguridad cibernética nacional; con una puntuación del 91% se sitúa por delante de Malasia (89%), y detrás del primer lugar, Singapur (92%). Además de estos tres países, la lista de los 10 países de la UIT incluye a países desarrollados como Francia, Canadá y Australia, y también a países menos desarrollados, como Estonia, Mauricio y Georgia. El único país de Oriente Medio en el listado es Omán, que ocupó el cuarto lugar.[4]

No obstante, en el contexto mundial, los países, atraviesan por procesos coyunturales como lo son elecciones, emergencias sanitarias, problemas en la administración pública, repartición de recursos, estabilidad bancaria, multilateralismo, etc., desplazando la atención y recursos asociados a la ciberseguridad nacional e internacional, lo que deriva en el paulatino desinterés y falta de apoyo.

El perfeccionamiento de la tecnología avanza a pasos agigantados y sin verdaderas estrategias nacionales y/o acuerdos que regulen la ciberseguridad y eviten la ciberguerra con canales de cooperación multilateral, la amenaza de desarrollar y ocupar el espacio *ciber* para el conflicto y la búsqueda de poder, se acrecientan.

El creciente riesgo, no solo se refleja en los datos sobre ciberseguridad que arroja cada país, en las tensiones políticas que pueden tener lugar por acusaciones de

[4] Ulises León Kandiko, "¿Qué países son los mejores en ciberseguridad?", *CXO- Community Latam*, Buenos Aires, 14 de julio 2017.

ciberataques entre Estados y que daña la relación entre los mismos; sino que vulnera la seguridad humana de millones de civiles, sus derechos en diversas esferas, etc., los cuales sufren directa, y mayoritariamente, las consecuencias de la desatención a la protección cibernética, misma que debido al contexto actual debería encontrarse dentro de las áreas de atención predilectas.

1. La ciberguerra en el escenario internacional.

Actualmente cualquier área o actividad humana está interconectada: los sistemas de defensa, de seguridad, comerciales, energéticos, sanitarios, comunicaciones, de transporte, bancarios, alumbramiento y todo lo que afecta tanto nuestra vida diaria, como la seguridad de los Estados como tal. Antes, cuando se hablaba de ciberseguridad, ésta se enmarcaba en el contexto de las *"low politics"* [5]*, ya que no se consideraba como algo vital para preservar la seguridad y la supervivencia del Estado, se trataba como un tema económico o social que no afectaba el bienestar de este.[6]

A partir de la interconexión descrita con anterioridad es que la red ha evolucionado en su grado de relevancia e influencia dentro de la dinámica mundial. La tecnología y el espacio cibernético han repuntado desde finales del siglo pasado como un elemento fundamental para la supervivencia de los Estados, tanto a nivel nacional como internacional en materia de seguridad y defensa. Por lo que la ciberseguridad se enmarca en las "*high politics*" *; que significa el riesgo potencial que representa el acceso a la tecnología como herramienta facilitadora para causar daño, razón fundamental que constituye una llamada de atención para su estudio y regulación, ya que es complejo conocer los límites de un espacio que no tiene materialmente un alcance definido.

En el presente capítulo se abordará el estudio de la ciberguerra, en el escenario internacional como una alternativa potencial de conflicto, que desde el enfoque neorrealista será necesario conocer las implicaciones de su implementación, sus características y la amenaza que supone para la seguridad de los Estados, en específico. Además, se destacarán los actores y objetivos que persiguen los ataques cibernéticos, sin dejar de lado los preceptos teóricos neorrealistas y los conceptos que contextualizan a la ciberguerra como un canal que implementa la tecnología, a través del ciberespacio; y, como una herramienta que condiciona el conflicto entre Estados.

---

[5] *Robert Keohane y Joseph Nye, en su modelo de interdependencia compleja, consideran tres postulados dentro de los cuales explican que "prevalece una jerarquía en las cuestiones de política internacional, según la cual una "alta política" formada por asuntos de defensa y seguridad y, a la cual está subordinada la "baja política" de los temas "socioeconómicos". Véase: Robert Keohane; Joseph S. Nye, *Power and Interdependence*, New York, Longman, 2000, 3rd edition.

[6] Gema Sánchez Medero, "El ciberespionaje", *Derecom. Revista Internacional de Derecho de la Comunicación y de las Nuevas Tecnologías,* Nueva Época, España, No. 13, marzo-mayo 2013, 115p.

1.1 Caracterización de la ciberguerra.

El desarrollo tecnológico ha modificado la forma como las confrontaciones toman lugar a lo largo de la historia de las relaciones internacionales y de igual manera, ha servido como motor para la innovación. El saber humano ha definido la evolución de comunicaciones y transportes, y también en las herramientas y estrategias para hacer la guerra.

Fernando Sampaio, investigador de la Organización para Estudios Científicos de Brasil, propone que, tras la aparición de la tecnología, ha existido una dependencia entre el ser humano social y el ciberespacio, expresado en sus recursos tangibles e intangibles, y con la intención de facilitar los procesos cotidianos. Sin embargo, la relación que expone ha sido nociva por el grado de potencial y vulnerabilidad que ha creado en la seguridad de los Estados y de todos los actores que de él dependen. Lo anterior ha construido y constituido espacios de debilidad que pueden ser aprovechados y penetrados por un enemigo para atacar las estructuras que el Estado haya colocado en control del ciberespacio.[7]

La capacidad tecnológica se puede observar en el dominio de un nuevo espectro; lejano a las armas tradicionales que poseen los Estados y las fuerzas militares, así como su capacidad convencional, atrae nuevas amenazas a cualquier sistema de carácter gubernamental, militar, económico, o social que forme parte del ciberespacio.[8]

El rol que desempeña la tecnología de guerra en escenarios de conflicto se refleja de distintas formas; desde el inicio de la historia humana las flechas y catapultas, pasando por los fusiles, los tanques, los barcos de guerra, submarinos, hasta los portaaviones, los modernos misiles y robots de guerra. El ser humano se encuentra actualmente en medio de una explosión tecnológico-armamentista que ha introducido vehículos no tripulados como drones, armas de energía nuclear, misiles balísticos, entre otros a la escena del conflicto entre diversos actores estatales. Cabe resaltar que, en esta nueva etapa, al desarrollo tecnológico se le ha encaminado a disponer de toda arma

---

[7] Fernando Sampaio, “Ciberguerra: guerra eletrônica e informacional, um novo desafio estratégico”. *Escola Superior de Geopolítica e Estratégia*. Porto Alegre, Brasil, Organização para Estudos Científicos (OEC)*,* 2001.

[8] Stevenson G. Smith, “Recognizing and preparing loss estimates from cyber-attacks”. *Information Systems Security*, Dakota, Estados Unidos, Jan/Feb 2004; 12, 6. México, ISSUE, 2004, Vol. 12, pp. 46-57.

materialmente existente; adaptándolo a estrategias más discretas, pero sin duda con igual o mayor letalidad que la de las armas convencionales: las armas cibernéticas en una nueva modalidad de conflicto, la ciberguerra.

En el escenario internacional, la ciberguerra aparece como una posibilidad cada vez más viable para los Estados en su búsqueda por la obtención del poder. Debido al bajo costo, precisión, y rapidez, la implementación de esta modalidad como medida de disuasión y confrontación ha ido en aumento. Los Estados, en primer lugar, están empleando el ciberespacio para conseguir información de sus "posibles" enemigos potenciales. Con la presencia de *hackers* o cibersoldados que se introducen en un servidor mediante un *software*, archivos adjuntos de correo electrónico o aprovechando las vulnerabilidades de los navegadores de internet, logran conseguir los *passwords* (contraseñas) necesarios para adentrarse en un determinado sistema y generar daños u obtener información, controlar webs, tomar el mando de los ordenadores, borrar ficheros, formatear el disco duro, averiguar las actividades que está realizando el usuario, capturar pantallazos, etc.

De esta manera, los Estados pueden obtener información que resulta muy valiosa para sus intereses, ya que les permite acceder a datos sobre los avances de otros países relacionados con las operaciones defensivas y ofensivas[9], desaparecerlos o manipularlos.

Algunos ejemplos, son los hechos ocurridos en Estonia en 2007, a consecuencia de los ataques recibidos desde Rusia (en ese momento se acuña el término ciberguerra), otro suceso fue Stuxnet 2010, en la Planta Natans en Irán, o el *malware Flame* en 2012 y su robo de datos a países de Medio Oriente. Los casos anteriores dieron pie a tensiones cada vez mayores y frecuentes entre Estados. En ese contexto emergen una serie de debates en torno a los impactos nocivos a la vulneración de la seguridad y soberanía de los Estados, así como el tema de la regulación de un espacio que se estructura como idóneo para la confrontación interestatal.

Por norma general, se considera que los ciberataques son más baratos que los ataques físicos, y a su vez, las repercusiones sobre la infraestructura crítica pueden ser

[9] Gema Sánchez Medero, "Internet: Una herramienta para las guerras del Siglo XXI", *Revista Política y Estrategia,* España, Academia Nacional de Estudios Políticos y Estratégico, N° 114, 2009.

de igual o mayor capacidad de daño que el que ocasionan las armas convencionales. Lo anterior debido a que las herramientas que se necesitan para llevar a cabo un ciberataque son de fácil acceso y son asequibles tanto para Estados como para otros actores de las relaciones internacionales (transnacionales, organizaciones intergubernamentales, fuerzas transnacionales, etc.), y también para los grupos de crimen organizado o *hackers* independientes.[10] En un mundo hiperconectado e hiperinformatizado como el actual, cualquier impacto en el corazón de los canales de información y de tecnología, podría generar pérdidas millonarias a cualquier país o institución, además del daño y las repercusiones que representan en la materialización de los ataques orquestados en la infraestructura crítica que desestabilizan la dinámica de cualquier país.

En las últimas décadas, el concepto tradicional del conflicto bélico ha venido experimentado una metamorfosis que se explica en gran medida por los avances en materia de tecnología, comunicación e información, los cuales han posibilitado la introducción de los enfrentamientos a un nuevo ámbito de hostilidades: el ciberespacio.[11] El ex subsecretario de Defensa de Estados Unidos, William J. Lynn, precisó en 2010 que la ciberguerra fue reconocida por el Pentágono como un nuevo escenario de conflicto en el que las operaciones militares son tan importantes como en los frentes tradicionales:

> A partir de la posguerra fría, se plantea una nueva tipología de batalla que se caracteriza por el empleo de las computadoras y la comunicación en red (que integra a las terminales al sistema mundial) para atacar a un enemigo mediante el empleo de información con fines psicológicos y de desarticulación logística, o por hacer uso de las tecnologías de la información para la organización estratégica, operacional y logística de los diversos componentes y recursos de las fuerzas militares a nivel global.[12]

Por una parte, la cibernética fue definida como el estudio teórico de los procesos de comunicación y de control en sistemas biológicos, mecánicos y artificiales; su nombre proviene de la voz griega *kybernetes*, traducida como timonel o gobierno, y la

---

[10] Enrique Fojón; Adolfo Hernández, "#BásicosPolext: Riesgos del Ciberespacio", *Estudios de Política Exterior*, España, 2014.
[11] Sergio Villaescusa, "Ensayo sobre vulnerabilidad cibernética", *CISDE Observatorio,* España, 2016
[12] Ryan Henry; Edward Peartree, *"Military theory and information warfare"* Parameters, Center for Strategic & International Studies, 28, 1998, 121-135 p.

comunicación se asocia con las nociones de control, regulación y dominio[13]. Por otra parte; etimológicamente deriva del prefijo *ciber,* el cual hace referencia a una relación con redes informáticas, según la Diccionario de la Real Academia Española.

Norbert Wiener, la define como "la ciencia del control y la comunicación entre el animal y la máquina, el arte de la dirección"[14]. La cibernética estudia los flujos de información que rodean un sistema y la forma en que esta información es usada por éste como un valor que le permite controlarse a sí mismo. Entonces, la información es para la teoría cibernética un elemento fundamental para la organización del sistema.[15]

Es imperativo desprender a partir de las definiciones anteriores, los conceptos eje para el total entendimiento del espacio dentro del que se encuentra el tema de estudio, la ciberguerra. Es preciso comenzar por comprender al espacio dentro del cual ésta se lleva a cabo, el ciberespacio. A principios de los años 80, William Ford Gibson III, un escritor de ciencia ficción, acuñó el término "ciberespacio" por primera vez para describir una red de computadoras ficticia y sus interconexiones, que contenía enormes cantidades de información que podría explotarse con el fin de adquirir riqueza y poder.

Para el escritor y filósofo tunecino **Pierre Levy**, el ciberespacio "designa el universo de redes digitales como un mundo de interacción y aventura, [es] el espacio de conflictos globales y una nueva frontera económica y cultural".[16]

El **Dr. Rafael De Gasperin** elaboró una noción del concepto con una comparación respecto al internet, y menciona que el ciberespacio y la Internet no son lo mismo; Internet es la infraestructura y el ciberespacio es el contenido. Generalmente los usuarios también forman parte del contenido a través del correo electrónico, la web, los *newsgroups*, las listas, el Gopher, algoritmos, etc. El ciberespacio es multiusuario, aunque no siempre lo es en tiempo real."[17] Sin embargo, en contraste a este postulado, es el ciberespacio más amplio que la internet (y la engloba) ya que es el área en que,

---

[13] Ignacio Siles, "Cibernética y sociedad de la información: el retorno de un sueño eterno", *Signo y Pensamiento*, Bogotá, Núm. 50, 2007.
[14] Norbert Wiener "*Cibernética o el control y comunicación en animales y máquinas".* Barcelona Tusquets, 1998. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5206500
[15] Andrés Gaitán Rodríguez, *Op. Cit.*
[16] Pierre Levy, "*¿Qué es el ciberespacio?",* España, Editorial: Paidos Ibérica,1997.
[17] Rafael De Gasperin, *"Adolescencia y ciberespacio"*, *Revista OEI*, Monografías virtuales: ciudadanía, democracia y valores y sociedades plurales. Línea temática: Valores y TICs, Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura, núm. 5, 2005.

mediante navegadores, servidores y conexión a internet, se llevan a cabo e incluyen las interacciones en línea, no solo la conexión física de dispositivos. Tal como lo describe el *Security Service* (MI5), comprende "los medios electrónicos de las redes digitales utilizados para almacenar, modificar y comunicar la información. Incluye no solamente el internet, sino también otros sistemas de información que soportan las empresas, infraestructuras y servicios."[18]

Además, el espacio cibernético se ha convertido así en una alternativa para la sociedad digital (o cibernética), hecha posible mediante computadoras y redes de computadoras. Cuando se hace referencia al mismo, de forma abstracta, significa la suma total de información disponible electrónicamente, el intercambio de esa información y las comunidades que emergen como consecuencia del uso de esa información.[19]

A partir de que la tecnología se incorpora como una herramienta que condiciona el contexto y, a su vez, a la dinámica social, es que nace una relación entre la sociedad, la tecnología y la información. Es por tanto que el orden social también se modifica al formar parte del nuevo espacio cibernético emergente. Nuevas comunidades nacen dentro de este ciberespacio, llamada "cibersociedad" o "sociedad cibernética", que consiste en "una sociedad basada en la información y el conocimiento gestionados por las nuevas tecnologías. Tecnologías que se aplican sobre el conocimiento y no al revés como en las anteriores revoluciones científicas"[20]

Con anterioridad se ha definido lo ciber como parte del concepto ciberguerra, por su parte la palabra "guerra", que conforma a dicho concepto proviene del germano "werra" que quiere decir pelea o discordia; conferido del alto alemán antiguo "wërra" y del neerlandés medio «warre». Han sido muchos los autores que han brindado su propia definición al respecto; desde las concepciones griegas más antiguas como la del filósofo Aristóteles, siendo la guerra "un medio violento para obtener y defender el derecho de una ciudad", pasando por el precepto de **Carl Von Clausewitz**, "la guerra es la

[18] MI5, *The Threats: Cyber*. Reino Unido, https://www.mi5.gov.uk/cyber
[19] Luis Manuel Martínez; Paula Elvira Ceceñas Torrero; Verónica Clementina Ontiveros Hernández (Coor.), *Virtualidad, ciberespacio y comunidades virtuales*, México, Red Durango de Investigadores Educativos, 2014, 144 pp.
[20] Jesús Fernández; David Molina, "Cibersociedad y ciencias humanas: el caso de la Historia Actual", *Revista TEXTOS de la CiberSociedad*, Argentina, núm. 9, 2006.

continuación de la política por otros medios. Trastoca el Estado y trasciende de las fronteras" y retomada por Foucault, ésta ha ido incorporando elementos conforme se han perfeccionado las estrategias, armas y espacios para llevarla a cabo y a su vez llegar a una definición más elaborada que englobe la mayoría de sus características.

La Real Academia Española, define la guerra como una "desavenencia y rompimiento de la paz entre dos o más potencias. La guerra puede definirse como una lucha armada entre dos o más Estados, o entre sectores de un mismo país (guerra civil). También se llama guerra a la oposición violenta entre dos o más personas por distintos intereses."

Para **Max Sorensen**, "la guerra es el nombre tradicional de una contienda entre dos o más Estados, en la cual sus respectivas fuerzas armadas están enfrentadas en acciones de violencia recíproca. El fin de la guerra es derrotar a la otra parte e imponer los términos de paz que el ganador esté dispuesto a conceder."[21]

La tendencia del ser humano a extender el empleo de la fuerza a nuevos escenarios de confrontación con el fin de desarrollar nuevos tipos de estrategias para ganar la guerra, parte de la existencia y validez que ha representado el poder en la historia bélica-militar.[22] En primera instancia el conflicto se desarrolló en el escenario terrestre, evolucionando al plano marítimo, para finalmente alcanzar la altura de la atmósfera y la estratósfera. Lo anterior ha sido producto de los procesos de desarrollo científico propio de las naciones y, por ende, de sus ejércitos. La evolución y traslado de los escenarios donde la guerra acontecía no habría sido posible, si el ser humano, a través de la tecnología no lo hubiera hecho así: posteriormente a la constitución del poder terrestre, que surgiera el marítimo con sus distintivos submarinos; el aéreo con las aeronaves y portamisiles y; espacial, llevando a la gravedad cero cohetes en una carrera por llegar a espacios menos explorados, así como centros espaciales de alta tecnología.

El desarrollo bélico depositó en su eje primario la creación de una industria armamentista que de primera mano le permitiera protegerse de los animales (armas defensivas), o atacarlos (armas ofensivas) para conseguir alimento; esto evidencia que el ser humano pensaba en sobrevivir como objetivo básico. "La guerra sería el producto

[21] Max Sorensen, *"Manual of International Law"*, New York: St. Martin's Press, 1998, 771 pp.
[22] Andrés Gaitán Rodríguez, *Op. Cit.*

paulatino cada vez que el hombre se convirtió en sujeto organizado en unidades políticas y vinieron los conflictos por intereses comunes".[23]

Christopher Bellamy, afirma que la guerra es un fenómeno adscrito históricamente al escenario terrestre[24]. Sin embargo, ésta trascendió espacios debido a la tecnología aplicada, por más primitiva que fuera en un principio, y así, extender la práctica bélica, perfeccionarla, y dotarla de un mayor alcance.

Tomando en cuenta las definiciones anteriores que conforman al concepto de ciberguerra, es que es necesario destacar que las concepciones que se tienen de ella son variadas. De acuerdo con **Richard Clarke**, ex funcionario del gobierno estadounidense y experto en seguridad, la ciberguerra se define como el "conjunto de acciones llevadas a cabo por un Estado-Nación para infiltrarse en las computadoras o redes de otro, con el objetivo de generar un daño".[25] En el ciberespacio se guarda toda la información y comunicación disponible de una red, y la ciberguerra es su mayor amenaza. Sus tácticas consisten en identificar vulnerabilidades y hackear sistemas para acceder a dicha información, afectando desde la institucionalidad de un país hasta su estructura crítica.

También conocida como "guerra cibernética", es una modalidad de guerra donde la conflictividad no ocurre con armas físicas, sino a través de la confrontación con medios electrónicos e informáticos en el ciberespacio. En su uso más común y libre, el término se utiliza para designar ataques, represalias o intrusión ilícita en un ordenador o en una red.

A su vez, para la investigadora española **Gema Sánchez Medero**, el concepto de ciberguerra puede ser entendido como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponer la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación y alterar sus bases de datos; es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la

[23] Luis Ángel Gutiérrez, "Evolución de la tecnología militar y "su impacto" en España", *Cuadernos de Estrategia*, España, núm. 75, 1995, p. 83.
[24]Christopher Bellamy, *The evolution of modern land warfare: Theory and practice*, Londres, Routledge, 2015.
[25] Simón Vargas Aguilar, "Guerra Cibernética: la nueva amenaza", *La Jornada*, México, julio 2013.

violencia física sino un ataque informático que va desde “la infiltración en los sistemas informáticos enemigos para obtener información, hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento, etc.” [26]

La ciberguerra se puede describir como “el uso de capacidades basadas en la red de un Estado, para interrumpir, denegar, degradar, manipular o destruir información residente en computadores y redes de ellos, o los propios ordenadores y las redes de otro Estado”[27]

Para **Kevin Coleman**, la guerra cibernética se define como “un conflicto que utiliza transacciones hostiles o ataques a ordenadores y redes en un esfuerzo por interrumpir las comunicaciones y otras piezas de la infraestructura, como un mecanismo para infligir daño económico o alterar y atacar las defensas”. Por otro lado, **Nils Melzer** afirma que la ciberguerra, en su definición más básica es “la guerra llevada a cabo en el ciberespacio a través de medios y métodos cibernéticos”

La **RAND Corporation (s.f.)**, tanque de pensamiento estadounidense en constante trabajo conjunto con las Fuerzas Militares norteamericanas, define la ciberguerra como aquella que “involucra las acciones de una organización del Estado nacional o internacional para atacar y tratar de dañar las computadoras de otra nación o redes de información a través de, por ejemplo, virus informáticos o ataques de denegación de servicios”.

Las implicaciones y aproximaciones que rodean a la ciberguerra como una modalidad de conflicto en un espacio de reciente creación son bastas. La concepción sobre los elementos que la conforman se actualiza y enriquece conforme el estudio de esta avanza, paralelamente, con los fenómenos que se presentan día a día dentro del mismo. Reconocer de manera totalitaria dicho espacio y las variables que rodean al conflicto cibernético, demanda partir de los preceptos más básicos como lo son sus

[26] Raymond Colle, “Internet: un cuerpo enfermo y un campo de batalla”, *Revista Latina de Comunicación Social*, Tenerife, España, núm. 30, junio 2000.
[27] CESEDEN; Grupo de trabajo Nº3, *Guerra Cibernética: Aspectos organizativos. XXXIII Curso de Defensa Nacional,* España, Centro Superior de Estudios de la Defensa Nacional, 2013.

definiciones, aún más, en un espacio cuyas fronteras no son palpables, y mucho menos sus alcances.

1.2 Aproximaciones teórico-conceptuales desde el neorrealismo para el análisis del fenómeno de la ciberguerra.

Para desarrollar esta investigación, nos apegamos a los preceptos de los postulados neorrealistas, la cual surge a finales de la década de 1970, a partir del trabajo *La Teoría de la Política Internacional* de **Kenneth Waltz**. Para él, el sistema internacional consiste en un número de grandes potencias, cada una tratando de sobrevivir en un ambiente descentralizado y anárquico. Se refiere a un sistema conformado por Estados soberanos donde no existe un sistema central por encima de las unidades que lo componen. Ese escenario de anarquía previene a los actores del sistema internacional de ingresar a sistemas cooperativos para terminar el estado de guerra.

El neorrealismo parte de una nueva concepción científica, que se asume como una aproximación objetiva, deductiva, abstractiva y predictiva, que busca apartarse del realismo y del "Behaviorismo". La propuesta neorrealista se basa en la anarquía del sistema y se enfoca en el tercer nivel de análisis, el cual reside en el sistema internacional conformado por el resultado de las interacciones entre los Estados. Dentro de esta situación internacional, los Estados, dado su inalienable deseo de supervivencia, se alinean de manera automática para generar un equilibrio entre potencias.[28]

Para el neorrealismo, el foco de estudio está en la estructura del sistema internacional y cómo ésta modela la forma en la cual los componentes se vinculan entre sí. Indica que la estructura del sistema internacional lleva a las grandes potencias a prestar especial atención a la relación de fuerzas y obliga a los Estados a priorizar ante todo su seguridad, así como a competir entre sí por el poder, ya que el poder es el mejor medio para la supervivencia.

A su vez, refiere que la causa del conflicto en el sistema internacional se debe a la estructura anárquica del mismo. Sin embargo, afirma que la ausencia de una autoridad central no implica una falta de organización, sino otra forma de organización. La

[28] Carlos Torres White, *Las teorías tradicionales de las Relaciones Internacionales*, México, Centro Iberoamericano de Estudios Internacionales, Colombia, 2017.

estructura en el caso de estudio corresponde a los Estados en la región y en el mundo, de la cual forman parte Estados Unidos y Rusia (Cap. 3), así como todos los actores estatales del sistema internacional que se ven afectados por los movimientos al interior de cada uno de ellos. Cada actor produce un efecto en la estructura a partir de cambios internos en sus políticas; en este caso en el aumento de capacidades que afecta la posición relativa de cada uno dentro de la estructura[29]

Barry B. Hughes, profesor de la Universidad de Denver e investigador, señala en su libro *Continuity and Change in World Politics* (1999) que los teóricos de la aproximación neorrealista introducen dos elementos clave para el entendimiento de la dinámica internacional; por un lado, tenemos a las relaciones entre sistema y estructura; y, por el otro, el tema de la distribución de capacidades que se mide en términos de fuerza y poder militar. En el primero, Hughes apunta que los neorrealistas dirigen su atención a las estructuras sistémicas del escenario internacional, a la distribución de capacidades dentro del sistema y a las implicaciones que las condiciones de éste tienen sobre el comportamiento individual del Estado. Por lo tanto, la anarquía es concentrada como una forma alternativa de organización, resultando así en que los Estados con mayores capacidades relativas son quienes tienen una mayor voz en la estructura.[30] Respecto al segundo elemento, destaca que dichas capacidades son las que configuran la posición de cada Estado frente a los demás, tanto a nivel regional, como a nivel mundial; lo cual se traduce en líneas aéreas, terrestres, marítimas, nucleares, y recientemente, cibernético-tecnológicas.

Dichas capacidades actúan con un arma de dos filos en la lógica de la disuasión a través de la fuerza o de la demostración de ésta, lo cual se refleja ineludiblemente en la estructura del sistema internacional. De acuerdo con sus intereses que los Estados, en caso específico, son los que pueden mantener o modificar el *statu quo* a través del desarrollo de carreras armamentistas, entendiendo que dentro de este marco la teoría y la realidad social han demandado también la consideración de los “virus” o mejor

[29] Daniel A. Gómez Llinás*, Análisis del ciberataque para la seguridad de los estados y su incidencia en la transformación del status quo: Stuxnet el virus informático*, Bogotá, Colombia, Universidad Colegio Mayor de Nuestra Señora del Rosario, Facultad de Relaciones Internacionales, 2017, 34 pp.

[30] Senny Hernández, *“*La teoría del realismo estructuralista y las interacciones entre los Estados en el escenario internacional”, *Revista Venezolana de Análisis de Coyuntura*, Venezuela, Vol. 14, núm 2, 2008, pp. 18-19.

denominadas, “armas cibernéticas” en dichas carreras. Al suscitarse un cambio en esta balanza podría originar inseguridad para otros Estados y/o actores, y por supuesto un cambio en la dinámica internacional.

La balanza del poder, ya mencionada con anterioridad, se asocia a la estructura planteada por los preceptos neorrealistas, debido a que en ella es como se reflejan y entienden los aumentos de las capacidades relativas de un Estado frente a los demás actores en el sistema.[31] Con relación a esta balanza subjetiva donde la distribución del poder (conjunto de capacidades para subordinar), Waltz afirma que el balance de éste se asocia con las capacidades que tienen los Estados en un momento dado dentro de la historia y se refiere a la polaridad del sistema; es decir, a la inclinación de la balanza en el sistema internacional, sea bipolar o multipolar, según el número de potencias que concentren el poder.[32]

Es importante destacar que el enfoque teórico neorrealista considera espacios emergentes de confrontación en el mundo a partir de la incorporación de nuevos temas y amenazas para la seguridad de los Estados. De esto se deriva como consecuencia la aparición de otros actores no estatales dentro de la imagen de análisis del escenario internacional (*Think Tanks*, organizaciones no gubernamentales, corporaciones, organizaciones autónomas descentralizadas, ciudadanos particulares, etc.) así como la incorporación de herramientas y/o medios empleados (*malwares*, virus informáticos, gusanos cibernéticos, etc.).

Si bien con anterioridad se retomó el concepto de Kenneth Waltz (2007) sobre el poder. De forma general, es necesario destacar que la aproximación neorrealista desarrolla una desagregación del concepto de poder, en tres categorías: económico, político y militar, hecho que permite contar con más elementos y soltura explicativa al momento de analizar los fenómenos contemporáneos. Aunado a esa desagregación, es que las amenazas y sucesos acontecidos en el ciberespacio, guiados a la obtención de poder, emergen y repercuten en las categorías antes enunciadas debido a la diversidad de objetivos que los ataques cibernéticos persiguen, lo cual se tratará con mayor detenimiento más adelante.

[31] Ibid., pp. 22-24.
[32] Ibid., pp. 23-24.

En suma, para el neorrealismo el poder es la capacidad combinada de un Estado para salvaguardar su integridad y actuar bajo su interés nacional, de acuerdo con su estructura, distribución de capacidades y facultades para enfrentar los cambios de la sociedad internacional anárquica y plural, la cual es una condición necesaria para la supervivencia de los Estados. **Joseph Nye** por su parte, considera que los recursos de información son los que en la era tecnológica conceden dominio, considerando la explotación de toda la información posible mediante sistemas interconectados y la infraestructura que el ciberespacio brinda.[33]

Por otro lado, el concepto de seguridad es fundamental para erigir los términos en los que se enuncia, trata y fomenta en el escenario internacional. Es por tanto que en ello destaca el teórico **Barry Buzan**, quien entiende a la seguridad como "la búsqueda de estar libres de amenazas y la capacidad de los Estados y sociedades para mantener su identidad independiente y su integridad funcional frente a las fuerzas de cambio que percibe como hostiles"[34] Como señala el propio Buzan, habrá que tener presente que son varios los ámbitos a considerar en relación con la seguridad (seguridad militar, seguridad política, seguridad económica, seguridad social y seguridad medioambiental). Si bien todos ellos se encuentran claramente interrelacionados; en este sentido es que la ciberseguridad se introduce dentro de las diferentes variantes de seguridad que deben retomarse para abarcar con mayor totalidad el sentido de preservación.

Por su parte, **Virginia Ibarra** y **Mónica Nieves**, profesoras de la Facultad de Derecho de la Universidad de Uruguay, comprenden que la ciberseguridad es definida en líneas generales como "la seguridad de la información digital almacenada en redes electrónicas, aunque aún hoy no hay un consenso en su definición".[35] Sin embargo, la asociación internacional*, Information Systems Audit and Control Association* (ISACA), la define como la "protección de activos de información, a través del tratamiento de

[33] Joseph S. Nye, *Cyber Power*, United States, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010, p. 3.
[34] Traducción propia
[35] Virginia Ibarra y Mónica Nieves, *La seguridad internacional determinada por un mundo on-line: el Estado ante el desafío del terrorismo y la ciberseguridad.* Memorias " Argentina, Universidad Nacional de La Plata VIII Congreso de Relaciones Internacionales", 2016.

amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

De forma más completa el Departamento de Defensa de Estados Unidos, define la ciberseguridad como:

> La prevención de daños para la protección y restauración de computadoras, sistemas electrónicos de comunicación, servicios de comunicación electrónica, comunicaciones alámbricas y comunicación electrónica, incluyendo información contenida en ellos, para asegurar su disponibilidad, integridad, autenticidad, confidencialidad y no repudio.[36]

En un contexto de anarquía, búsqueda del poder y de preservación, deben considerarse los riesgos y amenazas que la ciberseguridad de cada Estado debe retomar en forma externa a su área de influencia y alcance, así como de control cibernético que le corresponda. Tomando en cuenta que la información, datos, o intromisión a los sistemas de control de las infraestructuras críticas, actualmente determinan en el ciberespacio una variable importante en el conflicto entre actores, y al mismo tiempo como un alto valor como herramienta de disuasión.

Desde el enfoque neorrealista, **Carrillo y Vargas**, definen a la ciberguerra como "el uso de capacidades basadas en la red de un Estado, para interrumpir, denegar, degradar, manipular o destruir información residente en ordenadores y redes de ordenadores, o los propios ordenadores y las redes de otro Estado".[37] Esto con el objetivo de dañar la infraestructura informática con la que cuenta el Estado, impidiendo que los flujos de operación del país funcionen correctamente debilitando y entorpeciendo la dinámica del mismo dentro de la esfera gubernamental, o directamente en las estructuras críticas que se traducen en repercusiones a la sociedad civil, demostrando así superioridad ante el Estado atacado. Todo esto a partir de un ciberataque, que de la forma más general se define como un ataque de ordenador a ordenador que afecta, inhabilita, destruye o toma el control de un sistema informático; o que daña o roba la información que dicho sistema contiene.

---

[36] Jaime Romero,"*Conceptualización de una Estrategia de Ciberseguridad para la Seguridad Nacional de México*". Revista Internacional de Ciencias Sociales y Humanidades, México, Universidad Autónoma de Tamaulipas, 2018, vol. XXVIII, núm. 2.

[37] César L. Carrillo Farfán; Deisy P. Vargas Cantor, *Ciberguerra: descripción de estrategias políticas internacionales y algunos planteamientos jurídicos para afrontarla*, Bogotá, Universidad Militar Nueva Granada, Facultad de Derecho, 2016, 114 pp.

A partir de las definiciones anteriores, es que destaca la característica de un nuevo espacio para la confrontación. En la lógica neorrealista, dicho conflicto se establece en un margen de anarquía en la que las capacidades de cada actor determinarán su seguridad y preservación. Así, en palabras de **Senny Hernández**, "los actores tienen mayor capacidad de establecer los parámetros bajos los cuales otros menos capaces se desenvuelven, brindándoles mayores posibilidades de maniobra dentro del sistema y en la estructura; es claro que cuando existe anarquía se puede dar otra forma de organización sistémica, en este caso una jerarquía a partir de las capacidades"[38].

Lo anterior, conduce a considerar a la cooperación en el marco neorrealista, la cual exclusivamente se erige a partir de un interés o sentido de supervivencia, donde las potencias con mayores capacidades incurren en ella determinando los ejes de dicha cooperación si para su interés en términos de seguridad le significa algún beneficio, o bien participan en ella como una formalidad de imagen dentro de la sociedad internacional.

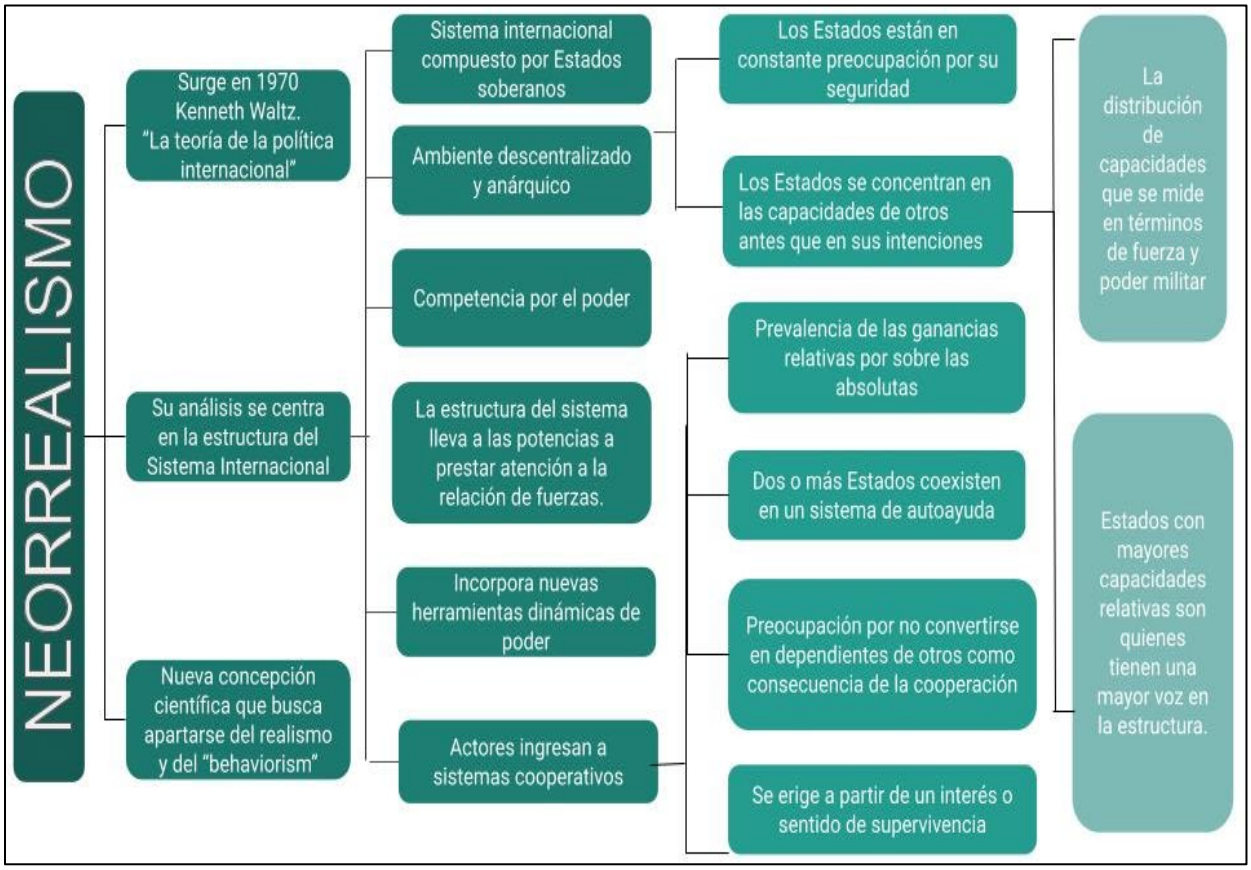
Asimismo, Hernández señala que cada Estado partirá de su capacidad para alzar la voz dentro del contexto anárquico; lo mismo sucede para las cuestiones cooperativas. En el caso de las hegemonías, las iniciativas de agrupación surgen a partir de una lógica diplomática, de interés común o de puntos de acuerdo regionales que ayuden a su desarrollo e imagen ante la sociedad internacional, mientras que a los actores más pequeños se apegan por un estricto sentido de preservación.

Caso contrario es cuando los hegemones (también en un sentido unilateral), impulsan particularmente acuerdos de cooperación con otros actores o Estados en específico, ya que sus capacidades se ven mermadas por las de otro, y por lo tanto le determinan un riesgo para su seguridad de forma más contundente. Por lo tanto, el sentido de cooperación en la lógica neorrealista en el conflicto cibernético apunta a la capacidad de los actores dentro de la estructura del sistema y cómo al interior pueda o no determinar una amenaza, en específico, para vulnerar las herramientas tecnológicas e infraestructuras críticas de cada uno.

[38] Senny Hernández, *Op. Cit.,* pp. 18-19.

A continuación, se expondrá un esquema con los aspectos que integran al enfoque neorrealista y que servirán de guía para conocer a lo largo de esta investigación los límites y las percepciones que los actores tienen respecto al espacio cibernético de confrontación.

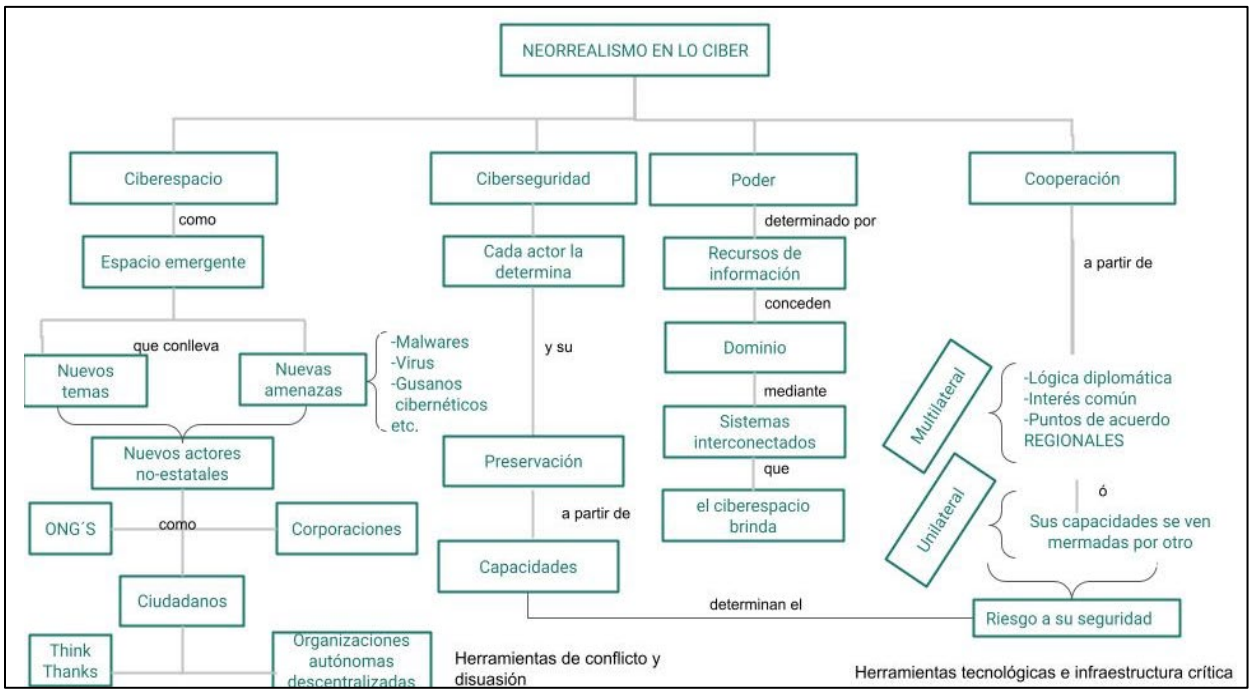
Figura 1. Características del enfoque neorrealista.



Fuente: Elaboración propia a partir de los textos de Senny Hernández, Kenneth Waltz y Barry Buzan.

Si bien este esquema da cuenta de las principales características del enfoque neorrealista, destacando, como se puede apreciar, los elementos que lo integran, a continuación, se presenta otro esquema que sintetiza al neorrealismo con elementos relativos a las interacciones que se dan en el ciberespacio.

Figura 2. El neorrealismo en el ciberespacio



Fuente: Elaboración propia a partir de los textos de Senny Hernández, Kenneth Waltz y Barry Buzan.

A partir del esquema anterior es importante destacar que el enfoque neorrealista *per se*, no se modifica, sino que se coadyuva a comprender la dinámica del espacio cibernético dentro del cual los actores y elementos propios del ciberespacio toman lugar. Los postulados contribuyen a explicar y delimitar la realidad de naturaleza inmaterial que involucra las relaciones entre actores estatales, la influencia de los no estatales y las capacidades de cada uno en escenarios de conflicto y tensión constantes.

Este organizador gráfico sintetiza el marco referencial del neorrealismo en el ciberespacio, lo que conduce la investigación en los siguientes capítulos a desarrollar. Desde nuestra perspectiva, en lo cibernético, la aproximación neorrealista es una herramienta sustancial para poder dar una explicación más clara de la realidad que se analiza.

1.3 Características y actores del conflicto cibernético.

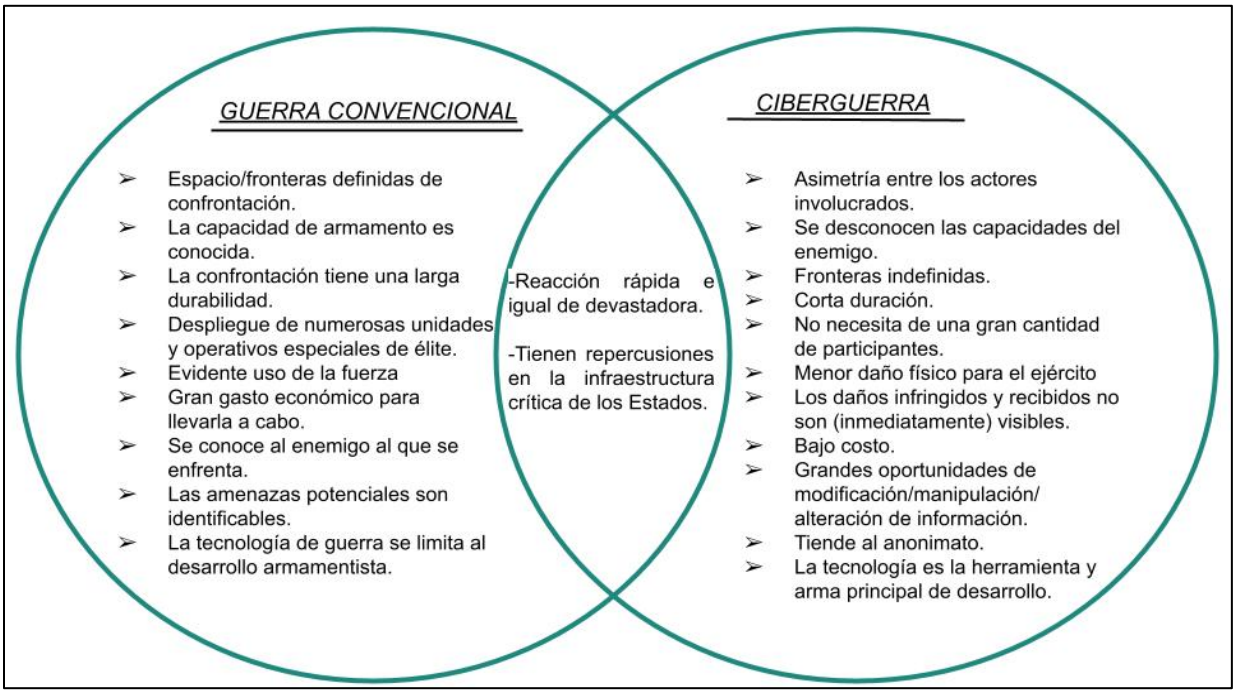
A la ciberguerra se le considera como una de las 3 clases de amenazas ciberespaciales, junto con el cibercrimen y el ciberterrorismo.[39] Las características de la guerra cibernética podrían parecer evidentes; sin embargo, es necesario señalarlas para dimensionar de mejor manera las ventajas de un Estado frente a otro en un escenario del conflicto, por lo que en este apartado se destacarán dentro de las muchas características que tiene.

La ciberguerra se caracteriza por su complejidad, asimetría, limitación de objetivos, corta duración, menor daño material para las fuerzas armadas, mayor espacio de combate y menor densidad de tropas, menor evidencia del uso de la fuerza, lucha intensa por la superioridad de la información, aumento de la integración, mayores exigencias impuestas a los comandantes, nuevos aspectos de la concentración de fuerzas y, finalmente, implica una reacción rápida e igual de devastadora que una guerra convencional.[40]

[39] Fernando Navarrete, "*Los ámbitos no terrestres en la guerra futura: Espacio",* Anu. Mex Der. Inter. España-Argentina, Monografías del CESEDEN, vol. 14, 2014. pp. 869-874. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542014000100028&lng=es&nrm=iso

[40] Gema Sánchez Medero; "Los Estados y la Ciberguerra", *Revista Boletín de Información,* España, Universidad Complutense de Madrid, núm. 317*,* 2010, pp. 63-76.

Figura 3. Diferencias entre la guerra convencional y la ciberguerra.



Fuente: Fuente: Elaboración propia a partir de los textos de Senny Hernández, Kenneth Waltz y Barry Buzan.

En el diagrama plasmando con anterioridad, la asimetría es un elemento que destaca ya que la ciberguerra permite poner en un mismo nivel a distintos actores; los instrumentos necesarios para involucrarse en la contienda cibernética son prácticamente los mismos, solo se encuentran en dependencia de los conocimientos informáticos para competir con otros actores que estén dotados de un ordenador y conexión a internet. Estados, o actores pequeños se ven en las mismas posibilidades de infringir daño anteponiéndose a los más grandes.

Teniendo en cuenta las características antes mencionadas, hay que reconocer las variantes de la ciberguerra. Sánchez Medero señala que existen tres clases de ciberguerra:

- Clase I. *Personal Information Warfare:* área relacionada con las cuestiones y la seguridad personal, así como la privacidad de los datos y del acceso a las redes de información.
- Clase II. *Corporate/Organizational Level Information:* área del espionaje clásico entre organizaciones de diferente nivel (de la empresa al Estado) o al mismo nivel (de Estado a Estado).

- Clase III, *Open/Global Scope Information Warfare:* área relacionada con las cuestiones de ciberterrorismo a todos los niveles, como pueden ser: los ataques realizados desde computadoras a centros tecnológicos; la propaganda como forma para enviar sus mensajes y para promover el daño ocasionado por sus ataques; o la planificación logística de atentados tradicionales, qímico-biológicos o tecnológicos.

Por otro lado, a diferencia de la guerra convencional, donde muchas veces se presumen las capacidades armamentistas (misiles, aviones de combate, tanques, etc.). En la ciberguerra el principio básico es la ocultación, nadie devela las armas que tiene; cuándo obtienes un arma, o dispones de ella o la sigues desarrollando. Los desfiles armamentistas están quedando de lado; lo que antes suponía una exhibición de las capacidades de armamento, y su capacidad de infringir daño, hoy con la modalidad de la guerra cibernética, nadie sabe realmente a lo que se enfrenta; sus autores, dirección o magnitud son encubiertos por la incertidumbre que caracteriza a este espacio y forma de confrontación, que a pesar de las clases que la autora menciona, predomina en todas ellas dicha discreción.

La ciberguerra tenderá al logro de objetivos asociados a los elementos que se citan enseguida[41]:

- Dañar un sistema o entidad hasta el punto en que ya no puede funcionar ni ser restaurado a una condición útil sin que lo reconstruyan por completo.
- Interrumpir o romper el flujo de la información.
- Destruir físicamente la información del adversario.
- Reducir la efectividad o eficiencia de los sistemas de comunicación del adversario y sus capacidades de recolección de información.
- Impedir al adversario acceder y utilizar los sistemas y servicios críticos.
- Engañar a los adversarios.
- Lograr acceder a los sistemas del enemigo y robarles información.
- Responder rápidamente a los ataques o invasiones del adversario.

[41] *Ibid.*, pp. 69.

Al hablar de los actores que participan en la ciberguerra, se debe tener en consideración la gran variedad de ciberatacantes. Pueden entrar en dos categorías básicas utilizadas comúnmente en los estudios de Relaciones Internacionales, los actores estatales y los no estatales. Los primeros hacen referencia a todos aquellos que se apegan a las instituciones y creación intelectual de los ciberataques subsidiados por el Estado con el objetivo de la preservación de este y/o seguir la línea de sus ideales políticos, económicos, militares, etc. Respecto a los no- estatales, se involucran aquellas instituciones privadas, hacktivistas, hackers particulares, y todo aquel organismo que no esté paralelamente asociado a los fines estatales, incluso puede ir en contra de dichos fines.

Para la compañía de seguridad, *Kaspersky*, no hay lugar a la duda que los diferentes perfiles de los actores y delincuentes han cambiado y se han perfeccionado, ya que en un informe publicado en su portal *"Securelist"* en 2012 menciona lo siguiente: "Hoy en día hay tres tipos conocidos de actores que desarrollan programas maliciosos y programas espía: los hacktivistas, los ciberdelincuentes y los gobiernos"[42]

Alberto Calvo, director de Sistemas de Seguridad de Indra, una de las principales compañías globales de tecnología y consultoría que inició sus operaciones en 1993 y tiene su base en Madrid, España, distingue cuatro perfiles de los atacantes:

- **Ciber-delincuentes y Mafias**: con el chantaje económico como medida de presión, estos actores amenazarían con difamar o destruir datos de sus víctimas, o bien los sustraerían con la intención de venderlos en el mercado negro.[43]
- **Ciber-terroristas**: que actuarían tanto para financiarse como para fines de propaganda o causar pérdidas en las instituciones e infraestructuras críticas de los países que consideran sus enemigos.[44]

[42] Kaspersky-GREAT, "Gauss: Troyano bancario se utiliza en el espionaje cibernético gubernamental", *SECURELIST- Kaspersky*, Rusia, Kaspersky Company Account, 13 de agosto de 2012. Disponible en http://www.viruslist.com/sp/weblog?weblogid=208188666.
[43] Luis Alberto Calvo, conferencia presentada en el Encuentro Internacional de Seguridad de la Información (ENISE), citado por Eguskiñe Lejarza Illaro, "Ciberguerra, los Escenarios de Confrontación*", Documentos de Opinión*, España, Instituto español de estudios estratégicos, 2014, p. 15.
[44] Ibid., 16 p.

- **Ciber-activistas**: se trataría de grupos antisistema, y la finalidad de las acciones sería desacreditar a aquellas instituciones contra las que actúan, con el fin último de modificar su comportamiento.[45]
- **Ciber-ejércitos**: con "una capacidad financiera muy superior a los atacantes habituales" así como "una sofisticación máxima"[46].

Debido al carácter estatal que la ciberguerra enuncia, es importante hacer hincapié en el último perfil mencionado por el autor. Así como se tienen ciber ejércitos, se debe remitir al perfil particular del ciber soldado. En su obra *Ciberguerra. La consolidación de un nuevo poder en las relaciones internacionales contemporáneas.* Andrés Gaitán menciona que, aunque los involucrados puedan o no utilizar uniformes, o hacer presencia en las fronteras geográficas lineales de las fuerzas militares, son el grupo más altamente especializado de individuos involucrados en la guerra cibernética de manera ofensiva y defensiva.

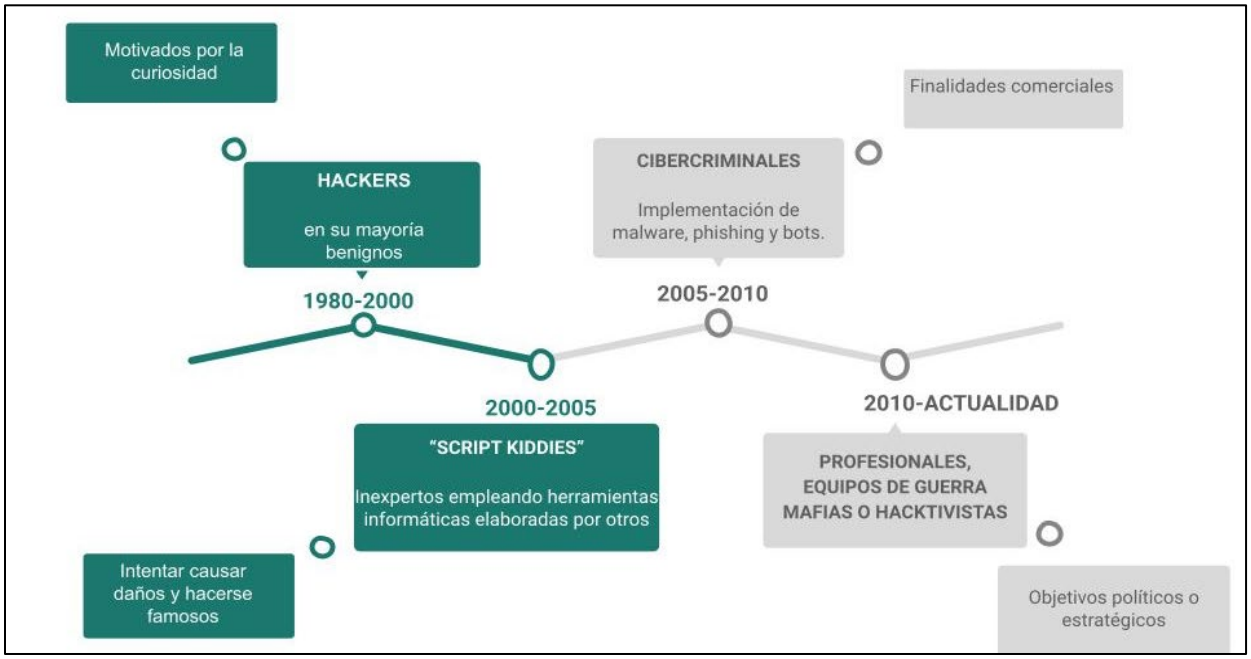
La figura del delincuente de la red ha evolucionado. Calvo presenta 4 etapas diferenciadas a partir de las características del actor hostil cibernético:

1. Desde 1980 hasta el 2000, dominada por hackers motivados por la curiosidad, pero la mayoría benignos.
2. Del 2000 al 2005, esta segunda etapa estaría protagonizada por los "*script kiddies*", se trata de personas inexpertas, que utilizan herramientas informáticas elaboradas por otros, con la finalidad de intentar causar daños y hacerse famosos, pero sin objetivos claros.
3. Del 2005 al 2010, entraron en escena los cibercriminales, que utilizarían *phishing, malware, bots* con finalidades comerciales.
4. Del 2010 hasta la actualidad, el perfil de actor hostil evolucionaría hacia "profesionales, equipos de ciberguerra, mafias o hacktivistas a los que moverían ya objetivos políticos o estratégicos" [47].

[45] Ibid., 16 p.
[46] Ibid., 16 p.
[47] Ibid., 16 p.

En el siguiente cuadro se sintetiza la evolución de los ciberatacantes con las características propias de cada uno de ellos en su respectiva etapa, presentadas por Alberto Calvo:

Figura 4. Evolución y características del actor hostil cibernético.



Fuente: Elaboración propia con base en **Alberto Calvo**, "Ciberguerra, los Escenarios de Confrontación", Documentos de Opinión, España, Instituto español de estudios estratégicos, 2014.

Destaca la evolución del perfil del ciberatacante de forma paralela al desarrollo y apertura del ciberespacio; la accesibilidad y rentabilidad de éste, dio pauta a crear mayores vulnerabilidades por la capacidad de perpetrar directamente la seguridad desde el flanco cibernético. Con ello el perfil y los objetivos escalan en el alcance de daños a gran velocidad; 30 años son los que Alberto Calvo presenta como etapas diferenciadas, sin embargo, las características que los ciberatacantes y sus agresiones son muy contrastantes desde las herramientas tecnológicas empleadas, hasta los objetivos de daño que persiguen.

Los diferentes actores preparan incluso durante tiempos de paz, el campo de batalla cibernético. Todos ellos buscan las vulnerabilidades del adversario, y se esfuerzan por infiltrarse en sus sistemas y plagarlos de "bombas lógicas" y detectar "puertas traseras", para poder utilizarlas cuando se inicien las hostilidades. Esto termina desvaneciendo la línea divisoria entre el tiempo de guerra y el de paz, lo que dificulta el

poder catalogar la conducta de los contendientes y denunciar a un actor cuando esté quebrantando la paz y la seguridad internacionales.[48]

Podría parecer que el perfil del *hacker* y de un cibersoldado son idénticos, por sus estrategias de ataque, herramientas e incluso su conocimiento, sin embargo, casi siempre sus fines son completamente distintos. Lo primero que hace cualquier *hacker* es visitar o buscar algunos de los sitios donde hay *scripts* (secuencia de comandos) para escanear el sitio al cual se quiere violentar, con el fin de determinar cuál es su arquitectura tecnológica básica. Esos *scripts* indagan en el servidor del sitio para determinar qué sistema operativo usa y que tipo de servidor de *software* emplean.

Posteriormente, sigue el paso más complicado; encontrar "agujeros" o fallas en la versión específica del *software* de ese sitio, ya que éste puede proporcionar las «entradas» que permitan romper su código. La información sobre las fallas del *software* inmediatamente pasa a ser de conocimiento público dentro de la comunidad *hacker*, (evidentemente cuando se trata de cibersoldados la información obtenida no se publicita)[49]. La información en el caso de actores apegados a fines estatales específicos, la recolectan y analizan conforme a los intereses nacionales que persigue dicho Estado, y la publicación de alguno de esos datos dependería de objetivos de disuasión o negociación en un futuro.

Respecto de la estrategia típica de un ciberataque en esta quinta dimensión, la mayoría de las intrusiones aprovechan las vulnerabilidades de los sistemas informáticos, particularmente de las redes críticas, donde el alcance, dirección, duración y propósito de los ataques cibernéticos observados son difíciles de identificar, ya que a menudo resulta complejo detectar y diferenciar los hilos de las diversas relaciones de causa y efecto que los caracterizan. En tal sentido, un adversario puede emplear diversas técnicas de encubrimiento para ocultar el origen de la acción, lo que complica su trazabilidad. Por ello, la determinación de la autoría, es decir, la identificación y

[48] Manuel R. Torres Soriano, "Los Dilemas Estratégicos de la Ciberguerra", *Revista Ejército*, España, año LXII, núm. 839, marzo-abril, 2011, pp. 14-19.
[49] Gema Sánchez Medero, *Op. Cit. p* 65.

localización de un atacante para iniciar las contramedidas, es un objetivo relevante y prioritario, pero sin lugar a duda difícil de lograr.[50]

A continuación, se presentan de manera gráfica las tres estrategias principales que se emplean en un ciberataque, propios de la guerra cibernética.

[50] Luis F. Sáez Collantes, *La Ciberguerra en los Conflictos Modernos*, Santiago, Chile, Fuerza Aérea Chile, 2012.

Figura 5. Estratégica típica de un ciberataque

Fuente: Elaboración propia a partir del texto de **René Leiva Villagra**, *La ciberguerra; sus impactos y sus desafíos. Cap.1. Aparece la ciberguerra,* Centro de Estudios Estratégicos de la Academia de la Guerra. Ejército de Chile, 2018.

Existen múltiples tipos y técnicas para realizar un ciberataque. A pesar de la gran gama que existe, dentro de la ciberguerra imperan ciertas modalidades, es así que estos ataques destacan por su alto grado de sofisticación técnica, lo que a su vez requiere de recursos tecnológicos y monetarios significativos y que no están al alcance de cualquier organización, menos aún de cualquier individuo/*cracker/hacker*. En seguida se enlistan dichas modalidades de ciberataques y sus características:

- ***Malware:*** Proviene de la abreviatura *malicious software,* que se traduce como “software malicioso”. Los canales por los que dicho *software* infecta los dispositivos son variados: a través de internet, correo electrónico,

descarga de archivos, aplicaciones (apps) engañosas, vídeos, música, etc. El *malware* puede causar el robo de información, bloqueo en el acceso a dispositivos o "secuestro" de los mismos, espionaje, etc.[51]

- ***Ransomware:*** El término deriva de la palabra *ransom,* "rescate" en español. El *ransomware*, es un *software* que niega el acceso a dispositivos y a cambio de su liberación exige una compensación monetaria. Dos ataques que se distinguieron por emplear esta modalidad a nivel global fueron Peyta y NotPeyta, los cuales afectaron a más de 80 empresas e instituciones públicas y gubernamentales.[52]
- **Gusano:** Se caracterizan por su capacidad de "trepar" de forma automática de una terminal a otra dentro de una misma red, y replicar su contenido malicioso. Lo anterior, significa que, sin la intervención del usuario, el gusano puede propagarse por sí sólo y ejecutar los comandos de infección de manera autónoma. [53]
- **Virus:** El virus se resume a ser y diferenciarse del gusano, por necesitar de una serie de acciones del usuario para efectuarse. Ya que los virus se alojan dentro de archivos o programas, al ser ejecutados por el usuario mediante un click, descarga o por introducir datos, el virus logra infectar la terminal y al dispositivo.[54]
- **Troyano:** Se distinguen por no propagarse. Los troyanos se "camuflan" como aplicaciones seguras y legítimas, y también necesitan de la ejecución del usuario para llevarse a cabo. Más allá del robo de información y de alterar el funcionamiento del sistema, los troyanos dejan una brecha o *backdoor* para acceder al mismo, lo cual lo hace más vulnerable a otro tipo de ciberataques.[55]

---

[51] ICA Sistemas y seguridad, *Los 9 tipos de ciberataque que deberías conocer,* España, Grupo ICA. Información y Comunicación Avanzada, s.a., Disponible en: https://www.grupoica.com/blog/-/blogs/9-tipos-ciberataque-debes-conocer
[52] Ibid. ICA Sistemas y seguridad.
[53] Ibid. ICA Sistemas y seguridad.
[54] Ibid. ICA Sistemas y seguridad.
[55] Ibid. ICA Sistemas y seguridad.

- **Denegación de servicio (DoS):** Del inglés *Denial of Service,* su objetivo es colapsar y/o bloquear un sistema a través de numerosas peticiones de conexión simultáneamente. Suelen ser realizados por ordenadores ya infectados y que en automático efectúan este tipo de ciberataques automáticamente. Normalmente para que esto suceda, los ordenadores ya infectados los antecede un Troyano y son controlados remotamente por ciberdelincuentes que realizan ataques distribuidos. Tanto la Denegación de servicio, como la Denegación de Servicio Distribuido (DDoS) afectan los sistemas de control de infraestructuras críticas estatales con mayor facilidad y frecuencia.[56]
- ***Phishing:*** A través de solicitar información personal datos bancarios o contraseñas, el *phishing* es una técnica fraudulenta que, por medio del correo electrónico y páginas redireccionadas falsas, solicita que se ingresen los datos que se buscan obtener por parte de quien lanza el ciberataque.[57]
- ***Spyware:*** Se ejecutan automáticamente cada vez que se enciende un equipo infectado, recopilando información que se compartirá posteriormente sin autorización. Pueden llegar a pedir dinero a cambio de no hacerla pública. [58]

Conocer la variedad de tipos de ciberataque y las maneras en las que trabajan, permiten que se pueda tener un panorama más amplio respecto a lo que ocurre y cómo ocurre cuando se emplean como herramientas bélicas o de disuasión durante un ciberconflicto. La gama de posibilidades que se tiene de manera cibernética para inmiscuir un programa, virus, *malware*, o gusano dentro de los sistemas estatales, en el caso de la ciberguerra, es infinita, y retomando las características de ésta; altamente efectiva, anónima y económica (salvo algunas excepciones, como en ciberataques sofisticados y de gran impacto).

Las características y actores de la ciberguerra no son estáticos, conforme la tecnología avanza, dota de nuevas capacidades el manejo del ciberespacio, así como

[56] Ibid. ICA Sistemas y seguridad.
[57] Ibid. ICA Sistemas y seguridad.
[58] Ibid. ICA Sistemas y seguridad.

para su estudio, comprensión, desarrollo del saber humano, entre otros beneficios, pero también abre la puerta a nuevas amenazas o canales de riesgo que los ciberatacantes, específicamente, aprovechan para crear lagunas de ciberseguridad para los actores del sistema internacional. Es necesario estar a la vanguardia de dichos cambios para tratar de dimensionar los alcances, límites y posibilidades dentro de este espacio de conflicto en aras de la dinámica social y los actores que en ella convergen como sociedad digital.

Conclusiones del capítulo.

Con relación a lo expuesto a lo largo de estas páginas, es posible vislumbrar que la ciberguerra es una modalidad de conflicto inacabada, sin límites claramente establecidos o posibilidades consumadas respecto a sus alcances, actores, amenazas, etc. Las variadas y múltiples definiciones que se acotaron al ciberespacio, y ciberguerra, resaltan elementos comunes que se encuentran en cada una de ellas; “espacio virtual”, “datos”, “redes”, “interconexión”, infraestructura de redes”, entre otros, mismos que confluyen para un mejor entendimiento de lo que la quinta dimensión representa. Por lo anterior, constata que su revisión y actualización conceptual debe seguir el ritmo de la metamorfosis cibernética.

Es necesario reconocer que la ciberguerra llega como consecuencia de la evolución del ser humano en su desarrollo intelectual que se compagina con el uso de la tecnología y la internet como herramientas que no son “buenas” ni “malas”, pero tampoco neutrales; condicionando los contextos y catalizando procesos diversos. Por lo tanto, el auge del ciberespacio como un lugar que da apertura a diversas relaciones entre actores existentes y emergentes, también se reconoce en dar pie al conflicto propio de un sistema anárquico, con la misma naturaleza de la sociedad internacional. Dentro de este espacio es que se debe reconocer que los actores que tienen lugar en él no son totalmente nuevos, ni tampoco lo es su comportamiento, sino que los canales bajo los cuales se desenvuelven han evolucionado a lo inmaterial, dotados con características propias del mismo. Por lo tanto, hay que estudiar, analizar y tratar de determinar, si es posible, patrones que esclarezcan las dinámicas que el mundo cibernético conlleva.

Asistidos por las teorías de relaciones internacionales existentes, es que la ciberguerra y otros fenómenos de naturaleza cibernética pueden tener un mejor análisis

permitiendo su aproximación. Al ser un fenómeno de confrontación y tensión política, es que el neorrealismo nos brinda sus preceptos para coadyuvarnos en el análisis, así como por su consideración por los nuevos espacios emergentes en la realidad social. En esa línea, el dilema de la seguridad en el quinto dominio, responderá con sus particularidades a la búsqueda por la supervivencia en un sistema anárquico y dadas las características de la ciberguerra, presentadas en este apartado, dónde resalta la primacía de la discreción operativa, la inseguridad en este espacio se potencializa y podría propiciar acciones político-militares como carreras armamentistas o cibernéticas en la autopreservación dentro del ciberespacio y otros planos materiales.

Conocer las características de los ciberataques, los actores (y la evolución de éstos) a lo largo del tiempo demuestra, en primera instancia, la velocidad con la que cambian los elementos que componen al quinto dominio. Además, evidencía el abanico de variaciones y posibilidades en que la realidad inmaterial impacta a la realidad material, dotando de fuerza los acontecimientos cibernéticos y sus consecuencias en aquellas dinámicas de gran envergadura como lo son la guerra y la balanza del poder, señaladas por el precepto teórico que acompaño éste primer acercamiento al tema de estudio. Finalmente, todo lo anterior posibilita “limpiar” la panorámica ciberespacial de las particularidades de otros espacios de confrontación para poder esclarecer así aquellos puntos en los estudios a realizar.

En los siguientes capítulos, ya con la delimitación y la recopilación de conceptos auxiliares para comprender el fenómeno de la ciberguerra, se abordarán a fondo los casos de Rusia y Estados Unidos como actores unilaterales en el conflicto de esta índole, así como sus agendas de seguridad inmersas como ejes clave de comprensión y solución para su disputa y que puede ser una propuesta para el resto de los Estados del Sistema Internacional que son parte del mundo cibernético.

2. La configuración de las agendas de ciberseguridad a partir de la ciberguerra como una modalidad emergente de conflicto bélico.

Los gobiernos y los organismos de seguridad reconocen que en la actualidad existe más riesgo de vulneración a la seguridad debido a los delitos informáticos, ciberterrorismo y las diversas amenazas cibernéticas[59] así como por los daños a la sociedad y pérdidas de carácter económico. La administración pública y las diversas organizaciones a nivel mundial han elevado sus capacidades tecnológicas de ciberdefensa y de seguridad de la información mediante sistemas y protocolos cada vez más sofisticados, con el fin de contrarrestar los riesgos y amenazas.

Simultáneamente, se ha generado la necesidad de crear un marco normativo y legal, además de actualizar la legislación y establecer normas técnicas de calidad, ya que la amenaza, cada vez mayor de los ciberataques a la infraestructura crítica, han incitado a que los países dediquen esfuerzos y recursos crecientes para gestionar la seguridad en el ciberespacio; ejemplo de ello son los avances de China y Rusia por desarrollar su internet soberano.

Debido a que los ataques cibernéticos tienen la capacidad de causar efectos en el mundo físico, específicamente a la infraestructura crítica de los países, éstos se han visto obligados a valorar la ciberseguridad como una piedra angular para su preservación y para procurar el desarrollo a nivel nacional.

La ciberguerra, particularmente, refiere una opción más dentro de los espacios de conflicto internacional tradicionalmente conocidos; en las próximas décadas la implementación de la ciberguerra se vislumbra como una posibilidad latente que se adaptará perfectamente al avance de la tecnología, misma que los gobiernos utilizarán como una herramienta en la búsqueda de sus objetivos nacionales.

Por otro lado, la confrontación cibernética mantiene hasta cierto punto la discreción o, mejor dicho, el anonimato de la persona o grupo que comete el ataque, a diferencia de otras modalidades bélicas, como se explicó en el capítulo anterior. Al tener esta característica, las naciones pueden inclinarse a su implementación para no mostrar de forma evidente las acciones de guerra o agresiones hacia sus adversarios y así

[59] Daniel Reyna Ramos; Daniel A. Olivera Gómez, “Las amenazas cibernéticas”, *10 Temas de Ciberseguridad.* Veracruz, México, Editorial Universidad de Xalapa, 2017, pp. 49-72.

mantener su reputación frente a la opinión pública internacional, o bien hacer un hibrido entre las prácticas bélicas tradicionales y la guerra cibernética.

El hecho de que la ciberguerra se perfile como un recurso de poder a nivel internacional, condiciona a los países para establecer estrategias de ciberseguridad que perfilen la protección y defensa de la conservación estatal, así como la de la sociedad civil.

La diversidad de canales por las que un ciberataque se puede llevar a cabo conlleva que en la agenda de seguridad nacional se considere el espacio cibernético como un tema clave a tratar y se elaboren distintas estrategias para fortalecer y resolver la amenaza que una ciberseguridad mal administrada puede significar.

En el diseño e implementación de estrategias es necesario que se tome en cuenta a las instituciones gubernamentales, al sector privado e incluso a la sociedad civil, generando así propuestas y acciones de protección que engloben a la mayoría de las áreas y canales por las que podría vulnerarse la seguridad y la preservación nacional de los países.

La evaluación del compromiso con la ciberseguridad de los Estados es un ejercicio complicado que depende de un amplio número de factores. En esta línea están surgiendo numerosas iniciativas que pretenden obtener una imagen precisa con la cual comparar y detectar los puntos de mejora en los que puede trabajar un país.

Las iniciativas encaminadas a velar por la ciberseguridad se están produciendo en ámbitos con distintos alcances que van desde lo global, como es el caso de Naciones Unidas a través de la Unión Internacional de Telecomunicaciones; regional, como son la Unión Europea, la Organización de Estados Americanos o la Unión de Naciones Suramericanas; hasta la esfera nacional, donde cada Estado las define con base en sus intereses, percepción de las amenazas, agenda interna y capacidades tecnológicas.[60]

Aun cuando existen diversas iniciativas en materia de ciberseguridad que responden a contextos específicos, sigue presente el reto de eficientar los recursos al

[60] Daniel Ramírez Morán, "*La visión internacional de la ciberseguridad",* Documento informativo, España, Instituto Español de Estudios Estratégicos, núm. 02, 2015. Disponible en: /www.ieee.es/Galerias/fichero/docs_informativos/2015/DIEEEI02-2015_VisionInternacional_Ciberseguridad_DRM.pdf

interior de los Estados, pues en la medida con que las tecnologías y canales sean seguros, se imposibilitará o reducirá la vulneración a los sistemas e infraestructura crítica.

Reconocer y atender a la ciberseguridad como un elemento clave para el desarrollo de las naciones es fundamental para garantizar la preservación de los Estados en todas sus áreas, tales como: la económica, la energética, la social, la alimenticia, de derechos humanos, etc.

En el presente capítulo se analizará la evolución que ha tenido la seguridad cibernética a nivel internacional, así como los temas centrales que se abordan en las agendas de seguridad a nivel nacional e internacional. Así mismo, se reflexionará sobre el impacto que genera tener (o no) a la ciberseguridad como un elemento a tratar dentro de las agendas. En este sentido, se propone considerar cómo ha afectado la ciberguerra a la sociedad civil, cuándo ésta ha tenido lugar, así como sus efectos e implicaciones.

Con base en lo anterior, se presentará una propuesta crítica para demostrar la importancia y necesidad de incorporar los temas de ciberseguridad y de ciberguerra dentro de los ejes articulares para la preservación de la seguridad nacional en el contexto tecnológico que la engloba.

2.1 Evolución de las agendas de seguridad y ciberseguridad de los Estados. Una panorámica de la inserción de los temas de ciberseguridad por países representativos.

El concepto de seguridad se ha ampliado en las últimas décadas como consecuencia de la propia evolución de la sociedad internacional, los cambios en los paradigmas tecno-económicos o en las revoluciones industriales. Los temas que han cobrado significado han sido la escasez de combustibles fósiles, el déficit de la salud pública en el mundo, el hambre endémica, la pobreza, el colapso climático, hasta llegar a la regulación del ciberespacio.

El marco tecnológico en el que nos encontramos y los cambios observados en el equilibrio de poder desde el término de la Guerra Fría, han dado origen a un nuevo debate sobre la seguridad.

En efecto, en el contexto de la *détente* (distensión) y con el fin de la Guerra Fría iniciaron los debates académicos y políticos entre dos posturas principales: los

“ampliacionistas” cuyos argumentos se situaban a favor de ampliar la definición tradicional sobre lo que se entiende por seguridad y su campo, así como el entendido de que la agenda de seguridad va más allá de la preservación de los Estados y los temas estratégicos que la Guerra Fría estableció en determinado momento.

Otra postura está representada por los “reduccionistas”, quienes proponían mantener una definición y una agenda reducidas sobre la seguridad, centrándose en cuestiones militares de seguridad nacional.[61]

De manera muy general, la primera de estas aproximaciones se identifica con las corrientes liberales y neo-institucionales de las relaciones internacionales; la segunda, con la teoría realista.

Es importante destacar que la ciberseguridad, a pesar de ser un tema de “reciente” incorporación a los debates sobre seguridad, no entra dentro de la lógica ampliacionista, ya que la naturaleza de resolución de problemáticas como la ciberguerra, el cibercrimen, el ciberterrorismo entre otros, sigue siendo en primera instancia de forma estatal, militar y que gira en torno a la seguridad nacional *per se*. No es menester iniciar un debate sobre si la ciberguerra y ciberseguridad son temas derivados de la visión ampliacionista y por tanto de la teoría neoliberal, sino simplemente distinguir que éstas son afines a los postulados neorrealistas, que guían al presente trabajo de investigación.

A inicios de la década de los noventa, en múltiples espacios internacionales de discusión (complementaria) se comenzó a reclamar atención sobre la necesidad de encarar conjuntamente los problemas derivados del uso de las tecnologías de la información y la comunicación, principalmente en los países desarrollados donde la penetración de la tecnología y su avance fue más fuerte.

Con el fortalecimiento de la sociedad de la información y el conocimiento en el marco de la Tercera Revolución Industrial, se hizo cada vez más común la apertura de espacios de reflexión académica, jurídica, política y económica, sobre todo alrededor de las consecuencias del mal uso de las TIC y sus implicaciones para la sociedad.

Conviene aclarar que la tecnología no determina la política exterior y de seguridad de los Estados, sino que, más bien, podría afirmarse que existe una correlación entre el

[61] Alex Comninos, *Una Agenda de Ciberseguridad para la sociedad civil: ¿Qué hay en juego?,* España, Asociación para el Progreso de las Comunicaciones, Temas emergentes, 2013. 11 pp.

posicionamiento de un Estado como actor de la política internacional, su marco tecnológico y su necesidad de velar por garantizar su seguridad.

Hasta hace poco, el término "ciberespacio" era considerado ambiguo, incluso, el desarrollo de nuevas aplicaciones y la complejidad de los procesos de apropiación social tecnológica, a nivel global, han abierto un amplio abanico de concepciones y definiciones alrededor de éste, que, siguiendo la propuesta de **Gabriel Pérez**, algunas son tecno-optimistas y otras tecno-pesimistas. Este hecho hace que se tomen direcciones distintas y que, en su mayoría, dificulten controlar un espacio virtual al no estar bien delimitado o acotado su campo de acción.

Pérez, señala que la visión optimista del impacto social de las tecnologías sigue la lógica de los trabajos de McLuhan (1992), De Kerckhove (1999), Negroponte (1995) y Dertouzos (1997), dentro de los que predomina la creencia de que la evolución de las TIC está directamente relacionada con la productividad, el crecimiento económico y social. En este sentido, el común denominador de dichos autores está dado por la creencia de que la inserción de las TIC derivará en avances dentro de los procesos de industrialización, aplicaciones militares, energía atómica, discurso que estuvo presente a lo largo de las décadas de 1960 y 1970.

Una visión contraria, la pesimista, resalta los efectos negativos de lo que la visión optimista consideraba como ventajas del avance tecnológico. Polución, deshumanización y la posibilidad del aniquilamiento global total fueron temas que empezaron a empañar, en algunos sectores, la hasta entonces prácticamente inmaculada imagen de la ciencia y la tecnología.[62]

Si a la idea del autor agregamos la del actual riesgo personal y colectivo, respecto a la inseguridad de la información y los datos de los usuarios civiles y gubernamentales, la balanza puede inclinarse hacia la visión pesimista y destacar el impacto social, y aún más, de seguridad que tienen las tecnologías en el contexto nacional e internacional.

En suma, la regulación y las ideas de jurisdicción y competencia no tenían claridad cuando se trataba de lo acontecido dentro del ciberespacio, así como de

[62] Gabriel Pérez Salazar, *"Hacia una tecnología socialmente significativa"*, en Santos, M. J. y De Gortari, R. (coords) *Computadoras e Internet en la biblioteca pública mexicana*, México, UNAM, 2009, pp. 1-26.

aquellas conductas sin consecuencias directas en el mundo físico como la intrusión en servidores informáticos, fraudes, robo y venta de bases de datos, etc.

Los primeros esfuerzos por crear protocolos legales y mecanismos de respuesta frente a estas amenazas fueron locales. Un ejemplo es la temprana *Computer Fraud and Abuse Act* (CFAA) aprobada en Estados Unidos en 1986. Lamentablemente, por el carácter de su propia naturaleza, la efectividad de estas medidas estaba limitada al ámbito doméstico y perdieron vigencia.[63]

En 1995, el Consejo de Europa crea un comité de expertos en materia informática para poder analizar, proponer y recomendar en torno a la temática y problemáticas cibernéticas, y así garantizar la seguridad de la información e informática.

Lo anterior deriva en lo que actualmente se conoce como el Convenio de Budapest o Convenio sobre Ciberdelincuencia, aprobado en 2001. Este documento refleja lo que, hasta ese momento, eran las preocupaciones iniciales de los países, esencialmente: la creación, fortalecimiento e incorporación de los ciberdelitos a las legislaciones nacionales; y el avance para la investigación y el aumento de la cooperación internacional para su mutua protección ante amenazas informáticas. En la actualidad, el Convenio ha sido ratificado por más de 50 naciones de todo el mundo.

Por otro lado, el concepto de seguridad amplía su campo conforme la dinámica social internacional y los temas coyunturales que emergen. Algunos acontecimientos que han determinado dicho cambio son: la securitización de la agenda a partir del atentado del 9/11, las guerrillas en América Latina, el surgimiento de Rusia como República, las Primaveras Árabes, la epidemia del ébola, los atentados terroristas en Europa, el auge comercial asiático, entre otros.

En suma, es necesario destacar los temas que imperan dentro de las agendas de seguridad, para así abrir paso al análisis en torno a la ciberseguridad como un elemento considerado (o no) dentro de ellas y poder determinar las consecuencias positivas y negativas que derivan de su incorporación dentro de los temas a atender para la conservación de la seguridad y ciberseguridad de los países.

---

[63] Hiperderechos, “Una breve historia de la ciberseguridad importada”, *Derechos Digitales. Derechos Humanos y Tecnología en América Latina,* Chile, julio 2018. Disponible en: https://www.derechosdigitales.org/12329/una-breve-historia-de-la-ciberseguridad-importada/

En primera instancia es imperativo reconocer que las agendas de seguridad nacional de cada Estado están determinadas por el contexto social, económico, cultural, incluso geográfico del que son parte. Por ejemplo, para las pequeñas islas del Caribe, amenazadas cada año por la temporada de huracanes, no existe espacio en la agenda de riesgos para temas como el terrorismo o el narcotráfico. En contraste, para México, que se ha visto seriamente vulnerado al compartir una de sus fronteras con Estados Unidos, temas como el tráfico de drogas, armas y personas, así como la inseguridad pública son considerados prioritarios en su agenda de seguridad nacional.[64]

Ciertamente, tanto en el caso de las personas como en el de los países o los gobiernos, la seguridad es un concepto altamente subjetivo, puesto que lo que constituye, o es percibido como una amenaza para uno, no lo es para otro y viceversa; cada uno formúla la propia de acuerdo con sus criterios, intereses y percepciones.

Es importante destacar que, bajo el enfoque neorrealista, empleado en la presente investigación, las diferencias derivadas del contexto de cada nación destacan lo que consideran dentro de su agenda de seguridad nacional particular, lo que denota algunos aspectos considerados bajo la lógica ampliacionista, que no corresponde a la lógica de las amenazas tradicionales consideradas como parte de la supervivencia del Estado.

Para **Walter Astié Burgos**, las principales amenazas que prevalecen en el siglo XXI para los países desarrollados (especialmente para Estados Unidos) contrastan con las de aquellos países en vías de desarrollo, lo que influye muchas veces en las temáticas de seguridad nacional de cada uno[65]. Las principales amenazas serán valoradas de forma diferente. Por ejemplo:

[64] Gerardo Rodríguez Sánchez Lara*, "Antiguas y nuevas amenazas a la seguridad de América Latina",* Revista *Bien Común,* México, Vol. XIII No. 152, 2007, pp. 15-18.
[65] Walter Astié Burgos*, "Seguridad internacional y diplomacia para la salud global", Revista Mexicana de Política Exterior*, México, núm. 102, septiembre-diciembre 2014, 141-171 pp.

Tabla 1. Principales amenazas a la seguridad

AMENAZAS A PAÍSES DESARROLLADOS	AMENAZAS A PAÍSES EN VÍAS DE DESARROLLO
● Militares-terrorismo internacional. ● Proliferación de armas nucleares. ● Competencia por recursos naturales escasos. ● Crecimiento demográfico. ● Pandemias/bioterrorismo. ● Cambio climático.	● Pobreza-marginación-enfermedades. ● Estallidos sociales. ● Crimen organizado. ● Competencia por recursos naturales escasos. ● Desastres naturales. ● Salud-pandemias. ● Militarización global. ● Cambio climático.

Fuente: Elaboración propia con base en Walter Astié Burgos, *"Seguridad internacional y diplomacia para la salud global".* 2014.

Con base en lo anterior, se evidencía como para los países en vías de desarrollo las principales amenazas a su seguridad son distintas, pues si bien se coincide con algunas de las naciones desarrolladas, como las relativas a la competencia por los recursos naturales cada vez más escasos, o el cambio climático, la agenda de seguridad es completamente diferente. Aunque problemáticas como el crimen organizado, los desastres naturales o de la salud también afectan a los países acaudalados, éstos cuentan con mayores recursos para afrontarlos, lo que muchas veces no es el caso de los menos avanzados.[66]

Bajo esta perspectiva, la configuración de las agendas de seguridad nacional varía en su contenido. Para esta investigación es importante identificar dónde se encuentra (o no) la ciberguerra considerada en dichas agendas, por lo cual se presenta a continuación una recopilación de los temas principales de las agendas y estrategias de seguridad de algunos países para contrastarlas, y así, elaborar un análisis a partir de lo observado.

Es importante señalar que en la elección se consideró al menos un país por región, para así obtener una visión más completa sobre los temas que imperan no sólo en lo individual de forma Estatal, sino también en la región y bajo los distintos contextos de los cuales son parte.

Cabe destacar que los criterios de inclusión/exclusión que se toman en cuenta para la selección de dichos países son los siguientes:

[66] Ibid., pp. 148-149.

1. Si han sufrido algún ciberataque de relevancia mundial a lo largo de la historia.
2. El grado de relevancia a nivel regional y/o mundial respecto al avance tecnológico o de desarrollo.
3. Que no sean países totalmente próximos geográficamente para tratar de abarcar el continente del cuál son parte y por ende la diversidad de contextos dentro del mismo.
4. Si han destacado de manera positiva o negativa dentro del reporte anual *Global Cybersecurity Index** (Índice de Ciberseguridad Global de la Unión Internacional de Telecomunicaciones).[67]

Continente: **América**

País: *Estado Unidos*
Documento: Washington D. C, diciembre 2017. Estrategia de Seguridad Nacional de los Estados Unidos de América.

La Nueva Estrategia de Seguridad Nacional establece una dirección estratégica que proyecta los intereses nacionales de Estados Unidos y la protección de estos. La Estrategia identifica cuatro intereses nacionales vitales, o “cuatro pilares”:

I. Proteger la patria, a los estadounidenses y su forma de vida.
   - Controlar las fronteras y reformar el sistema de inmigración;
   - Combatir el terrorismo y sus prácticas de asesinatos, represión y esclavitud, destacan las **redes virtuales como herramienta de difusión ideológica y la dirección de complots;**

[67]* El Índice Global de Ciberseguridad es una referencia confiable respaldada por la Unión Internacional de Telecomunicaciones que analiza el compromiso de los países con la ciberseguridad a nivel mundial, además de reflejar el nivel de compromiso y preparación ante las ciberamenazas, lo cual permite tener un panorama sobre el nivel de vulnerabilidad o seguridad en el que se encuentren con base en la evaluación de cinco factores fundamentales: 1) Medidas legales. 2) Medidas técnicas. 3) Medidas organizativas empleadas. 4) Creación de capacidad. 5) Cooperación. Con el análisis de estas cinco variables se suma y se agrega en una puntuación global que categoriza a cada país en una lista que va del más seguro a los más inseguros.
Se toman en cuenta los datos obtenidos del Reporte 2020. International Telecommunication Union, *Global Cybersecurity Index 2020, Measuring commitment to cybersecurity*. Switzerland. 2020, 172 pp.

- Perseguir organizaciones criminales transnacionales; narcotráfico y violencia que debilitan a las instituciones democráticas; y
- Desarrollar un sistema defensivo de misiles.

II. Promover la prosperidad de América.
- Rejuvenecer la economía estadounidense en beneficio de los trabajadores y empresas estadounidenses;
- Buscar relaciones económicas libres, justas y recíprocas;
- **Promover la investigación en tecnología e innovación. Protección a la propiedad intelectual y bases de datos;** y
- Tener dominio de la energía para garantizar la apertura de los mercados internacionales.

III. Conservar la paz mediante la fuerza.
- Reconstrucción de la fuerza militar de los Estados Unidos para garantizar su perfeccionamiento;
- Implementación de las herramientas del arte de gobernar, en relación con competencia estratégica: diplomática, de información, militar y económica para la protección de los intereses nacionales;
- **Fortalecimiento de las capacidades en diversos ámbitos, con mayor atención al ciberespacio, y al espacio exterior;** y
- Buscar el equilibrio de poder a favor de Estados Unidos en las regiones Indo-Pacífico, Europa y Medio Oriente.

IV. Incrementar la influencia estadounidense.
- Profundizar la influencia estadounidense en el exterior;
- Redoblar los esfuerzos diplomáticos en el campo bilateral, multilateral y de la información en busca de nuevas oportunidades económicas y de competencia;
- Búsqueda de alianzas con Estados con ideologías afines a la promoción de economías de libre mercado, crecimiento del sector privado, paz y estabilidad política; y
- Defensa de los valores estadounidenses (Estado de derecho y los derechos individuales).

A partir de los cuatro intereses principales referidos con anterioridad, es que se desglosan los temas de seguridad nacional de la agenda que aplican al interior y al exterior del país. Los principales desafíos y tendencias en la posición que ocupa en el mundo son:

- Revisión de poderes como los de China y Rusia que incluye el uso de la tecnología, propaganda y la coacción para configurar un mundo antiético a nuestros intereses y valores;
- Dictadores regionales que propagan el terror, amenazan a sus vecinos y persisten en las armas de destrucción masiva; y
- Terroristas yihadistas que fomentan el odio para incitar a la violencia contra inocentes en nombre de una ideología perversa, y organizaciones criminales transnacionales que vierten drogas y violencia en nuestras comunidades.[68]

País: *México*
Documento: *Ciudad de México, 16 de mayo de 2019. Estrategia Nacional de Seguridad Pública.*

Objetivos de la Estrategia Nacional de Seguridad Pública:

I. Erradicar la corrupción y reactivar la procuración de justicia.
II. Garantizar empleo, educación, salud y bienestar.
III. Pleno respeto y promoción de los Derechos Humanos.
IV. Regeneración ética de la sociedad.
V. Reformular el combate a las drogas.
VI. Emprender la construcción de la paz
VII. Recuperación y dignificación de los Centros Penitenciarios.
VIII. Seguridad pública, seguridad nacional y paz.

[68] United States Government, *National Security Strategy of the United States of America*, *United States of America,* diciembre 2017. 68 pp., Disponible en: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2017/NSS-Final-12-18-2017-0905.pdf

Estrategias específicas:

Como parte fundamental de la Estrategia Nacional de Seguridad Pública se han desarrollado las siguientes estrategias específicas que no son limitativas, pero que constituyen temas prioritarios y urgentes a atender:[69]

- Nuevo modelo policial.
- Prevención del delito.
- Estrategias focalizadas en las regiones y participación ciudadana.
- Nuevos criterios de distribución de los recursos federales en materia de seguridad.
- Estrategia de combate al mercado ilícito de hidrocarburos.
- Estrategia de combate al uso de operaciones con recursos de procedencia ilícita, defraudación fiscal y finanzas de la delincuencia organizada, así como el papel de la Unidad de Inteligencia Financiera (UIF) en el abatimiento de estos delitos.
- Estrategia para agilizar los procedimientos de extinción de dominio y utilización social a la delincuencia.
- Estrategia para combatir el robo a autotransporte y pasajeros en carreteras.
- Estrategia para abatir el tráfico de armas.

País: *Uruguay*
Documento: *Montevideo, 23 de diciembre de 2020. Política de Defensa Nacional.*[70]

Propuesta de Política de Defensa Nacional formulada por el Consejo de Defensa Nacional (CODENA).

Objetivos estratégicos del Estado Uruguayo:

I. Mantener la integridad territorial, marítima, aeroespacial y del ciberespacio del país
II. Inserción internacional e Integración hemisférica.
III. Protección de la población ante situaciones de emergencia.

[69]Gobierno de México, *Estrategia Nacional de Seguridad Pública* (Resumen del documento presentado por el Presidente de la República al Senado de la República) 2019-2024, Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5560463&fecha=16/05/2019

[70] Poder Ejecutivo; Ministerio de Defensa de Uruguay, "Propuesta de Política de Defensa Nacional, Decreto N°371/020", *Diario Oficial*, Montevideo, Uruguay, Centro de Información Oficial, núm. 30 599, 7 de enero de 2021, Disponible en: https://www.impo.com.uy/bases/decretos-originales/371-2020

IV. Desarrollo del país y la materialización de la Seguridad Humana en todos sus órdenes.
V. Promoción de la Democracia en el hemisferio.
VI. Protección del ambiente.
VII. Protección de los recursos estratégicos renovables y no renovables.
VIII. Presencia en el Continente Antártico.

Los objetivos de la Defensa Nacional se desprenden de los Objetivos Estratégicos del Estado y responden a una visión holística de la Seguridad Nacional, que coloca a las personas, la sociedad y al Estado como objetos referentes de la seguridad.

Se definen como Objetivos de la Defensa Nacional:

I. Asegurar la soberanía del Estado en los espacios terrestres, marítimos, aeroespaciales, y del ciberespacio.
II. Garantizar la paz de la República, así como el estricto cumplimiento de la Constitución y sus leyes.
III. Asegurar la alineación estratégica entre la política exterior y la defensa nacional.
IV. Contribuir a generar las condiciones para la seguridad humana y el bienestar social de la población.
V. Profundizar las relaciones de cooperación y confianza mutua con los países hemisféricos y extracontinentales, a través de la participación en los tratados internacionales suscritos por el país.
VI. Contribuir a la protección del ambiente y garantizar la protección de los recursos naturales estratégicos renovables y no renovables.
VII. Participar en misiones en el exterior dentro del marco de organismos y tratados internacionales en los que el Estado forme parte; con fines defensivos, humanitarios, de estabilización o de mantenimiento y preservación de la paz.

Cabe destacar que la Estrategia de seguridad marca un apartado en el que especifica las amenazas comprendidas por el Estado, dentro de las cuales comprende a los **ciberataques** y se presenta a continuación:
De acuerdo con la propuesta **los ciberataques son conceptualizados como una amenaza, y refiere a acciones realizadas por un individuo o grupo de individuos, sean estatales o no estatales, a través del ciberespacio, utilizando recursos de**

tecnologías de la información y de las comunicaciones, con el fin de afectar la disponibilidad, integridad o la confidencialidad de la información digital, manejada por un sistema informático objetivo. Dicha afectación podrá tener efectos solamente lógicos o incluso físicos acorde al sistema al cual se dirija.

Finalmente, dentro de las Directivas de la Política de Defensa Nacional, se comprende en el punto 12 especificidades en el tópico de ciberseguridad y ciberdefensa, al respecto se enuncia:

12. Acompañar el desarrollo tecnológico del país y sus iniciativas de gobierno digital con medidas que garanticen un ciberespacio seguro y confiable.

a. A nivel nacional, a través del Centro Nacional de Respuesta a incidentes de Seguridad Informática (CERTuy), se busca favorecer **la mejora en ciberseguridad y apoyar la creación de equipos de respuesta a incidentes de seguridad informáticos especializados en los diferentes sectores de actividad, y en la instalación y operación de herramientas de monitoreo y alerta.**

b. Desde el Consejo de Defensa Nacional (CODENA/CIDEN), en coordinación con el Sistema Nacional de Emergencias (SINAE**), se actualizará el inventario nacional de Infraestructuras Críticas y se propondrá el marco normativo para su protección física y ciberespacial. Esta última considerará no solo los tradicionales elementos de tecnología de la información, sino también los sistemas operativos de todos los servicios públicos esenciales.**

c. Desde el Ministerio de Defensa Nacional (MDN) se avanzará en la **creación de un Comando Conjunto de Ciberdefensa para dotar a las Fuerzas Armadas de nuevas capacidades de disuasión conjunta y sectorial en el dominio ciberespacial.**

Continente: **Europa**

País*: Federación de Rusia.*
Documento: *San Petersburgo, diciembre de 2015*[71] Estrategia de seguridad nacional de Rusia Edicto 683.*

Los intereses estratégicos nacionales a largo plazo son:

I. Fortalecer la defensa del país, asegurando la inviolabilidad de la Federación de Rusia orden constitucional, soberanía, independencia e integridad nacional y territorial.
II. Fortalecer el acuerdo nacional, la estabilidad política y social, desarrollar instituciones democráticas, y perfeccionamiento de los mecanismos de cooperación entre el Estado y la sociedad civil.
III. Elevar el nivel de vida, mejorar la salud de la población y garantizar la estabilidad del país desarrollo demográfico.
IV. Preservar y desarrollar la cultura y los valores espirituales y morales tradicionales de Rusia.
V. Aumentar la competitividad de la economía nacional.
VI. Consolidar el estatus de la Federación de Rusia como potencia mundial líder; cuyas acciones son dirigidas a mantener la estabilidad estratégica y las asociaciones mutuamente beneficiosas en un mundo policéntrico.[72]

Por otro lado, los intereses nacionales se aseguran mediante la implementación de las siguientes estrategias y prioridades nacionales:

- Defensa Nacional.
- Seguridad pública y estatal.
- Crecimiento económico.
- Ciencia, **tecnología** y educación.

[71]* Se retoma la estrategia de seguridad del año 2015 por el marco de temporalidad que la presente investigación delimita. La última actualización de la Estrategia de Seguridad Rusa se realiza en julio de 2021. Véase el Anexo para su consulta y referencia.
[72] *Russian National Security Strategy, December 2015 – Full-text Translation*, España, IEEES, 2016, 29 págs. Disponible en: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf
(Traducción del inglés al español por Mariana Corona Fragoso)

- Cuidado de la salud.
- Cultura.
- Ecología de los sistemas vivos y el uso racional de los recursos naturales.
- Estabilidad y asociación estratégica equitativa.

La estrategia específica en el apartado referente a la Defensa Nacional, punto 37 y 38, incluye la implementación de la tecnología y el reconocimiento a la diversidad de espacios de confrontación, al respecto se puntualiza:

37. La organización militar del Estado debe mejorarse mediante la identificación oportuna de riesgos y amenazas militares existentes y potenciales, el desarrollo equilibrado de los elementos de organización militar, el aumento de la capacidad de defensa, el equipamiento a las Fuerzas Armadas de Rusia además de las tropas, y la formación y agencias militares con armas modernas y equipos militares y especializados, **por medio de hardware especializado basado en la innovación de la industria de defensa de la Federación Rusa.**

38. La mejora de las formas y métodos de despliegue de las Fuerzas Armadas de la Federación Rusa, tropas, formaciones y agencias militares incluye la consideración oportuna de **desarrollos que alteran la naturaleza de las guerras y conflictos armados modernos,** la creación de condiciones para una **implementación más completa de la capacidad de combate de las tropas** (fuerzas), y el desarrollo de requisitos para futuras formaciones y **nuevos métodos de combate armado.**[73]

[73] Federación Rusa, *Estrategia de Seguridad Nacional de la Federación Rusa*, 31 de diciembre de 2015, Texto original disponible en: http://static.kremlin.ru/media/events/files/ru/l8iXkR8XLAtxeilX7JK3XXy6Y0AsHD5v.pdf

País: Suecia.
Áreas de acción de las Fuerzas Armadas y objetivos alineados a la Unión Europea.

La consulta de los documentos oficiales que marcan las directrices de la seguridad nacional de Suecia no se encuentra a disposición pública, como se señala en el portal de las Oficinas Gubernamentales de Suecia. Maneja como exenciones a aquellos tópicos que comprometan los siguientes intereses:

- La seguridad del Reino o sus relaciones con otro Estado u organización internacional.
- La política fiscal, monetaria o cambiaria central del Reino.
- La inspección, control u otras actividades de supervisión de una autoridad.
- El interés de prevenir o perseguir el delito.
- Los intereses económicos de las instituciones públicas.
- La protección de las circunstancias personales o económicas de los particulares.
- La preservación de especies animales o vegetales.

Sin embargo, para esta investigación, retomaremos aquellos objetivos que persigue conforme su estatus de miembro de la Unión Europea (UE). Para 2020 se han establecido cinco objetivos ambiciosos para medir el progreso y el grado en que éstos se alcanzan, los cuales se enlistan a continuación:

I. Empleo.
II. Investigación e innovación.
III. Cambio climático y energía.
IV. Educación.
V. Lucha contra la pobreza.

Los Estados miembros han adoptado sus propios objetivos nacionales en cada una de estas áreas. Además, han acordado una serie de actuaciones concretas a nivel nacional en las que se incluye **"sociedad digital"** como parte fundamental para el desarrollo de los objetivos dentro de un marco de seguridad y cooperación[74].

[74] DesQbre, *Unidad 1. Módulo 3. Los cinco objetivos para la UE en 2020, Introducción a la estrategia Europa 2020 y H2020,* España, Fundación Andaluza para la divulgación de la innovación y el conocimiento, 2019, pp. 1-5.

Por otro lado, en el portal de las Fuerzas Armadas Suecas, se enlistan los temas principales que tratan dentro de la conservación del Estado y la seguridad nacional de país europeo, lo que permite bosquejar los intereses u objetivos en torno a la seguridad:

- Cooperación para la defensa Nórdica.
- Cooperación de defensa con Finlandia.
- Guardia Nacional.
- **Defensa Cibernética.**
- Armada, marina y fuerzas aéreas.
- Servicio de seguridad e inteligencia.[75]

País: *España*
Documento: *1 de diciembre de 2017. Estrategia de Seguridad Nacional*

Objetivos Generales.

Se explican a la luz de los principios rectores de la Política de Seguridad Nacional. Son comunes a todos los ámbitos de esta política y responden a la necesidad de que España se posicione oportunamente ante las implicaciones de seguridad del nuevo contexto internacional:

I. Desarrollar el modelo integral de gestión de crisis.
II. Promover una cultura de Seguridad Nacional.
III. Favorecer el buen uso de los espacios comunes globales.
IV. Impulsar la dimensión de seguridad en el desarrollo tecnológico.
V. Fortalecer la proyección internacional de España.

Objetivos y líneas de acción estratégicas para los ámbitos de la Seguridad Nacional:

- Defensa Nacional.
- Lucha contra el terrorismo.
- **Ciberseguridad. (*Garantizar un uso seguro de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable.)***

[75] Swedish Armed Forces. Disponible en: https://www.forsvarsmakten.se/en/

- Lucha contra el crimen organizado.
- Seguridad económica.
- Seguridad energética.
- No proliferación de armas de destrucción masiva.
- Ordenación de flujos migratorios.
- Contrainteligencia.
- Protección ante amenazas y catástrofes.
- Seguridad marítima.
- **Protección de las infraestructuras críticas.**
- Seguridad del espacio aéreo y ultraterrestre.
- Seguridad frente a pandemias y epidemias.
- Preservación del medio ambiente.[76]

Contienete: **Medio Oriente**

País*: Arabia Saudita*
Documento: *No se encontró un documento o portal con acceso público para la consulta de su Estrategia de Seguridad Nacional.*

País*: Irán*
Documento: *(No existe acceso público para la consulta de un documento, se enlistan a partir de la consulta documental de distintos autores e investigadores)*

Carlos Echeverría, profesor de Relaciones Internacionales de la Universidad Nacional de Educación a Distancia, (España), señala que las prioridades estratégicas de la República Islámica de Irán son las mismas desde hace varias décadas. Son los acontecimientos regionales e internacionales se consideran aquellos que han influido para su consecución.

I. Consolidar el régimen.

a) Mantener la cohesión interna y garantizar su supervivencia.

[76] Gobierno de España, Consejo de Seguridad Nacional, *Estrategia de Seguridad Nacional. Un proyecto compartido de todos y para todos,* España, Presidencia del Gobierno, 2017, 128 pp. Disponible en: https://www.defensa.gob.es/Galerias/defensadocs/Estrategia_Seguriad_Nacional_2017.pdf

b) Consolidación del proceso político electoral, evitando fisuras por sanciones internacionales.

c) Mantener a punto los arsenales para reforzar la capacidad de disuasión.

d) Fortalecer la industria de defensa a través de herramientas civiles y militares, así como por la flexibilidad de un mundo cada vez más volátil en la producción y comercio de armamento.

II. Posicionarse como líder regional interactuando en escenarios concretos

a) Seguir apostando por la caída de Israel y por la expulsión de Estados Unidos de la región.

b) Expandir la zona de influencia *chií.*

III. Sobrevivir a las tensiones actuales como un vértice más de un triángulo que agrupa a Irán con la Federación de Rusia y con la República de Turquía.[77]

a) Gestión del desafío kurdo.

b) Guerra en Nagorno Karabaj o Alto Karabaj

País: *Israel*

A lo largo de su corta historia, Israel nunca ha articulado oficialmente una estrategia de seguridad nacional que identifique los objetivos del país *(ends)*, exponga las distintas maneras de conseguirlos *(ways)* y perfile los medios a emplear para alcanzarlos *(means).* Solamente ha asegurado su determinación de defender la integridad del Estado por todos los medios posibles, una vaguedad que le ha permitido responder dinámicamente ante cualquier cambio en la región, pero siempre garantizando que cualquier violación del *statu quo* tendría inexorablemente una respuesta inmediata.[78]

[77] Carlos Echeverría Jesús, "Las Prioridades Estratégicas de Irán", *Revista General de Marina*, España, Armada de la Defensa Española, Año 2020, Vol. 279, diciembre 2020, pp. 925-933.

[78] Guillem Colom Piella, "La evolución de la Estrategia de Seguridad Israelí (I)", *Boletín de Información,* España, Ministerio de la Defensa, Nº. 309, 2009, pp. 67-80. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3061967

Continente: **Asia**

País: *Japón*

Documento: *1957, Política de Defensa. Libro Blanco japonés sobre defensa.*

La Política de Defensa se fundamenta en un documento base aprobado en 1957 por el Consejo de Defensa Nacional. Conceptualmente, el principal documento político de referencia es la Estrategia de Seguridad Nacional aprobada por el primer ministro. Ambos documentos establecen la premisa de que Japón busca un pacifismo activo basado en la cooperación internacional que preserve la seguridad nacional y la estabilidad en la región Asia-Pacífico.

Las principales directrices en materia de política de Defensa están reflejadas en el Libro Blanco, cuya última versión se publicó en 2019 y que, en julio de 2020, se ha actualizado como consecuencia de la pandemia de la COVID-19.[79]

Con base en distintos documentos, la seguridad nacional asume los siguientes temas de relevancia en la agenda nipona:

I. El desarrollo de armamento nuclear en Corea del Norte.
II. Actividades militares de China y Rusia, las primeras en la zona al sur de Okinawa, y las segundas en la zona entre Hokaido, las Kuriles y Sajalin, en atención a las intromisiones al espacio aéreo y marítimo nacional.
III. Terrorismo islámico, en cuanto pueda suponer amenazas a los intereses japoneses o de sus ciudadanos.
IV. Creación de una Unidad de Misiones Espaciales en el dominio espacial, como una dependencia de la Fuerza Aérea. Con el objetivo de proporcionar comunicaciones vía satélite y servicios de navegación, y de garantizar la defensa de los sistemas propios frente a amenazas externas. *[80]

[79] Carlos Calvo González-Regueral, "Política de Defensa de Japón", *Documento de opinión,* Instituto Español de Estudios Estratégicos, España, octubre 2020, pp. 3-5.

[80] * El anuncio de creación de la unidad, que estará operativa en 2022, fue realizado en el parlamento japonés por el propio presidente Abe, durante su intervención para inaugurar el curso político en enero de 2020. Para ampliar el tema sobre el programa espacial japonés, véase: Fatton, L. "Japan's Space Program: Shifting Away from Non-Offensive Purposes?", Asie Visions, Nº115, IFRI, July 2020.

V. Garantizar y promover la seguridad cibernética, a través del fortalecimiento de la Ley Nacional de Ciberseguridad de 2014 que promueve el aumento de los efectivos en organizaciones de ciberdefensa y la cooperación internacional en este campo.

País: *China.*
Documento: *1 de julio de 2015. Ley de Seguridad Nacional de la República Popular de China adoptada en la 15ª reunión del Comité Permanente del 12º Congreso Popular Nacional de la República Popular de China.*

Dentro del "Capítulo II. Tareas de mantenimiento de la seguridad nacional", se mencionan los aspectos fundamentales para salvaguardar la seguridad nacional, para efectos prácticos se parafrasea a continuación cada uno de ellos:

I. Art. 15: El Estado se adhiere al liderazgo del Partido Comunista de China, desarrollando una política democrática socialista, para fortalecer el mecanismo de restricción y supervisión del funcionamiento del poder y proteger los derechos del pueblo.
II. Art.16: Creación de buenas condiciones para la supervivencia, el desarrollo y un entorno laboral y de vida estable; protección a la vida y a la propiedad de los ciudadanos y otros derechos legítimos e intereses.
III. Artículo 17: El Estado fortalece la construcción de la defensa fronteriza, costera y aérea, adopta todas las medidas de defensa y control necesarias para proteger la seguridad del territorio.
IV. Art. 18: Fortalecer la revolución, **modernización y regularización de sus fuerzas armadas**, y construir fuerzas armadas acordes a las necesidades de salvaguardar la seguridad nacional y los intereses del desarrollo. Llevar a cabo acciones de cooperación de seguridad militar internacional, implementar operaciones de mantenimiento de la paz, rescate internacional, escolta marítima y militares de las Naciones Unidas.
V. Art. 19: Mantener el sistema económico nacional básico y el orden de la economía socialista de mercado, mejorando los mecanismos institucionales para prevenir y

disminuir los riesgos de seguridad económica, y garantizar la estabilidad de industrias importantes y áreas clave.

VI. Art. 21: Utilizar y proteger racionalmente los recursos estratégicos y la energía.

VII. Art. 22: Completar el sistema de garantía de la seguridad alimentaria, protegerá y mejorará la capacidad general de producción de granos.

VIII. Art. 24: Construcción de capacidades de innovación independientes, aceleraron del **desarrollo de tecnologías clave centrales y de alta tecnología estratégicas** independientes y controlables en campos importantes, fortalecimiento en el uso y protección de los derechos de propiedad intelectual y la construcción de **capacidades de confidencialidad científica y tecnológica,** y garantía de la seguridad de las principales tecnologías y proyectos.

IX. Art. 25: Consolidar la construcción de un sistema de **garantía de seguridad de la red y de la información**; mejorar las capacidades de protección de la seguridad de la red y de la información; fortalecer la investigación, el desarrollo y la aplicación innovadora de la tecnología de la información y las redes. La seguridad de los datos será controlable; fortalecimiento de la gestión de la red, para **prevenir, detener y castigar los ataques a la red, las intrusiones en la red, el robo de la red, la difusión de información ilegal y dañina y otras actividades delictivas e ilegales en la red,** y salvaguardar la soberanía y la **seguridad del ciberespacio nacional** e intereses de desarrollo.[81]

País: *Indonesia*
Documentos: *1945. Constitución de la República de Indonesia y 2015. Libro Blanco de la Defensa de Indonesia*

Los objetivos nacionales enumerados en el preámbulo de la Constitución de Indonesia están escritos para su protección. Se guían a partir de tres objetivos principales:

[81] Gobierno de la República Popular China, *Ley de Seguridad Nacional de la República Popular China* (Orden del Presidente No. 29), Xinhua, China, Agencia de noticias, 2015. Disponible en : http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm?fbclid=IwAR0MVdm5gjVFplGrVExHMSdjZyDD37tkd_4n_cCLEz5v_Z9P1FOLkT6dCMI

I. Proteger físicamente a Indonesia y a su gente de amenazas contundentes y posible explotación.
II. Educar y promover el bienestar general.
III. Participar en el establecimiento del orden mundial.

Los objetivos del Estado son mantener su soberanía política, autosuficiencia en economía y su fuerte carácter basado en la cultura: El gobierno ha formulado nueve prioridades:

I. Recuperar los roles del país en la protección de todas las personas y brindar seguridad a todos los ciudadanos de Indonesia.
II. Acelerar la participación del Gobierno en la edificación limpia, gobernabilidad, gobierno eficaz, democrático y confiable.
III. Construir Indonesia desde la periferia para fortalecer estas áreas y pueblos en el marco del Estado Unitario de la República de Indonesia.
IV. Rechazar el concepto de "Estado débil" mediante la reforma de la ley de fortalecimiento del sistema de ejecución libre de corrupción, digno y de confianza.
V. Mejora de la calidad de vida humana en Indonesia.
VI. Mejorar la productividad y la competitividad de las personas en el mercado internacional.
VII. Alcanzar la independencia económica acelerando la estrategia de sectores de la economía nacional.
VIII. Llevar a cabo una revolución sobre el carácter de la nación.
IX. Fortalecimiento de la diversidad y la restauración social.[82]

[82] Ministerio de Defensa de la República de Indonesia*, Libro Blanco de Defensa, Capítulo 4 Política, estratégica y manejo de la Defensa Nacional*, Indonesia, 2015, Disponible en: https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIA-DEFENCE-WHITE-PAPER-ENGLISH-VERSION.pdf (Traducción del inglés al español realizada por Mariana Corona Fragoso)

Continente: **Oceanía**

País: *Australia*
Documento: *2020 Estrategia de Seguridad Nacional.*

Objetivos de seguridad nacional:

I. Proteger y fortalecer la soberanía.
II. Garantizar una seguridad y población resiliente.
III. Asegurar los activos, infraestructura e instituciones.
IV. Promover un ambiente internacional favorable.

Dentro de dichos objetivos, se encuentran los retos a afrontar para mantener la seguridad nacional los cuales se traducen en los siguientes riesgos clave:

- Espionaje e injerencia extranjera
- Inestabilidad den Estados frágiles y en desarrollo
- Actividad cibernética maliciosa
- Proliferación de armas de destrucción masiva
- Delincuencia organizada
- Conflicto o coerción estatal que afecte los intereses de Australia
- Terrorismo y extremismo violento.[83]

País: *Papúa Nueva Guinea*

Documento: *2013 Política de Seguridad Nacional de Papúa Nueva Guinea.*

Áreas prioritarias para el gobierno:

I. Ley y orden.
II. Soborno y corrupción y buen gobierno.
III. Abusos a los Derechos Humanos y violencia de género.
IV. Control fronterizo.
V. Desastres naturales y cambio climático.
VI. Proliferación de armas pequeñas y ligeras.
VII. Pesca ilegal y caza furtiva.
VIII. Drogas, alcohol y abuso de sustancias.
IX. Ataques microbianos a plantas, animales y derechos humanos.
X. Emergencias médicas incluyendo VIH SIDA, tuberculosis y malaria.

[83] Gobierno de Australia; Departamento del primer ministro y Gabinete, *Estrategia para la Seguridad Nacional de Australia*, Australia, 2013, Disponible en: https://www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf

Estrategia de implementación.

Existen 10 áreas prioritarias para la atención del Gobierno a través de los objetivos de política y las estrategias de implementación propuestas. Estas 10 áreas prioritarias se capturan en los 9 objetivos de la Política de Seguridad:

I. Garantizar que Papúa Nueva Guinea (PNG) se mantenga políticamente estable, segura y protegida.
II. Garantizar que PNG siga siendo económicamente próspera.
III. Garantizar la protección de la diversidad cultural de PNG, del servicio de entrega y de la armonía social.
IV. Mantener una relación cordial y amigable con la comunidad global.
V. Mantener la integridad del espacio soberano de PNG.
VI. Apoyar, mantener y fortalecer los marcos legislativos nacionales.
VII. Garantizar la seguridad ambiental.
VIII. Garantizar la seguridad tecnológica.
IX. Coordinación eficaz de la seguridad nacional y su implementación a través de un enfoque nacional completo.[84]

País: *Nueva Zelanda*

Documento: *2018 diciembre 2018. Prioridades de inteligencia y Seguridad Nacional Departamento del primer ministro y Gabinete (DPMC).*

En diciembre de 2018, el Gabinete aprobó un nuevo conjunto de prioridades de inteligencia y seguridad nacional. Las 16 prioridades de inteligencia y seguridad nacional son:

I. Bioseguridad y salud humana.
II. Medio ambiente, cambio climático y recursos naturales.
III. Influencia extranjera, injerencia y espionaje.
IV. Economía, comercio e inversiones globales. Avances en la gobernanza del comercio internacional y las relaciones comerciales bilaterales, plurilaterales y multilaterales de Nueva Zelandia.
V. ***Implicaciones de la tecnología emergente.*** **Las implicaciones de las tendencias emergentes de tecnología e innovación para la seguridad**

[84] Gobierno de Papúa Nueva Guinea, *Política de Seguridad Nacional, Capítulo 6, Metas y estrategia de implementación de la política*, Papúa Nueva Guinea, 2013, Disponible en: https://www.aspistrategist.org.au/wp-content/uploads/2014/08/2013-PNG-National-Security-Policy.pdf
Traducción del inglés al español realizada por Mariana Corona Fragoso.

nacional, las relaciones internacionales y el bienestar económico de Nueva Zelanda.

VI. *Gobernanza internacional, geopolítica y seguridad global.*
VII. ***Actividad cibernética maliciosa.*** **Amenazas cibernéticas a Nueva Zelanda por parte de actores malintencionados patrocinados por el Estado y otros.**
VIII. Seguridad regional de Oriente Medio.
IX. Interés estratégico de Nueva Zelanda en la región de Asia.
X. Estabilidad regional del Pacífico.
XI. Proliferación de armas de destrucción masiva y armas convencionales.
XII. Seguridad espacial.
XIII. Seguridad territorial y soberanía.
XIV. Terrorismo.
XV. Amenazas a los neozelandeses en el extranjero.
XVI. Delincuencia organizada transnacional.[85]

Continente: **África**
País: *Egipto*
Documento: *2019. Objetivos de política exterior y seguridad nacional*

El primer ministro, Moustafa Madbouli, dio la declaración de política del gobierno, la que se implementará durante el segundo mandato presidencial del presidente Abdel Fattah Al-Sisi (2019-2022), incluida la política exterior y los objetivos de seguridad nacional.

Los objetivos de política exterior y seguridad nacional de Egipto se centrarán en cuatro temas principales:

I. Mantener una política equilibrada con todas las potencias mundiales.
II. Garantizar la seguridad y estabilidad de la Región del Golfo.
III. Garantizar la seguridad nacional en los ámbitos regional y africano.
IV. Activar el papel del Centro Internacional de El Cairo para la resolución de conflictos, el mantenimiento de la paz y la consolidación de la paz.[86]

[85] Departamento del Primer Ministro; Gabinete*, Prioridades de inteligencia y Seguridad Nacional,* Nueva Zelanda, 2018, Disponible en: https://dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security-and-intelligence-priorities
[86] Gobierno de Egipto, *Fundamentos de la Política Egipcia,* Egipto, Servicio de información estatal, 2019, Disponible en: https://www.sis.gov.eg/section/0/52?lang=en-us

País: *Kenia*

Documento: *2017. Política de Defensa Nacional. Libro Blanco de Defensa de Kenia.*

En el marco para el Libro Blanco de Defensa, se consideran los siguientes temas para la preservación de la Seguridad Nacional:

I. Hacer frente a las amenazas militares.
II. Terrorismo.
III. Paz y seguridad regionales e internacionales.
IV. Amenazas cibernéticas.
V. Amenazas para la seguridad sanitaria nacional.
VI. Explotación de la Zona Económica Exclusiva.
VII. Degradación ambiental.
VIII. Actividades para el desarrollo económico nacional.
IX. Actividades de desarrollo industrial nacional y de defensa.
X. Investigación de desarrollo en ciencia espacial y defensa.
XI. Administración de recursos.
XII. Desarrollo de recursos humanos.
XIII. Creación de capacidad para el componente civil.
XIV. Incorporación de la perspectiva de género.
XV. Terreno para el uso militar.[87]

País: *Botswana*

Documento: *No tiene una Estrategia de Seguridad Nacional*

[87] Ministerio de la Defensa de la República de Kenia, *Libro Blanco de la Defensa*, Kenia, 2017. Disponible en: https://mod.go.ke/download/national-defence-policy/

Tabla 2. Países cuyas Agendas de Seguridad Nacional incluyen a la ciberseguridad o ciberguerra

Países cuyas Agendas de Seguridad Nacional incluyen a la ciberseguridad o ciberguerra																	
																	
Estados Unidos	México	Uruguay	Rusia	Suecia	España	Arabia Saudita	Irán	Israel	Japón	China	Indonesia	Australia	Papúa Nueva Guinea	Nueva Zelanda	Egipto	Kenia	Botswana
✓	✗	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✓	✗	✓	✗	✓	✗
¿Cuentan con una Estrategia de Ciberseguridad Nacional?																	
✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Fuente: Elaboración propia con base en la información presentada en el capítulo

A partir de la documentación de las estrategias de seguridad anteriormente presentadas, se procederá a analizar lo que involucra la consideración del ciberespacio para la seguridad nacional en general, específicamente, en la vulneración a las infraestructuras críticas.

Como respaldo para dicho análisis se hará referencia al *Global Cybersecurity Index 2020,* en lo relativo a los datos cuantitativos que arroja, y también al estudio sobre la Percepción de Riesgos Globales del Foro Económico Mundial en su edición del 2020.

Para dar comienzo al análisis, un estudio realizado anualmente por el Foro Económico Mundial enlista los 10 riesgos globales más significativos para la seguridad nacional y el bienestar global. Parte de la iniciativa de Riesgos Globales, incluye un análisis sostenido a nivel mundial, regional y a distintos niveles de la industria; reúne líderes de las empresas, del gobierno y de comunidades sin fines de lucro, además utiliza las conclusiones de este documento para informar sobre cuáles son los puntos de vulnerabilidad para la seguridad, la economía, y la sociedad.

El Foro divide dicho listado en dos partes; primero señala los 5 riesgos globales en “Términos de probabilidad” y hace referencia a los otros 5 en “Términos de impacto”, lo que permite distinguir entre aquellas posibilidades de vulnerar el bienestar y la preservación global, mientras que señala por otro lado, el daño que pueden generar dichos riesgos en dado caso de suscitarse. A continuación, se presenta dicho listado:

Figura 6. El panorama de la evolución de riesgos, 2007-2020

Fuente: Foro Económico Mundial. Reporte Global de Riesgos. El panorama de Riesgos, 2007-2020

La tabla anterior señala que en ambas categorías (Términos de Probabilidad y Términos de impacto), la presencia de riesgos relacionados al sector tecnológico se encuentra presente de forma variada, entre ellas destacan: daño a la infraestructura crítica, ciberataques o fraude/robo de datos. Hay que destacar, que en la primera categoría estos riesgos tienen presencia de manera más evidente durante todo el periodo abarcado por el estudio, aún más, de 2017 a 2019.

Es imperativo resaltar el año 2007, año en el que aconteció el primer incidente cibernético de carácter estatal con daño a la infraestructura crítica en Estonia; dicho suceso claramente concuerda con el riesgo clasificado en el primer lugar, que se expone en el cuadro anteriormente presentado.

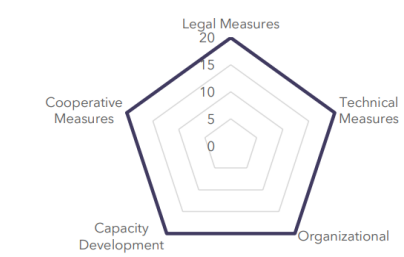
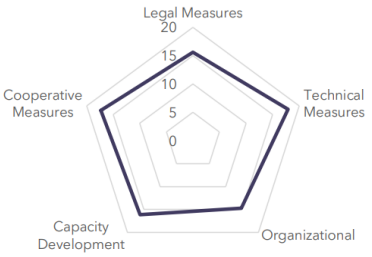
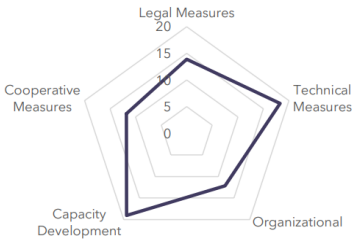
A su vez, con el paso del tiempo se incorporan otros riesgos, que involucran factores económicos, medioambientales, geopolíticos y sociales. Sin embargo, aquellos años en los que los riesgos tecnológicos se acrecientan, coinciden con algunos de los ciberataques más importantes en la historia. (Ciberataque a *Dropbox* 2012, a *eBay* en 2014, ataque a la red eléctrica de Ucrania en 2016, Virus *Wanna Cry* 2017, el ataque al Bundestag alemán en 2019, etc.).

En contraste con la documentación de la Agendas de Seguridad Nacional, se evidencía que aquellos países que retoman los temas de seguridad cibernética dentro de las áreas a atender dentro de sus Estrategia de Seguridad Nacional son los mismos que son considerados “líderes” o “desarrollados”, para la Sociedad Internacional y su discursiva.

A partir del estudio del Foro Económico, es posible resaltar cómo es que esos países, que tomaron en cuenta a la ciberseguridad en sus directrices, tuvieron una importante ventaja ante los riesgos constantemente presentes durante el periodo de 2007-2020, así como de los ciberataques, daño a la infraestructura crítica, y robo de datos.

Por otro lado, las estadísticas arrojadas por el *Global Cybersecurity Index 2020* coincide con el lugar en el que se ubica a los países seleccionados para este análisis en los primeros y últimos lugares, global y regionalmente como se muestra a continuación:

Tabla 3. Relación de países seleccionados en Ranking global y regional.

País	Lugar Global	Lugar Regional	Perfil del país
Estados Unidos	1	1	*United States of America***  **Development Level:** Developed Country **Area(s) of Relative Strength** Legal, Organizational, Cooperative Measures, Capacity Development **Area(s) of Potential Growth** N/A
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
México	52	4	*Mexico*  **Development Level:** Developing Country **Area(s) of Relative Strength** Cooperative Measures **Area(s) of Potential Growth** Organizational Measures
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
Uruguay	64	5	*Uruguay (Eastern Republic of)*  **Development Level:** Developing Country **Area(s) of Relative Strength** Capacity Development **Area(s) of Potential Growth** Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
100.00	20.00	20.00	20.00	20.00	20.00

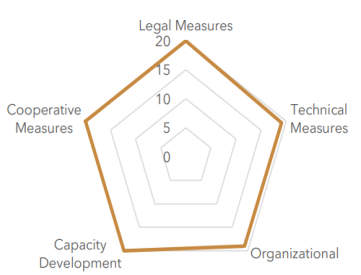
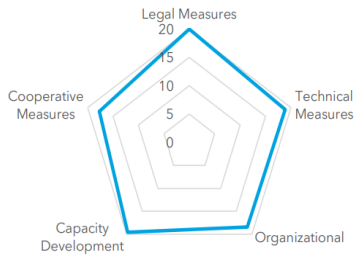
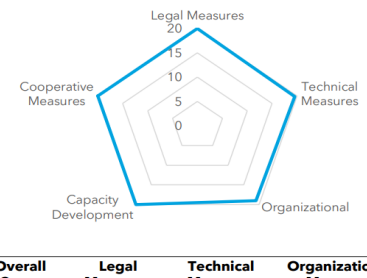
Source: ITU Global Cybersecurity Index v4, 2021

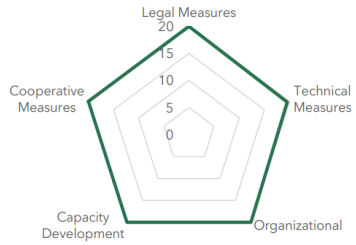
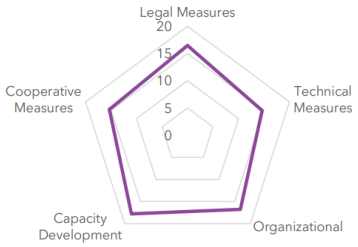
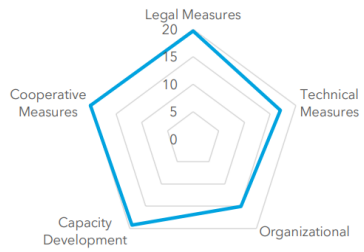
Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
81.68	15.61	17.90	14.70	16.13	17.34

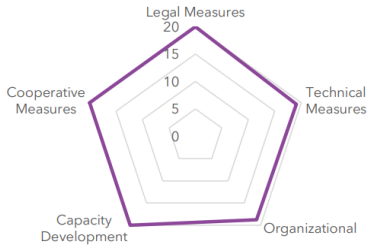
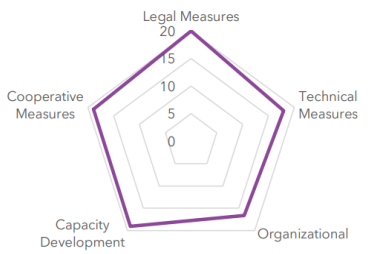
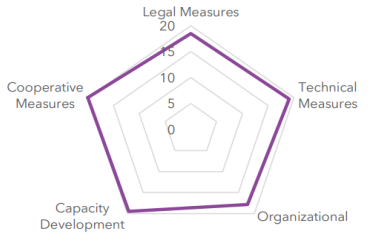
Source: ITU Global Cybersecurity Index v4, 2021

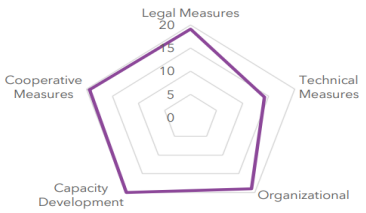
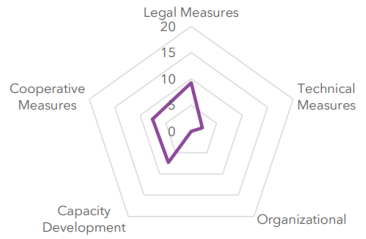
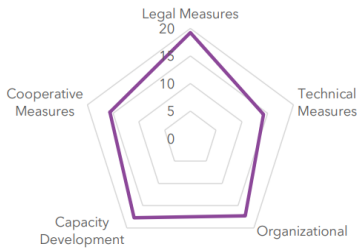
Overall Score	Legal Measures	Technical Measures	Organizational Measures	Cooperative Measures	Capacity Development
75.15	13.90	18.27	12.13	19.04	11.81

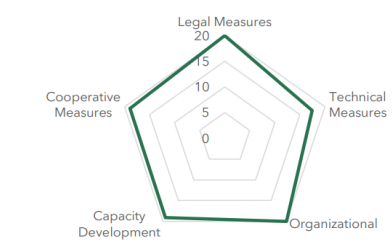
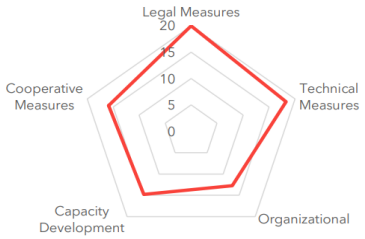
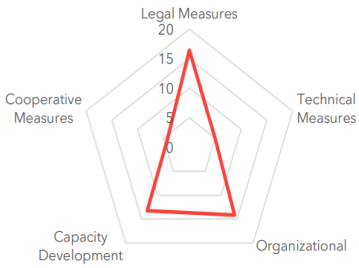
Source: ITU Global Cybersecurity Index v4, 2021

País	Lugar Global	Lugar Regional	Perfil del país
Rusia	5	1	*Russian Federation*  **Development Level:** Developed Country **Area(s) of Relative Strength** Legal, Cooperative Measures, Capacity Development **Area(s) of Potential Growth** Organizational Measures **Overall Score** 98.06 · **Legal Measures** 20.00 · **Technical Measures** 19.08 · **Organizational Measures** 18.98 · **Capacity Development** 20.00 · **Cooperative Measures** 20.00 Source: ITU Global Cybersecurity Index v4, 2021
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
Suecia	26	15	*Sweden*  **Development Level:** Developed Country **Area(s) of Relative Strength** Legal Measures **Area(s) of Potential Growth** Organizational Measures **Overall Score** 94.59 · **Legal Measures** 20.00 · **Technical Measures** 18.86 · **Organizational Measures** 18.46 · **Capacity Development** 19.57 · **Cooperative Measures** 17.70 Source: ITU Global Cybersecurity Index v4, 2021
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
España	4	3	*Spain*  **Development Level:** Developed Country **Area(s) of Relative Strength** Legal, Cooperative Measures, Capacity Development, Technical Measures **Area(s) of Potential Growth** Organizational Measures **Overall Score** 98.52 · **Legal Measures** 20.00 · **Technical Measures** 19.54 · **Organizational Measures** 18.98 · **Capacity Development** 20.00 · **Cooperative Measures** 20.00 Source: ITU Global Cybersecurity Index v4, 2021

País	Lugar Global	Lugar Regional	Perfil del país
Arabia Saudita	2	1	*Saudi Arabia (Kingdom of)*  **Development Level:** Developing Country **Area(s) of Relative Strength** Legal, Organizational, Cooperative Measures, Capacity Development **Area(s) of Potential Growth** Technical Measures **Overall Score** 99.54 · **Legal Measures** 20.00 · **Technical Measures** 19.54 · **Organizational Measures** 20.00 · **Capacity Development** 20.00 · **Cooperative Measures** 20.00 Source: ITU Global Cybersecurity Index v4, 2021
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
Irán	54	12	*Iran (Islamic Republic of)*  **Development Level:** Developing Country, Least Developed Countries (LDC), Landlocked Country **Area(s) of Relative Strength** Capacity Development, Organizational Measures **Area(s) of Potential Growth** Technical, Legal, Cooperative Measures **Overall Score** 81.06 · **Legal Measures** 16.48 · **Technical Measures** 14.63 · **Organizational Measures** 16.82 · **Capacity Development** 17.80 · **Cooperative Measures** 15.33 Source: ITU Global Cybersecurity Index v4, 2021
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
Israel	36	23	*Israel (State of)***  **Development Level:** Developed Country **Area(s) of Relative Strength** Technical Measures, Capacity Development **Area(s) of Potential Growth** Legal, Organizational Measures **Overall Score** 90.93 · **Legal Measures** 19.68 · **Technical Measures** 16.99 · **Organizational Measures** 15.02 · **Capacity Development** 19.24 · **Cooperative Measures** 20.00 Source: ITU Global Cybersecurity Index v4, 2021

País	Lugar Global	Lugar Regional	Perfil del país
Japón	7	3	*Japan*  **Development Level:** Developed Country **Area(s) of Relative Strength** Legal, Cooperative Measures, Capacity Development **Area(s) of Potential Growth** Organizational Measures **Overall Score** 97.82 | **Legal Measures** 20.00 | **Technical Measures** 19.08 | **Organizational Measures** 18.74 | **Capacity Development** 20.00 | **Cooperative Measures** 20.00 Source: ITU Global Cybersecurity Index v4, 2021
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
China	33	8	*China (People's Republic of)*  **Development Level:** Developing Country, Least Developed Countries (LDC), Landlocked Country **Area(s) of Relative Strength** Legal Measures **Area(s) of Potential Growth** Organizational Measures **Overall Score** 92.53 | **Legal Measures** 20.00 | **Technical Measures** 17.94 | **Organizational Measures** 16.63 | **Capacity Development** 19.04 | **Cooperative Measures** 18.91 Source: ITU Global Cybersecurity Index v4, 2021
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
Indonesia	24	6	*Indonesia (Republic of)*  **Development Level:** Developing Country, Least Developed Countries (LDC), Landlocked Country **Area(s) of Relative Strength** Cooperative, Technical Measures, Capacity Development **Area(s) of Potential Growth** Organizational Measures **Overall Score** 94.88 | **Legal Measures** 18.48 | **Technical Measures** 19.08 | **Organizational Measures** 17.84 | **Capacity Development** 19.48 | **Cooperative Measures** 20.00 Source: ITU Global Cybersecurity Index v4, 2021

País	Lugar Global	Lugar Regional	Perfil del país
Australia	12	5	*Australia*  **Development Level:** Developed Country **Area(s) of Relative Strength** Capacity Development, Cooperative Measures, Legal Measures **Area(s) of Potential Growth** Technical Measures **Overall Score** 97.47 | **Legal Measures** 20.00 | **Technical Measures** 19.08 | **Organizational Measures** 18.98 | **Capacity Development** 20.00 | **Cooperative Measures** 19.41 Source: ITU Global Cybersecurity Index v4, 2021
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
Papúa Nueva Guinea	118	21	*Papua New Guinea***  **Development Level:** Developing Country, Small Island Developing States (SIDS) **Area(s) of Relative Strength** Capacity Development **Area(s) of Potential Growth** Cooperative Measures **Overall Score** 26.33 | **Legal Measures** 9.26 | **Technical Measures** 2.18 | **Organizational Measures** 0.00 | **Capacity Development** 7.30 | **Cooperative Measures** 7.59 Source: ITU Global Cybersecurity Index v4, 2021
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
Nueva Zelanda	48	10	*New Zealand***  **Development Level:** Developed Country **Area(s) of Relative Strength** Legal Measures **Area(s) of Potential Growth** Technical Measures **Overall Score** 84.04 | **Legal Measures** 19.24 | **Technical Measures** 14.19 | **Organizational Measures** 17.27 | **Capacity Development** 17.71 | **Cooperative Measures** 15.63 Source: ITU Global Cybersecurity Index v4, 2021

País	Lugar Global	Lugar Regional	Perfil del país
Egipto	23	4	*Egypt (Arab Republic of)*  **Development Level:** Developing Country **Area(s) of Relative Strength** Legal, Organizational Measures, Capacity Development **Area(s) of Potential Growth** **Overall Score** 95.48; **Legal Measures** 20.00; **Technical Measures** 17.45; **Organizational Measures** 20.00; **Capacity Development** 19.12; **Cooperative Measures** 18.91 Source: ITU Global Cybersecurity Index v4, 2021
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
Kenia	51	5	*Kenya (Republic of)*  **Development Level:** Developing Country **Area(s) of Relative Strength** Legal, Technical Measures **Area(s) of Potential Growth** Organizational Measures **Overall Score** 81.70; **Legal Measures** 20.00; **Technical Measures** 18.27; **Organizational Measures** 12.75; **Capacity Development** 14.79; **Cooperative Measures** 15.89 Source: ITU Global Cybersecurity Index v4, 2021
País	**Lugar Global**	**Lugar Regional**	**Perfil del país**
Botswana	88	12	*Botswana (Republic of)*  **Development Level:** Developing Country, Landlocked Country **Area(s) of Relative Strength** Legal Measure **Area(s) of Potential Growth** Cooperative Measures, Technical Measures **Overall Score** 53.06; **Legal Measures** 16.44; **Technical Measures** 4.95; **Organizational Measures** 14.16; **Capacity Development** 13.23; **Cooperative Measures** 4.26 Source: ITU Global Cybersecurity Index v4, 2021

Fuente: Elaboración propia a partir de: **Unión Internacional de Telecomunicaciones**, *Global Cybersecurity Index 2020* [en línea], 155 pp, Ginebra Suiza, 2021,

En suma, a partir de los datos que se exponen en las tablas anteriores se observan dos elementos fundamentales:

1. Considerar a los ciberataques/ciberseguridad dentro de las prioridades de seguridad nacional, confirma tener una relación directa con la posición que cada país posee dentro de estudios o indicadores evaluativos acerca del nivel de seguridad que mantiene, ya que funciona como una estrategia ofensiva y defensiva, mejorando así sus condiciones ante ataques cibernéticos como los señalados en el cuadro del Foro.
2. Estar preparados ante posibles amenazas cibernéticas desde la génesis de la seguridad como son las Agendas de Seguridad Nacional, permite que la preservación del Estado no solo se mantenga desde un enfoque bélico-militar, sino que a su vez se extiende hacia la seguridad de otras áreas de vital importancia como la financiera, petrolera, ecológica (mismas que el estudio del Foro Económico señala en el cuadro presentado). Elevando así de manera general, la seguridad, aun cuando los contextos de cada Estado y sus prioridades de atención varían, ya que actualmente la tecnologización y digitalización de información abarca una gran diversidad de áreas y contextos.

La implementación de las tecnologías en un contexto donde la digitalización de la información es ineludible, conduce a los países necesariamente a sistematizar la red de instituciones encargadas de coordinar las funciones de la infraestructura crítica, social y gubernamental, así como de la información, las claves, los planes, los protocolos, y de una infinita cantidad de datos que son delicados en su manejo y conocimiento.

Al introducirse en el ámbito ciberespacial, se entra también en una zona de riesgo. En suma, va a depender de la consideración gubernamental y de la administración pública de cada país priorizar la ciberseguridad, y a su vez, reconocer el estatus activo de la ciberguerra dentro del ciberespacio mundial, lo que será determinante para poder salvaguardar las áreas e instituciones que garantizan la seguridad nacional.

En este contexto, a partir de los datos recabados en este capítulo, también se puede concluir que si bien la mayoría de los países consultados consideran los temas de ciberseguridad en su agenda y/o cuentan con una estrategia de ciberseguridad, la calidad de dichos protocolos condicionará e influirá en el nivel de seguridad y

vulnerabilidad que pueda tener cada país ante una ciberamenaza, lo cual se refleja en la evaluación que hacen diferentes organizaciones, como fue el caso de los dos referentes empleados en el análisis, principalmente en el *Global Cybersecurity Index,* específicamente en las gráficas anexas en la Tabla 3 que presenta los estándares evaluativos, y el puntaje obtenido al momento de calificar el nivel de ciberseguridad que cada Estado alcanza.

Lo anterior conduce a considerar una política y posición preventiva que inicia desde el reconocimiento imperante de la evolución de las agendas de seguridad nacional de la mano con las demandas del contexto digital, cibernético y tecnológico, del cual son parte.

Además, la imperante necesidad de concretar las líneas de procedimiento de cada país en el dominio ciberespacial de manera defensiva y ofensiva permitirán dilucidar la estructura del campo bélico que ha comenzado a ser implementado de manera cada vez más constante.

2.2 La evolución de la ciberguerra en el escenario internacional, como factor relevante en las dinámicas de conflicto.

En la última década, el ciberespacio y la securitización de éste, ha ganado atención debido a la fuerza con la que acompaña en todos los ámbitos al "ser humano moderno". El escenario internacional moderno se caracteriza por la aparición de nuevas amenazas estratégicas, entre ellas el terrorismo global, así como la presencia de diversas modalidades de ataque que emergen y se producen a través del ciberespacio; lo cual demuestra que la superioridad militar tradicional no garantiza ser un factor eficaz de disuasión, ni proporciona con certeza mayor seguridad en este escenario cibernético.[88]

Para **Andrés Gaitán** existen tres generaciones o "etapas" para comprender la incidencia de las TIC dentro de escenarios de conflicto bélico. Gaitán identifica, al mismo tiempo, coyunturas históricas en las que tuvieron lugar "[...] los computadores, la Internet y el ciberespacio como una dimensión de interacción humana, se han

[88] Julio Albert Ferrero, "La ciberguerra. Génesis, y evolución", *Revista General de Marina*, Madrid, España, Ministerio de Defensa, Vol. 264, enero-febrero 2013, p. 87.

prestado como medios para atacar a un enemigo o contendiente al interior de la categoría de los conflictos regulares [...]"[89]

1. **Primera Generación: el control psicológico.**

   Establecida en la década de 1990, se desarrolla a partir de la Guerra del Golfo Pérsico, el elemento clave a controlar fue a través de la generación de información/datos, imágenes y declaraciones falsas, así como de la simulación de escenarios ficticios. La manipulación psicológica del enemigo provocó que éste tomara decisiones precipitadas, o generara información que le significara una ventaja al contrario en la contienda.[90] Lo anterior se consiguió a través de las Operaciones de Información (OI), dichas operaciones se basaban en el análisis de la tecnología, los procesos y los factores humanos vulnerables de la mente de los tomadores de decisiones. A su vez, se diseñaron para ser dirigidas contra líderes o tomadores de decisiones de alto nivel al irrumpir en su capacidad para orientar eficazmente sus operaciones dado que imposibilita la generación de un razonamiento objetivo. El daño también puede instalarse en cada escalón de la estructura militar, industrial e incluso de la población en general[91]. El objetivo de esta generación se fundamentó en el principio de buscar la desarticulación parcial o total de los sistemas de comunicación del enemigo con un efecto psicológico en la contraparte, o bien, lo que se denomina como "estructura de comando y control".

2. **Segunda Generación: el control de la infraestructura crítica del Estado.**

   Con la entrada del modelo económico de la globalización y la introducción de diversos dispositivos informáticos, se dio paso a la conformación del ciberespacio, lo cual es fundamental para comprender la segunda generación de la ciberguerra.

   La distribución de dispositivos informáticos en las actividades individuales, colectivas, nacionales e internacionales, condicionaron que emergiera la comunidad y sociedad global interconectada, la cual, a su vez, demandó el

[89] Andrés Gaitán Rodríguez, "La ciberguerra y sus generaciones: un enfoque para comprender la incidencia de las TIC en la guerra regular", *Revista Científica de Estudios en Seguridad y Defensa,* España, Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacionales, Vol. 7, núm. 13, 2012, p. 1-2.
[90] Ibid. p. 6.
[91] Ashley Bradley K., *Anatomy of Cyberterrorism Is America Vulnerable*. United States, Air War College. Air University, 2003. p. 4.

rendimiento, dinamismo y acceso a la información que ya tenía impacto en la vida social, económica y política del ser humano.

A partir de la penetración tecnológica anteriormente descrita, fue que la transformación gubernamental en todo el mundo comenzó una evolución; es decir, diversos ministerios e instituciones encargadas de la administración pública modificaron la forma en la que sus actividades, procedimientos y articulación de las capacidades se desarrollaban, y se trasladaron al ámbito informático y ciberespacial. Los sistemas financieros, bancarios y bolsas de valores, empresas y compañías del sector privado, sistemas de control de tránsito (aéreo y terrestre), sistemas de funcionamiento (fuentes de energía, acueductos, gasoductos, redes de comunicación, etc.), las fuerzas y sistemas de defensa y seguridad, y finalmente, la misma sociedad.[92*]

En suma, el control de la infraestructura crítica de un Estado por los canales ciberespaciales en los que ya estaban adentrados los principales pilares de funcionamiento estatal fue una posibilidad completamente abierta en la búsqueda del debilitamiento del enemigo. El comandante William Gibson (especialista informático militar), explica dicha posibilidad, evidenciando que lo determinante de esta segunda generación, y etapa histórica, fue el fenómeno "causa y efecto" que correspondía perfectamente entre lo que acontece en el plano ciberespacial y en el plano físico-material; puesto que el mundo virtual y físico logran converger de forma tal, que las acciones desarrolladas en cada uno de ellos tienen repercusiones semejantes en el otro.[93]

En un conflicto interestatal, las acciones promovidas por un Estado que tengan por objetivo dañar las capacidades de otro, para disuadirlo en materia política, económica o de intereses nacionales, pero donde el medio empleado es un ataque informático, puede situarse en ventaja. Ejemplos de esta segunda

[92]*A la conjunción de estos elementos se le denomina "infraestructura crítica estatal". Los sistemas y los activos ya sean físicos o virtuales, que son sumamente vitales para los Estados Unidos y que en caso de ser incapacitados o destruidos, los activos tendrían un impacto debilitante en la seguridad, la seguridad económica nacional, la salud o la seguridad pública, o cualquier combinación de dichos asuntos.

[93] Op. Cit., Andrés Gaitán, p. 10.

generación se reflejan en conflictos como; Operación *Titan Rain* (China 2002)[94]*, Estonia 2007, Georgia 2008, Stuxnet 2010, etc.

3. **Tercera Generación: el control del armamento.**

Con los antecedentes de las dos generaciones anteriores, la tercera generación trasciende de gobernar sistemas informáticos que se encaminan a controlar los procesos estatales fundamentales de un Estado-Nación, al dominio de artefactos bélicos que conforman la estructura militar y de seguridad, materializando sus efectos de forma tangible. 2004 fue el año de referencia en el inicio de esta generación, bajo el contexto histórico en el que EE. UU se enfrentaba con países de Medio Oriente (Afganistán y Pakistán), en su búsqueda por desarticular al grupo terrorista Al Qaeda como resultado del atentado del 9/11, se posibilitó a los organismos de inteligencia a realizar un cambio sustancial en materia tecnológica. La presencia de máquinas dirigidas a control remoto refería que los canales de transmisión y sistemas de control que incorporaron dichas tecnologías entraban en el conglomerado de la red global de comunicaciones, la internet, y el ciberespacio *per se*.

Hacia el año 2010, con Israel en el foco de tensión bélica estadounidense se incorporan los drones que, entre muchas funciones, también se utilizaron como transporte de material de ataque y bombardeo. En el contexto de conflicto, el robo abarcó el control de mando de éstos a través de códigos cibernéticos. Las fuerzas militares que detentan la posesión y empleo de esta clase de aeronaves ya no son los únicos actores con la capacidad de ejercer la cibernética en el teatro de operaciones. Ahora, el contrario se encuentra con la capacidad de hacerse al control del armamento hostil.

> Esto, si bien no ha conllevado a nuevos episodios de ciberguerra, si pone de manifiesto que la figura de un enemigo con la capacidad para ejercer control sobre esta tecnología, cada vez tendrá una probabilidad mayor de poder despojar a sus contrarios de su armamento; o bien, no se debería descartar al momento de instaurar medidas de seguridad.[95]

[94] *Esta iniciativa fue puesta en práctica por el Gobierno Chino y el Ejército Popular de Liberación a partir del año 2002, con el fin de hackear los sistemas informáticos gubernamentales y de industria nacional de países como Estados Unidos de Norteamérica y Alemania, entre otros

[95]Op. Cit., Andrés Gaitán Rodríguez, p. 13.

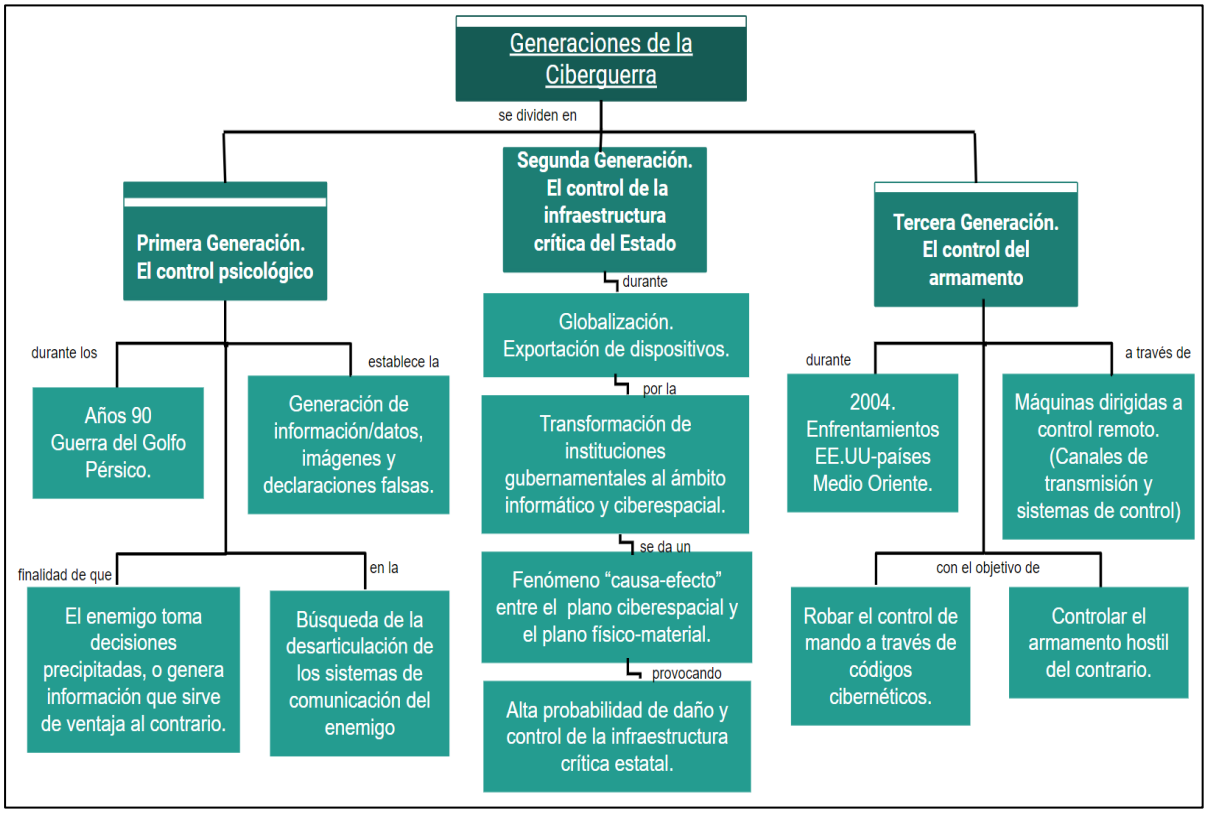
La taxonomía que hace Gaitán en su propuesta por identificar la evolución de las TIC como catailizadores de canales para el conflicto cibernético, demuestra cómo de manera social éstas han reconfigurado el espacio y la dinámica del conflicto entre Estados a nivel particular, nacional e internacional. Lo anterior evidencía que la tecnología es “social hasta la médula” y, por otra parte, que el perfeccionamiento tecnológico ha sido un arma de doble filo en la confrontación interestatal; por un lado, facilita el ataque a los sistemas y apropiación de armamento enemigo, pero a su vez es una puerta de vulnerabilidad a los propios. En este sentido, destaca que las tres generaciones que sugiere el autor van acompañadas de coyunturas históricas, mismas que a su vez se ven enmarcadas por la paulatina incorporación y perfeccionamiento de herramientas tecnológicas en el sector militar y de seguridad. Lo anterior, muestra que ciberespacio se ha convertido así en una “espacialidad en sí misma” y para la sociedad digital, que contiene relaciones de poder y situaciones específicas que lo convierten en un producto y productor de relaciones sociales.

Tomar en cuenta la propuesta de Gaitán constata que la ciberguerra y los ciberataques, son el resultado de un perfeccionamiento paulatino de las técnicas y herramientas, puestas en acción bajo determinados contextos históricos y, en la mayoría de los casos, en contextos de tensión política, o bélica.

A nivel internacional, éstas tres generaciones brindan tres momentos de evolución tecnológica e histórica. No obstante, también da paso a futuros debates que puedan enriquecer la evolución de la ciberguerra, pero estratégicamente, las mencionadas con anterioridad engloban lo social, lo bélico, lo estratégico, lo histórico y lo tecnológico en un terreno claro y definido de la configuración de la ciberguerra en el escenario internacional.

A continuación, se presenta un organizador gráfico para ilustrar los momentos anteriormente explicados:

Figura 7. Generaciones de la Ciberguerra



Fuente: Elaboración propia a partir de: **Andrés Gaitán**, *La ciberguerra y sus generaciones: un enfoque para comprender la incidencia del TIC en la guerra regular,* España, CEESEDEN Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacionales, 2012, 18 pp.

En cuanto a las organizaciones internacionales, los temas de seguridad cibernética y ciberguerra no han sido retomados por órganos como la Organización de las Naciones Unidas, de manera especializada ni específica.

La incorporación del tema a la agenda internacional como directriz de ésta, al menos en lo que respecta a la agenda de la Asamblea General Plenaria de las Naciones Unidas no ha tenido lugar. La siguiente tabla muestra los temas que ha tratado la Asamblea desde su 60° sesión celebrada en 2005.

Tabla 4. Lista de temas designados para el Debate General de la Asamblea General Plenaria de las Naciones Unidas en su 60º periodo de sesiones, 2005.

Sesión	Año	Tema
75ª	**2020**	**"El futuro que queremos, las Naciones Unidas que necesitamos: reafirmar nuestro compromiso colectivo con el multilateralismo, afrontar la COVID-19 mediante la acción multilateral eficaz".**
74ª	2019	"Impulsar los esfuerzos multilaterales para la erradicación de la pobreza, la calidad de la educación, la acción contra el cambio climático y la inclusión".
73ª	2018	"Conseguir que las Naciones Unidas sean pertinentes para todos: liderazgo mundial y responsabilidades compartidas para lograr sociedades pacíficas, equitativas y sostenibles".
72ª	2017	"Centrarse en los pueblos - luchar por la paz y por una vida digna para todos en el planeta".
71ª	2016	"Los Objetivos de Desarrollo Sostenible: un impulso universal para transformar nuestro mundo".
70ª	2015	"Las Naciones Unidas a los 70: un nuevo compromiso para la acción".
69ª	2014	"Cumplimiento y aplicación de una agenda transformadora para el desarrollo después de 2015".
68ª	2013	"El camino a seguir: una agenda para el desarrollo que tenga en cuenta a las personas con discapacidad para 2015 y después de ese año".
67ª	2012	"Lograr el ajuste o solución de controversias o situaciones internacionales por medios pacíficos".
66ª	2011	"La función de la mediación en el arreglo pacífico de controversias".
65ª	2010	"Reafirmación de la función central de las Naciones Unidas en la gobernanza global".
64ª	2009	"Respuestas efectivas ante las crisis mundiales: intensificación de las relaciones multilaterales y del diálogo entre las civilizaciones en pro de la paz, la seguridad y el desarrollo internacionales".
63ª	2008	"Las repercusiones de la crisis alimentaria mundial en la pobreza y el hambre en el mundo y la necesidad de democratizar las Naciones Unidas".
62ª	2007	"Respuesta al cambio climático".
61ª	2006	"Puesta en práctica de una alianza mundial para el desarrollo".
60ª	2005	"En pro del fortalecimiento y la eficacia de las Naciones Unidas: seguimiento y aplicación de los resultados de la reunión plenaria de alto nivel de septiembre de 2005".

Fuente: Organización de las Naciones Unidas. Asamblea General Plenaria. https://www.un.org/es/ga/sessions/regular.shtml

Con base en la información anteriormente presentada, se muestra como la agenda, en este caso de la organización internacional con mayor influencia en el mundo, incorpora una diversidad amplia de temáticas. Sin embargo, solo es en la 64° sesión de 2009 la cual hace mención a la seguridad de manera general; a pesar de ello, no existe una referencia hacia lo cibernético y existe sólo una resolución del año 2013 de la Asamblea durante la 68ª sesión de trabajo, titulada (A/RES68/243) *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional* [96] su objetivo al llevarse a cabo se centró en "mantener la estabilidad y la seguridad internacional ante factores que afecten negativamente a la integridad de la infraestructura de los Estados, en detrimento de su seguridad en las esferas civil y militar."[97]

Aun cuando aparece la referencia de una resolución, cabe destacar que, en los documentos sobre ciberseguridad presentados ante un órgano principal o subsidiario de las Naciones Unidas, sólo se encuentra ambiguamente señalado el aspecto de la ciberseguridad o ciberguerra. De manera textual se ubican en:

- El Sexto Examen de la Estrategia Global de las Naciones Unidas contra el Terrorismo A/RES/72/284.
- La Resolución del Consejo de Seguridad de la ONU 2341 (2017).
- La Resolución del Consejo de Seguridad de la ONU 2370 (2017).
- Texto del Consejo de Seguridad S/2015/939 (Principios rectores de Madrid).[98]

Los textos referidos, abordan el tema de la seguridad cibernética, a través del enfoque de combate al terrorismo, mismo que deriva de los acontecimientos de la caída de las Torres Gemelas en 2001, y que por supuesto se potencializa con las actividades de reclutamiento de miembros de grupos terroristas de Medio Oriente por medio de la red.

Específicamente, la actividad de Naciones Unidas y de su Consejo de Seguridad no gira en torno a la gran gama de áreas dentro de la cual el espacio cibernético ya

---

[96] AGNU, Resolución 68/243. *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, aprobada por la Asamblea General el 27 de diciembre de 2013 en el marco del 68° período de sesiones, publicado por Naciones Unidas el 9 de enero de 2014, A /RES/68/243.

[97] *Ibídem.*

[98] Organización de las Naciones Unidas; Consejo de Seguridad, *Resoluciones del Consejo de Seguridad de la ONU*. Naciones Unidas. Disponible en: https://www.un.org/securitycouncil/es/content/resolutions

influye de manera importante; deja de lado la consideración comercial, social, económica, estatal, y de infraestructura crítica que va más allá del ciberterrorismo.

Por otra parte, la multilateralidad no es un aspecto que destaque, lo que a su vez señala la necesidad de incluir no solo a los países que tengan un problema de ciberseguridad importante, sino a todos los demás; ya que el mundo cibernético no reconoce las fronteras políticas, espaciales o económicas.

El organismo especializado de Naciones Unidas que incorpora el tema cibernético es la Unión Internacional de Telecomunicaciones integrada en 1947 en el aparato de gestión de la ONU. Además, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) y el Grupo de Expertos en Ciberseguridad que nace en 2014, también atienden algunos aspectos relacionados con la ciberseguridad internacional.

El más reciente Índice de Ciberseguridad Global (ICG) publicado por la Unión Internacional de Telecomunicaciones (2020) muestra un compromiso creciente en todo el mundo para afrontar y reducir las amenazas a la ciberseguridad.

En aras de mejorar su ciberseguridad, distintos países están trabajando para enriquecerla a pesar de los desafíos de la pandemia por COVID-19, y el rápido cambio de las actividades cotidianas y de los servicios socioeconómicos hacia la esfera digital, como confirma el Índice de 2020. Según éste, alrededor de la mitad de los países a nivel mundial dicen haber formado un Equipo Nacional de Intervención en caso de Incidente Informático (EIII), lo que indica un aumento del 11% desde 2018.[99]

La rápida adopción de las tecnologías de la información y la comunicación (TIC) durante la pandemia de COVID-19 ha hecho de la ciberseguridad una prioridad; alrededor del 64% de los países considerados en el ICG, había adoptado una estrategia nacional de ciberseguridad (ENC) a finales de año, mientras que más del 70% llevó a cabo campañas de sensibilización a la ciberseguridad en 2020, en comparación con el 58% y el 66%, respectivamente, en 2018.[100]

Lo anterior evidencía un interés particular de cada Estado por mejorar su estatus de ciberseguridad y de prevención de ataques cibernéticos encaminados a la

[99] International Telecomunications Union, “Countries ramp up cybersecurity strategies”, Press Release ITU, 29 de junio de 2021. Disponible en: https://www.itu.int/en/mediacentre/Pages/pr06-2021-global-cybersecurity-index-fourth-edition.aspx

[100] Ciberseguridad Global, “*Expertos reportan una mejora en la ciberseguridad en el mundo”*, *El siglo de Torreón*, México, 30 de junio de 2021. Disponible en: https://www.elsiglodetorreon.com.mx/noticia/2021/expertos-reportan-una-mejora-en-la-ciberseguridad-en-el-mundo.html

ciberguerra; sin embargo, esto no exime la falta de la incorporación del tema a sus agendas particulares, y hacia las acciones encaminadas a la cooperación multilateral que se formalicen en acuerdos, tratados, convenciones etc., salvo algunas excepciones sobre las cuales se profundizará más adelante.

Julio Albert Ferrero, considera que "en general, las naciones de forma aislada no tienen capacidad técnica ni jurídica para enfrentarse a ciberataques masivos, por lo tanto, solo se puede abordar el problema desde la cooperación internacional"[101] .En este escenario debemos considerar que establecer una fuerte y contundente estrategia para salvaguardar la ciberseguridad, deberá observar la posición de hacerle frente de manera conjunta. No obstante, esto no es posible sin que las bases jurídicas, tecnológicas e institucionales particulares de cada Estado-Nación, en torno al uso y protección del ciberespacio, dejen de atenderse de manera determinante y específica. Tampoco exime de la responsabilidad nacional particular de delinear su agenda de seguridad/ciberseguridad, así como las estrategias que emanen de ella.

En este sentido, se sintetiza la idea acerca de atender de manera multilateral y alineada a los intereses nacionales de cada Estado, para fortalecer las acciones encaminadas a la securitización del ciberespacio y/o ante escenarios de ciberguerra, sin pasar por alto la inherente necesidad de atender dicha circunstancia a nivel interno para establecer bases sólidas individual y colectivamente (cuando convenga al equilibrio de fuerzas en el escenario internacional).

Actualmente la ciberseguridad y la atención a la amenaza de la ciberguerra se atienden de la forma que sugiere Ferrero, pero en organizaciones regionales, en grupos de países específicos, o entre aliados. Algunos ejemplos de cooperación respecto al tema en cuestión, que no forman parte de la ONU, o subsidiarias, son:

1) **La Organización del Tratado del Atlántico Norte (OTAN)**. En el año 2008 publicó un documento referido a su Política de Ciberdefensa para la protección de los sistemas de información y comunicaciones, la cual tuvo como propósitos: impulsar la integración de las ciberarmas en su Planeamiento de Defensa; impulsar el desarrollo del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN en Tallín, Estonia; y desarrollar el concepto de ciberdefensa de manera conjunta. También apoyó la creación de Equipos de

[101] Julio A. Ferrero, *"La ciberguerra. Génesis, y evolución",* Revista General de Marina, Madrid, España, Ministerio de Defensa, Vol. 264, enero-febrero 2013, p. 88.

Respuesta Inmediata (RRT) ante ciberataques, así como de la Autoridad para la Gestión de la Ciberdefensa. En 2010, se creó el Nuevo Concepto Estratégico bajo el cual se conduciría la OTAN, así como su Estrategia de Ciberseguridad; resalta la importancia de aumentar las capacidades de ciberdefensa. En marzo y junio de 2011 la OTAN aprobó respectivamente una Revisión de la Política de Ciberdefensa y un Plan de Acción de Ciberdefensa. A su vez, dicho Plan se centró en desarrollar normas en torno a la protección de la infraestructura crítica, de modo que se permitiera la implementación de nuevas estrategias de ciberdefensa a inicios del año 2013. La Política de Ciberdefensa especifíca las tareas de los Estados miembros, en su calidad de aliados, entre las que se encuentran: la defensa colectiva, la coordinación efectiva para la ciberdefensa desarrollando la capacidad de respuesta, la gestión de crisis, la protección garantizada de los sistemas de control crítico (CSI), tanto a nivel militar como civil, públicos y privados. Cabe aclarar, que a la OTAN la conforman 30 países, mismos que participan y ejecutan, en lo general y en lo particular, las acciones descritas con anterioridad, además si un integrante de la OTAN sufriera un ciberataque, éste podrá solicitar ayuda a la Alianza, ya que la organización proporciona ayuda a los aliados que sean atacados, según los principios rectores que la conforman.[102]

2) **La Unión Europea (UE).** Por su parte la UE, como primer paso, estableció el Concepto de Operaciones en Red de manera conjunta con la creación de la Agencia Europea de Defensa (EDA). Su objetivo, obtener superioridad en el manejo y control de la información buscando, como resultado, poder denegar la información y obtener una ventaja ante el enemigo para interrumpir, inutilizar, degradar o engañar los sistemas de mando y control, y anulando la capacidad del contrario para una toma de decisiones eficiente (La concepción que realiza aquí la UE, corresponde a algunos de los rasgos característicos de la Primera Generación de la Ciberguerra mencionada con anterioridad).

   Desde los primeros años del siglo actual, la UE fundó su propia agencia de ciberseguridad, la Agencia Europea de Seguridad de las Redes y de la

[102] Maria José Caro, *"Nuevo concepto de ciberdefernsa de la OTAN"*, Documento informativo del IEEE 09/2011, Instituto Español de Estudios Estratégicos, Ministerio de la Defensa, marzo 2011. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7271583

Información (ENISA), fue creada en 2004 y es totalmente operativa desde el 1 de septiembre de 2005.

Con el objetivo de atender de forma específica las demandas y amenazas en el ciberespacio, se elaboró, el Reglamento sobre la Ciberseguridad de la UE, que contribuye a mejorar la fiabilidad de los productos, servicios y procesos de las TIC mediante programas de certificación de ciberseguridad. Asimismo, se buscó la cooperación con los Estados miembros y con los organismos de la UE. Con esta serie de acuerdos, los países europeos se prepararon para los desafíos del mañana mediante el intercambio de conocimientos, la creación de capacidades y la sensibilización, además de adoptar sanciones en represalia por ataques.

En el año 2016 los ministros de justicia del Consejo de la UE acordaron mejorar la justicia penal en el ciberespacio, así como la implementación de distintas prácticas para mejorar la cooperación en aras de la lucha contra los ciberataques y ciberdelincuentes, a lo cual se le dio seguimiento durante 2017.

Además, la UE adopta medidas sobre actividades malintencionadas en las que resalta la importancia de un ciberespacio mundial, abierto, libre y seguro que vaya de la mano con el ejercicio de los derechos humanos, libertades fundamentales y el Estado de Derecho.

Para 2018 se aprueba el Reglamento sobre la Ciberseguridad en la Unión Europea, lo que permite que se introduzca una certificación sobre la ciberseguridad instalada en los dispositivos conectados a internet en toda Europa, y consolidando una agencia permanente en materia cibernética.

Un elemento clave se suscita en 2019 cuando el Consejo adquiere la facultad de imponer sanciones ante ciberataques, así como medidas restrictivas para impedir los mismos si representan una amenaza potencial para la UE o sus miembros. Desde entonces, de forma constante, existen reuniones de actualización y promoción de la ciberseguridad y ciberdefensa, donde se tratan temas sobre la red 5G, reglamentos, lucha contra la desinformación, ciberguerra, refuerzo de la unidad cibernética conjunta, etc.[103]

[103] Consejo Europeo, *"Ciberseguridad: cómo combate la UE las amenazas cibernéticas"*, Consejo de la Unión Europea. Consejo Europeo, abril 2022. Disponible en: https://www.consilium.europa.eu/es/policies/cybersecurity/

3) **La Organización de los Estados Americanos (OEA).** Con su programa de ciberseguridad, ayuda a sus 35 Estados miembros en el desarrollo de capacidades a nivel técnico cobre ciberseguridad y políticas públicas, garantiza un ciberespacio seguro, abierto y resistente. El programa vigila el desarrollo de dichas políticas, así como de la creación de capacidades conjuntas de respuesta a incidentes de seguridad informática, brinda asistencia técnica personalizada, además de ofrecer capacitación a las instituciones y organizaciones nacionales.

   En suma, la investigación y la divulgación sobre el tema cibernético es constante; orienta al personal de operación de infraestructura, a organizaciones privadas y a la sociedad civil en torno a los desafíos de ciberseguridad en América Latina y el Caribe, con el fin de que sean capaces de identificar la problemática, los riesgos y amenazas a los cuales se ven expuestos.

4) **El G7.** Los países del G7 (Estados Unidos, Japón, Alemania, Reino Unido, Francia, Italia y Canadá) han adoptado un marco común que se concentra en la protección del sistema financiero ante los ciberataques contra entidades e instituciones nacionales; este marco adoptado en 2016 destaca la importancia de mantener de manera eficaz el intercambio de información, lo cual amerita la revisión de las estrategias de ciberseguridad de los Estados miembros a nivel nacional para identificar deficiencias que puedan ponerlos en riesgo.[104]

5) **La Unión Africana (UA).** En primera instancia, la UA aprobó el Convenio sobre Ciberseguridad y Protección de Datos Personales en junio de 2014 como un primer acercamiento para atender la seguridad del ciberespacio de los 55 países miembros que la conforman. Para el año 2015, en la XXIV Cumbre de la Unión Africana para debatir su agenda 2063, se reconoce el concepto de "Sociedad de la información", con ello cobra importancia el tema ciberespacial como miembros de una comunidad tecnológica internacional; además, aborda muchas cuestiones relacionadas con el aumento del uso de las TIC en África. Asimismo, se establece un marco jurídico estándar para la realización del

[104] LA VARGUARDÍA, "*El G7 adopta un marco común para prevenir ciberataques al sector financiero",* LA VANGUARDÍA*,* Sección Economía, G7 Finanzas, Barcelona, España, 12 octubre 2016. Disponible en: https://www.lavanguardia.com/politica/20161012/41937750211/el-g7-adopta-un-marco-comun-para-prevenir-ciberataques-al-sector-financiero.html

comercio electrónico, la protección de los datos personales, la promoción de la ciberseguridad y el tratamiento de la delincuencia cibernética. Es imperativo señalar que dicha Convención ha sido criticada acuciantemente por los propios Estados miembros debido a las restricciones y vacíos existentes, así como por transgredir libertades básicas o de acceso a la información, y ampliar el poder gubernamental. No obstante, se incluye como ejemplo de cooperación ya que, si bien existen muchos aspectos para que su aplicación tenga efectos aún más provechosos y beneficiosos, sienta un precedente en la atención hacia los temas de ciberseguridad y ciberdefensa de manera conjunta en la región africana.[105]

La ciberguerra y la ciberseguridad como factores relevantes en las dinámicas de conflicto representan un reto que de manera individual debe ser atendido en las normas, reglamentos, estrategias y agendas nacionales de cada Estado. Cada país desarrolla, conforme su capacidad e intereses nacionales, diversos métodos para atender (o no) las amenazas que se gestan en el ciberespacio. No obstante, es de manera conjunta que se manifiesta un mayor margen de acción respecto al tema.

Ejemplo de lo anterior y de lo que considera Ferrero, es el Convenio sobre la Ciberseguridad, mejor conocido como el Convenio de Budapest[106]. Este Convenio forma parte de la serie de Tratados Europeos (No.185) del Consejo de Europa: celebrado en Budapest el 23 de noviembre de 2001; es el único antecedente de cooperación internacional respecto al tema de la seguridad cibernética, recalcando que es por parte de la región europea, de forma global, aún no existe un acuerdo o iniciativa que involucre, sino a toda, a la gran mayoría de la comunidad internacional.

Aun cuando se han presentado algunas organizaciones internacionales que atienden la problemática, es fundamental que, de manera particular e interna, se trabaje en la ciberseguridad para atender la ciberguerra como una amenaza constante dentro del conflicto internacional en el siglo XXI. Abordarla (o no) dentro de los foros y debates internacionales, y de forma ocasional, no es suficiente ante la creciente y

[105] International, *Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales,* LAWi, 20 de abril de 2018. Disponible en: https://leyderecho.org/convencion-de-la-union-africana-sobre-ciberseguridad-y-proteccion-de-datos-personales/

[106] Council of Europe, *"Convenio sobre la ciberdelincuencia", Serie de Tratados europeos.* Budapest, núm. 185, 23 de noviembre 2001. Disponible en: https://www.oas.org/en/sla/dil/treaties_agreements.asp
https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

cada vez más compleja exigencia tecnológica que brinda beneficios, pero también riesgos a nivel mundial, nacional, local e individual.

El significado de la presencia de la ciberguerra en el conflicto internacional se observa en la apertura de una amplia variedad de posibilidades. Actualmente las tres generaciones de la ciberguerra no solo son etapas que fueron surgiendo para explicar la coyuntura tecnológica y bélica del contexto bajo el que se suscita, sino que en suma las tres forman parte de la dinámica, riesgo, y amenaza tecnológica perfeccionada, que desemboca en las amenazas cibernéticas actuales. La guerra cibernética como un elemento cada vez más común en diversos escenarios de disuasión o tensión internacional, incorpora el control psicológico, el control de la infraestructura crítica y el control de armamento de los Estados ¿Por qué? Porque la fase en la que ésta se encuentra actualmente es la de "implementación", lo cual podría presentarse como la cuarta generación o bien, como resultado de la evolución de las tres generaciones anteriormente descritas. Sin embargo, es una táctica que evoluciona de manera silenciosa y a la cual no se le atiende con la relevancia que ha demostrado tener, aún antes de la temporalidad que delimita la presente investigación y que se consolidará con más fuerza a corto plazo ya que dentro de los momentos de tensión política y de conflicto, la herramienta cibernética para vulnearar toma un papel condicionante para el resultado final en el que desemboque una confrontación.

Un fenómeno conocido como la ciber-cinética, es decir, los efectos físicos, en el "mundo real", que puede tener una operación o ataque cibernético enmarca hoy en día el debate. La ciber-cinética se define como una clase de ataque cibernético que puede causar daño físico, directa o indirectamente, que puede provocar lesiones e incluso la muerte exclusivamente a través de la explotación de sistemas de información y procesos vulnerables[107], de ahí la importancia de tomar en cuenta la relevancia de los ciberataques en un escenario bélico. En los apartados anteriores se ahondó en las características de los ciberataques, así como de las consecuencias que su implementación tiene, se mostró cómo la consideración estatal, por la existencia y aplicación de ciberataques en la ciberguerra, debe ser formar parte de la conciencia de la comunidad internacional y de cómo se atiende desde la política nacional e internacional.

[107] Scott D. Applegate, *The Dawn of Kinetic Cyber*. 5th International Conference on Cyber Conflict, Tallin, Estonia, Publicaciones del CCD COE de la OTAN, 2013, p 5.

La importancia que va obteniendo la revisión de las agendas de ciberseguridad, a nivel nacional y en los planes de trabajo de los organismos internacionales, es un campo que exige reparar en las consecuencias de no considerar la ciberguerra como un escenario de amenaza cada vez más presente en la dinámica internacional. Si bien se ha retomado el tema de forma conjunta por parte de diversos organismos, su atención individual y activa se convierte en una exigencia de constante atención y actualización para la preservación estatal en general.

2.3 Implicaciones de las dinámicas sociales a partir del establecimiento de la ciberguerra en las Agendas de Seguridad Nacional y en las Agendas de Ciberseguridad.

Al pensar las consecuencias de la ciberguerra respecto al robo de datos de gran importancia a nivel estatal y político, del daño a la infraestructura crítica y sobre todo el control de armamento, es esencial, para evidenciar las afectaciones de ello a la sociedad civil.

Las consecuencias directas, ya sean positivas o negativas, de que se considere la ciberguerra dentro de las Agendas de Seguridad Nacional y Ciberseguridad respectivamente, así como el reconocimiento de la relevancia para atenderlas dentro de las prioridades de éstas, recaen en el sector civil.

Lo escrito anteriormente, conduce a analizar cómo afecta la ciberguerra al sector civil, además de las implicaciones que tiene en sus dinámicas de vida, y cómo el que esta temática tenga lugar en la agenda política nacional e internacional, influye en que se alteren dichas dinámicas.

A nivel mundial, se ha hecho cada vez más frecuente el reporte de distintos ciber-incidentes que involucran, como víctimas o supuestos perpetradores, a Estados, grandes empresas, y otros actores no estatales (grupos de hackers, ciber-activistas o hacktivistas, grupos terroristas, ciber-delincuentes, ex agentes de inteligencia que develan secretos a nivel público [*whistleblowers*], organizaciones de la sociedad civil), etc. Todo apunta a nuevas amenazas en el ciberespacio que ponen en riesgo la seguridad en las sociedades contemporáneas y a sus dinámicas cotidianas.

Se han mencionado en apartados anteriores, ciberataques relevantes a nivel Estatal. Más allá de redundar en dichos sucesos, es importante rescatar cuáles han sido los efectos a nivel civil en los que existe una correspondencia entre cada ciberataque dentro de un conflicto interestatal.

Cuando un virus, *malware*, gusano informático, etc., se introduce en los sistemas gubernamentales o empresas privadas, puede perjudicar los sistemas de individuos particulares o sociedad civil en general; ya que, en la búsqueda por obtener datos o información relevante, el ciberataque puede tener un alcance que no distingue entre los dispositivos que ataca.

En otras palabras, ya sea que cada ciberataque esté programado para dañar algún sector o sistema en específico, o no, las consecuencias se ven reflejadas de forma inmediata o paulatina, en el sector civil y entre particulares.

Con base en lo anterior, es que logran identificarse patrones de ataque y áreas contra las que arremeten los ciberataques. En este sentido, se presenta una tabla con las mencionadas áreas de ataque para que, de acuerdo con algunos de los ciberataques más conocidos en los últimos años, se pretende poder identificar las afectaciones en el plano civil. La información presentada es producto del análisis de diferentes noticias, reportajes, notas periodísticas y videos informativos respecto a lo que se suscitó en cada evento.

En la siguiente tabla se pretende ilustrar cómo los ciberataques, con sus respectivas características de naturaleza técnica (*malware,* virus, troyano, gusano DDoS, etc.) y contextual, infringen afectaciones a la esfera civil en al menos uno de los daños que sugiere la categorización propuesta.

Tabla 5. Eventos históricos relevantes de ciberguerra/ciberataques

Daño ocasionado / Evento	Robo de información (*Phishing*)	Negación de servicios públicos	Inhabilitar/ Robo de cuentas equipos informáticas	Pérdida material de la propiedad	Pérdida de dinero/ capital
Estonia 2007[108]	✗	✓	✓	✗	✓
Stuxnet 2010[109]	✓	✗	✗	✓	✗
BlackEnergy Ucrania 2015[110]	✓	✓	✗	✗	✗
PETYA 2016[111]	✓	✓	✓	✓	✓
WannaCry 2017[112]	✓	✓	✓	✗	✓

Elaboración propia a partir de: **John Snow**, *"Top 5 de los ciberataques más memorables".* Kaspersky, noviembre 2018. Disponible en: https://goo.su/LRZF42

[108] Estonia 2007: Estonia también fue blanco de enormes ciberataques que en algunos casos duraron semanas. Las páginas web de bancos, medios de prensa y organismos gubernamentales colapsaron debido a niveles sin precedente de tráfico en internet. Redes de robots informáticos -conocidos como *botnets*- enviaron cantidades masivas de mensajes basura (spam) y pedidos automáticos online para saturar los servidores. El resultado fue que los estonios se quedaron sin poder usar cajeros automáticos y servicios de bancos online. Los empleados estatales no pudieron comunicarse por correo electrónico, además de que los diarios y medios de comunicación se encontraron de golpe con que no podían transmitir las noticias. El gobierno ruso fue señalado directamente de la autoría de este ciberataque. (John Snow, *"Top 5 de los ciberataques más memorables".* Kaspersky, noviembre 2018. Disponible en: https://goo.su/LRZF42)

[109] Stuxnet 2010: El gusano era capaz de expandirse en oculto a través de memorias USB y penetrar incluso en computadoras que no estuvieran conectados a Internet o a una red local. El objetivo del *malware* fueron las infraestructuras críticas y entornos industriales en Irán, como centrales nucleares o plantas de energía; inutiliza las centrifugadoras de enriquecimiento de uranio en Irán, ralentizando varios años el programa nuclear del país. El virus Stuxnet se instalaba en los sistemas, robaba su información y más tarde les ordenaba que se autodestruyeran. Se señaló como posible responsable al gobierno de Estados Unidos por este ataque. (John Snow, *"Top 5 de los ciberataques más memorables".* Kaspersky, noviembre 2018. Disponible en: https://goo.su/LRZF42)

[110] Black energy. Ucrania 2015: Se suscita un apagón eléctrico generalizado en Ucrania. El ciberataque eliminó más de 60 centrales eléctricas en todas las regiones ucranianas, lo que causó incomunicación entre la población y entre instituciones, no hubo calefacción, considerando que era época invernal en el país. Se señaló como responsable al gobierno ruso de dicho ataque. (John Snow, *"Top 5 de los ciberataques más memorables".* Kaspersky, noviembre 2018. Disponible en: https://goo.su/LRZF42)

[111] Petya 2016: Este gusano cibernético se movía por la red, cifrando de forma irreversible todo lo que encontraba. El objetivo principal de la epidemia NotPetya eran las empresas. El daño del ciberataque se estima en 10,000 millones de dólares por lo cual se considera el ciberataque más costoso de la historia. Algunas empresas presentaron daños y consecuencias a servicios como aerolíneas, puertos marítimos, cajeros automáticos, lectores de tarjetas de transporte público, así como bancos, empresas e instituciones gubernamentales. Se pedía una cantidad de 300 dólares en bitcoins para devolver la información y el control de los sistemas. (John Snow, *"Top 5 de los ciberataques más memorables".* Kaspersky, noviembre 2018. Disponible en: https://goo.su/LRZF42)

[112] WannaCry 2017: Ordenadores en todo el mundo vieron afectados sus sistemas, se encriptaron sus archivos y se bloquearon los accesos de administrador a sus usuarios. WannaCry consiguió inutilizar más de 200,000 computadoras en 150 países, entre ellos infraestructuras críticas. En algunos hospitales, WannaCry cifró todos los dispositivos, incluido el equipo médico, y algunas fábricas se vieron obligadas a detener su producción. (John Snow, *"Top 5 de los ciberataques más memorables".* Kaspersky, noviembre 2018. Disponible en: https://goo.su/LRZF42)

Como se puede apreciar, la relevancia de atender los temas de ciberseguridad de manera inmediata evitará a corto o mediano plazo, repercusiones sociales, económicas, culturales, que afectan no solo a las grandes estructuras de un país, sino también a sectores civiles en estado de vulnerabilidad.

Por otro lado, securitizar desde los primeros círculos sociales de un país, asegura desde su base, la seguridad ciberespacial, y con ello el sustento del resto de la estructura del Estado-Nación, si se lograra comprender que la ciberseguridad comienza por preservar el bienestar de la sociedad civil en dicho espacio, se reducirían significativamente los espacios y posibilidades para que se vulnere cibernéticamente el resto de los pilares estatales. Es decir, la cultura de la prevención, así como las buenas prácticas en la internet.

No se puede, ni deben ignorarse las implicaciones que los ciberataques y la ciberguerra tienen para la sociedad. Si bien cuando se han suscitado, muchos usuarios incorporan mejores prácticas en el uso del ciberespacio, y los Estados prestan atención a la seguridad cibernética, las medidas precautorias deberían estar presentes y ser tomadas en cuenta comprometidamente antes de que un ciberataque desestabilice la dinámica cotidiana; incorporar una cultura en el uso del ciberespacio para la sociedad y priorizar la ciberseguridad en la Agenda de Seguridad Nacional son solo algunos ejemplos de la cooperación a gran escala. Cada Estado debe atender de manera interna y a todos los niveles la ciberseguridad, que sustenta actualmente muchas de las más importantes áreas de estabilidad y valor para los países. Así lo señala **Mariano J. Ferrero** en su texto *La ciberguerra en el marco de la preocupación por la seguridad internacional en las sociedades hiperconectadas contemporáneas*, tal y como se puede apreciar a continuación:

> Se ha señalado que una parte significativa de los problemas de seguridad en el ciberespacio obedece a la escasa atención que se había prestado en este ámbito a las consideraciones de seguridad. En este sentido, expertos han considerado que la 'despreocupación digital' es, todavía, el mayor problema ya que un gran número de computadores de empresas, e incluso de sitios de control de infraestructura crítica, están conectados a Internet sin la suficiente protección.[113]

Tal es el caso de Estonia; después del ciberataque presuntamente orquestado por el gobierno ruso en 2007; el cual perjudicó considerablemente la infraestructura

[113] Mariano Ferrero, *"La ciberguerra en el marco de la preocupación por la seguridad internacional en las sociedades hiperconectadas contemporáneas",* Serie Estudios, Chile, Biblioteca del Congreso Nacional de Chile, marzo 2015, núm., 02-15, p. 7.

crítica, el gobierno trabajó en conjunto con la sociedad civil para mejorar la ciberseguridad nacional (es así que lo incluye dentro de sus prioridades nacionales), prestando atención a la protección cibernética en todos los niveles estructurales del Estado. En suma, lo anterior paulatinamente llevaría a Estonia a tener un gran avance tecnológico y a posicionarse como uno de los líderes en materia de ciberseguridad global.

Atender la ciberseguridad, es atenderla a todos los niveles, pues solo así los Estados podrán preservar su seguridad y ciberseguridad de forma más completa. Los casos expuestos, son ejemplo de que los ciberataques aislados o bajo la lógica de la ciberguerra, pueden tener lugar a partir de distintos dispositivos, los cuáles pueden corresponder a alguna institución gubernamental del Estado, a un sistema computacional privado de alguna empresa, o bien a una computadora, correo, etc de una persona miembro de la sociedad civil.

Conclusiones del capítulo.

Hablar de la cibersecuritización de las agendas nacionales e internacionales, no es un tema que deba seguir considerándose de forma aislada. Atender la ciberseguridad es atender la seguridad nacional en toda su extensión, pues debido al contexto tecnológico en el que se encuentra la sociedad ha sido imperativo que la realidad y la información se hayan extendido al quito dominio, lo que a su vez ha generado que, en el caso del cifrado de datos, claves, información, etc., existan nuevos canales para ser vulneradas.

La economía, la infraestructura, los transportes, los hidrocarburos, los servicios de salud, entre muchos otros pilares que sostienen la dinámica de cualquier Estado, deben observarse y protegerse desde el ámbito cibernético para poder asegurar conjuntamente el buen funcionamiento y seguridad del área que atiende cada uno de ellos.

El objetivo de haber hecho un recorrido por las agendas de seguridad nacional de dieciocho países distintos, pertenecientes a contextos y latitudes contrastantes, permitió exponer las diferentes prioridades y tópicos que nutren cada estrategia de seguridad en lo que consideran fundamental para la preservación del país y su dinámica. Además, esta panorámica facilitó reconocer la importancia que global y

particularmente se le da a la seguridad cibernética, lo que directamente se refleja en diversos estudios, índices y rankings mundiales al respecto.

Asimismo, aquellos países que consideraron dentro de sus prioridades de seguridad nacional temas asociados con la ciberseguridad y la ciberguerra podrían haber sido menos vulnerables durante los años en que las amenazas globales que expone el Foro Económico Mundial tuvieron ataques cibernéticos (2007-2020), así, mientras aquellos que no las consideraron, estuvieron en riesgo o llegaron a sufrir algún daño al no tener cubiertas las áreas de ciberseguridad de forma particular.

Se debe puntualizar que, dentro del análisis de las agendas y estrategias, (específicamente en la Tabla 2) se hace una segunda revisión respecto a si los dieciocho países, tienen una estrategia de ciberseguridad en específico. Aunque la gran mayoría de los países seleccionados, sí tienen una estrategia de ciberseguridad, no es un tema que en todos los casos esté presente en la Agenda de Seguridad Nacional principal, y además, de tener un documento que atienda la seguridad cibernética específicamente, tendría que someterse a evaluación para determinar la calidad, funcionalidad, utilidad y capacidad de cada una ya que, a consideración de esta autora, tener una estrategia de ciberseguridad, muchas veces no es sinónimo de eficacia.

En lo que respecta a la evolución de la ciberguerra en el escenario internacional y su relevancia en las dinámicas de conflicto, en definitiva, la génesis de la ciberguerra no puede ser definida imperativamente a partir de en un evento o fecha específica, sino que se ha ido nutriendo y transformado conforme el desarrollo tecnológico, histórico, y social que la enmarca. Las etapas propuestas por Andrés Gaitán, no sólo permiten identificar históricamente la cronología de la ciberguerra, sino también ubicar los factores humanos que la perfeccionaron y llevaron a cabo; haciendo hincapié en aspectos psicológicos implicados en la práctica de los ciberataques, con lo que afirma que las tecnologías y su uso se encuentran íntimamente relacionados con los aspectos sociales, además de tener un alcance que involucra el control de armamento y situaciones bélicas más concretas. En este sentido, se invita a la reflexión en torno a si actualmente formamos parte de la tercera generación de la ciberguerra que plantea Gaitán, o si ya pudiéramos comenzar a definir una cuarta generación que no segmente las generaciones anteriores, sino que dado el momento evolutivo tecnológico, pueda retomarlas en su conjunto para implementarlas en una cuarta etapa de aplicación.

Como contrapartida a la evidente evolución de la ciberguerra, concluir que la atención internacional en, al menos, las últimas dos décadas no ha sido la más contundente, es un llamado a que se incorporen políticas tanto individuales como colectivas para llenar los vacíos que abren la posibilidad de vulnerar los sistemas de seguridad internacionales.

Al tomar en cuenta que las consecuencias tienen lugar a niveles macro y micro, de manera piramidal, y piramidal invertida, nos permite hablar sobre políticas públicas para la ciberseguridad, y condiciona su interconexión con el sector público, privado, gubernamental y civil. Por tal motivo a nivel regional y global, la cooperación en materia de seguridad en el quinto dominio puede seguir su curso multilateral, como algunos actores han optado por hacer.

Es importante que la comunidad internacional y los miembros de dichos acuerdos, tratados etc., mantenga el ejercicio colaborativo, a través de la firma y ratificación de estos, además de dar seguimiento y actualización a los acuerdos establecidos por las implicaciones del desarrollo tecnológico en el entorno actual y su rápido avance. Aunque es poco realista la perspectiva de pactar significativas normas vinculantes a escala global, la ciberdiplomacia sigue siendo un factor importante e influyente dentro de un ámbito en constante evolución y con diversidad de facetas, donde esa herramienta no puede, ni debe, ser descartada al tratar los temas que emanan del ciberespacio, su administración, agendas, o eventos que se susciten en él.

Finalmente, en un análisis que lleva por sí mismo la mirada hacía las altas esferas políticas, es menester considerar el impacto de la toma de decisiones y administración en otros niveles como lo es el sector civil. Reconocer la importancia de ejercer de forma total estrategias que involucren todos los sectores de un país en pro de la preservación de la seguridad y ciberseguridad nacional, permitirá proteger desde los escenarios más básicos la integridad nacional y generar protección desde los mismos.

3. Conformación de las agendas de ciberseguridad de Rusia y Estados Unidos.

El presente capítulo tiene el objetivo de exponer la relación cibernética entre Rusia y Estados Unidos como un caso de estudio, no únicamente relevante por los antecedentes históricos que la relación de ambos países ha marcado la política internacional, sino por la importancia que ambos han tenido dentro de la dinámica social que ahora se encuentra en una coyuntura tecnológica.

Los capítulos anteriores han resaltado la importancia y la amenaza que representa el ciberespacio dentro de dinámicas conflictivas, así como las características de la ciberguerra y sus elementos fundamentales. Además, se analizó a profundidad la imperativa necesidad de atender la ciberseguridad dentro de la planeación y estructuración de la seguridad nacional de las naciones. En suma, finalmente todos los elementos anteriormente expuestos, pretenden ser desembocados en la relación que tanto Rusia como Estados Unidos tienen individualmente en su desenvolvimiento en el ciberespacio y con la ciberseguridad interna, pero también cómo se han desenvuelto entre ellos bajo la premisa de “eternos contrincantes”, portadores de dos de las ideologías políticas más influyentes del siglo XX y XXI, y por supuesto, como sujetos hegemónicos mundiales.

A través del ejercicio de estudiar y comparar las agendas de ciberseguridad rusa y la estadounidense respectivamente, se sostiene que este terreno se ha convertido en un imperativo de seguridad nacional para ambos países, y a su vez, permitirá reconocer y diferenciar los conceptos, estrategias, visión y defensa respecto al ciberespacio. Lo anterior, es con el objetivo de responder a la hipótesis rectora del presente trabajo de investigación, específicamente a la premisa de cómo la tensión entre Rusia y Estados Unidos, no se detuvieron o apaciguaron después de la Guerra Fría, sino que se proyecta en distintos espacios y escenarios como lo es el cibernético. A través de evidencias documentales se tratará de fortalecer la premisa y así entender la relación cibernética entre ambos Estados.

3.1 Estructura de la ciberdefensa en Rusia y Estados Unidos.

La ciberdefensa y ciberseguridad se han convertido en áreas claves para los países casi de manera obligatoria por el desarrollo tecnológico, además de que el fenómeno migratorio de la información al quinto dominio es casi inevitable dada la interconexión que se oferta a través de la red. Su desarrollo actual coincide con el advenimiento de la sociedad de la información, las redes intercomputacionales, e Internet, cuya expansión ha configurado el más reciente espacio para la guerra moderna y ha afectado sensiblemente la vida cotidiana de los diversos actores en el mundo globalizado a distintos niveles. Es así como su estudio se convierte en una tarea obligada para la conducción político-estratégica de la defensa de las naciones, es un asunto de soberanía y seguridad, que influye en la gobernanza nacional.

Para darle sustento a la seguridad nacional en general, cada país estructura las instituciones de seguridad y defensa apegadas a: los intereses particulares, objetivos y, aún más, a partir del contexto del cual forman parte; se retoman aspectos sociales, económicos, comerciales, e incluso geográficos que definen tanto los tópicos centrales del plan de desarrollo que cada Estado y su agenda de trabajo, como de igual manera lo hace con el área encargada de la seguridad.

> Una estrategia nacional de ciberseguridad, y seguridad, describe una visión de la situación y articula prioridades, principios y enfoques para comprender y gestionar los riesgos. Las prioridades para las estrategias nacionales en torno al tema variarán según el país, pero todas son importantes. En algunas naciones, el enfoque puede estar en proteger los riesgos críticos de la infraestructura, mientras que otros países pueden interesarse en resguardar los datos e información relacionados a la propiedad intelectual, y aún otros pueden dedicarse a mejorar la conciencia de los ciudadanos.[114]

Delinear la estructura de ciberdefensa, no es tarea fácil para los países, puesto que se traslada al quinto dominio prácticamente toda la información y funcionamiento de áreas e instituciones en materia económica, social, de educación, energéticos, etc. En otras palabras, el diseño de la ciberseguridad y ciberdefensa debe corresponder a salvaguardar todo lo que sustenta al Estado, pero en un nuevo espacio donde las fronteras no son del todo definidas, así como sus actores, riesgos y alcances.

---

[114] Andrea Rizzi: *"¿Quién tiene más ciberpoder? Una radiografía de las capacidades de EE UU, China, Rusia y otras potencias"*, El País, Sección "Internacional", enero 2022. Disponible en: https://elpais.com/internacional/2022-01-30/quien-tiene-mas-ciberpoder-una-radiografia-de-las-capacidades-de-ee-uu-china-rusia-y-otras-potencias.html

Rusia y Estados Unidos han desarrollado la ciberdefensa a partir de la necesidad global que surge y evoluciona con la tecnología, así como por la relevancia en el impacto de la seguridad interna de cada uno en el mundo. Hablar de la ciberseguridad de uno, es imperativo para entender la ciberseguridad del otro. Históricamente ambos actores han sido un referente en la comprensión de la configuración de la seguridad de Occidente y Oriente; la confrontación derivada en la Guerra Fría es un acontecimiento que constantemente se retoma para comprender el dinamismo de la relación que mantienen, y en la documentación que se hará en el presente capítulo, no será una excepción. Estudiar la conformación de las Agendas de ciberseguridad de Rusia y Estados Unidos, podría brindar una panorámica importante respecto a la evolución de cada Estado en el perfeccionamiento de su seguridad y, al mismo tiempo, para abrir una puerta importante para la reflexión de lo que en siglo XXI y el desarrollo del ciberespacio como un lugar que facilita la mutación del conflicto internacional, ha significado para el caso ruso-estadounidense.

3.1.1 La agenda rusa de ciberseguridad.

Antes de abordar la agenda de ciberseguridad de Rusia, se presentarán a continuación algunos datos básicos de carácter contextual para ubicar al lector en la dinámica de la Federación de Rusia.

Figura 8. Datos básicos de la Federación de Rusia

Fuente: Elaboración propia con base en el texto: *Rusia. Federación de Rusia*, Ministerio de Asuntos Exteriores. Unión Europea y Cooperación, Oficina de Información Diplomática, abril 2021, p.20.

Rusia como la conocemos hoy en día es el resultado de una serie de procesos político-sociales muy fuertes. Después de la caída de la URSS (1991), el país tuvo que rearticular su administración pública y orden gubernamental; pasó de ser una nación de corte federal y con un sistema marxista-leninista, a una República Federal Presidencialista. Boris Yeltzin, primer presidente de la Federación afrontó los primeros altibajos en la transición económica del país con la liberalización de la economía, la reforma industrial, así como comercial. "Rusia nunca había sido un Estado nación en el sentido que le damos a este concepto en Occidente. Rusia había sido un imperio, pero nunca había sido un Estado nación".[115]

[115] Mira Milosevich, en S/A, *Cómo Putin logró restaurar el estatus de Rusia como potencia global tras el colapso de la URSS hace 30 años*, BBC News, Mundo, diciembre 2021. Disponible en: https://www.bbc.com/mundo/noticias-internacional-59671737

Sin embargo, para efectos útiles de este trabajo de investigación, se retoma la Reforma Constitucional Rusa de 1994, que con la administración de Vladimir Putin promulgada el 31 de diciembre de 1999, proyecta con mayor firmeza una serie de cambios en las instituciones de la Federación.

Desde la reforma constitucional, el presidente puede nombrar a diversos ministros encargados de la seguridad nacional, de defensa y de la implementación de la ley, básicamente fueron; Defensa, Asuntos Exteriores, Justicia, Interior y Situaciones de Emergencia para designar a estos funcionarios, consultó al Consejo de la Federación, así como a los jefes de las estructuras de seguridad. Bajo este contexto, se sectorizó la administración de las principales esferas de sustento y desarrollo nacional; agricultura, economía, energéticos, etc., y sin lugar a duda, a las instituciones encargadas de la seguridad nacional.

Delinear los contornos de la visión de rusa sobre la guerra es fundamental para comprender su estrategia cibernética ya que la percepción sobre la ciberseguridad está anidada en la comprensión de la evolución de Rusia sobre la naturaleza de la guerra y está moldeada por su concepto de “guerra de la información” [116]*.

En el sector gubernamental y militar de los rusos, hablar sobre el tema de la ciberseguridad es sinónimo de una noción occidental, ya que para ellos el término correcto es “seguridad de la información” (*information naya bezopasnost*), lo que es relativo y forma parte de la “guerra de la información”, esta última comprendida como:

> […] la confrontación entre dos o más Estados en el espacio de la información con el propósito de infligir daño a los sistemas, procesos y recursos de información, estructuras críticas y de otro tipo, socavando los sistemas políticos, económicos y sociales, una manipulación psicológica masiva de la población para desestabilizar al Estado y la sociedad, así como coaccionar al Estado para que tome decisiones en beneficio de la fuerza contraria.[117]

La definición anterior identifica dos elementos importantes de la guerra de la información: el elemento técnico de la infraestructura de la información que combina “herramientas técnicas y sistemas de formación, creación, transformación, transmisión, uso y almacenamiento de información" (correspondientes a cuestiones

[116] *La literatura y la doctrina militar de Rusia utilizan tres términos que pueden traducirse aproximadamente como “guerra de información”. Estos *son informazione protivoborstvo* (lucha de información o confrontación de información), *informatsionnaya voina* (guerra de información) e *informatsionnaya borba* (pelea de información). Explicar los matices de cada término está más allá del alcance de este documento y, para los fines de esta investigación, utilizaremos la traducción "guerra de información". Véase también Giles 2016, pág. 6, nota al pie 8.

[117] Ministerio de Política Exterior de la Federación Rusa: Doctrina de Seguridad de la Información, Presidente de la Federación Rusa, 2000.

relativas a la información y ciberseguridad en Occidente), y el componente psicológico de la guerra de información, que implica influir cognitivamente en la población y en los tomadores de decisiones del Estado contrario para erosionar su voluntad de lucha y sus estructuras y procesos de toma de decisiones".[118] El segundo elemento, incluso, hace referencia a una de las etapas de la ciberguerra que Andrés Gaitán señalaba como "Primera Generación de la Ciberguerra" que incluía los factores psicológicos y de toma de decisiones. (Véase: Capítulo, apartado 2.2).

Los documentos sobre el Concepto de Política Exterior, la Estrategia de Seguridad Nacional y la Doctrina Militar, de acuerdo con **Andrew Monaghan**, son esenciales para analizar la Política Nacional de Seguridad rusa, siendo así que la Estrategia de Seguridad Nacional muestra el posicionamiento ruso frente a las amenazas y los peligros que afectan al Estado. Ambos documentos pretenden garantizar la independencia, soberanía, integridad territorial y estabilidad del Estado, mediante mecanismos económicos, políticos, sociales y militares; es decir, son una declaración de las intenciones de los intereses nacionales rusos.

Las acciones anteriores, son coordinadas principalmente por el Ministerio de Defensa, el Ministerio del Interior y el Ministerio de Asuntos Exteriores, así como por el Servicio Federal de Seguridad que mantiene conexión con las Fuerzas Armadas de Rusia.

Ahora, es preciso cuestionarse, ¿cuándo es que la ciberseguridad se introduce dentro de los temas de Seguridad Nacional? Partiendo del referente que, en el año 2000, el concepto de "seguridad nacional" incorporó por primera vez el quinto dominio como un área que supondría una amenaza a la seguridad nacional de Rusia por otros países que a su vez intentaban posicionarse dentro de la esfera de la información y desarrollar sus propios principios y líneas de dirección en la guerra de la información (ciberguerra).[119]

Para el año 2010, la Doctrina Militar Rusa proyecta aún más la importancia y presencia de esta modalidad de conflicto, y marca un cambio en la comprensión sobre las amenazas a la nación. Por primera vez se resalta el papel cada vez más

---

[118] Bilyana Lilly; Joe Cheravitch, T*he Past, Present, and Future of Russia's Cyber Strategy and Forces,* 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade, Tallinn, NATO CCDCOE Publications, 2020, pp. 5-6.

[119] Bilyana Lilly; Joe Cheravitch, *The Past, Present, and Future of Russia's Cyber Strategy and Forces,* 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade, Tallinn, 2020, NATO CCDCOE Publications, 2020, p. 6.

importante de la guerra de la información dentro de los conflictos bélicos contemporáneos, así como lo imperativo de que las fuerzas armadas y las instituciones encargadas de vigilar la seguridad del Estado pudieran desarrollar capacidades, herramientas, y protocolos que atendieran de manera particular las implicaciones de la seguridad y de la guerra cibernética.

En diciembre de 2015, se publicó la actualización de la Estrategia de Seguridad Nacional de Rusia bajo el Edicto 683. (Véase: Capítulo 2, apartado 2.1, Rusia). En ese momento, Rusia reconoce para la defensa del Estado: la implementación de *hardware* especializado, así como la consideración de mejorar las formas y métodos de despliegue de las Fuerzas Armadas, a partir del perfeccionamiento de su capacidad de combate con la implementación de nuevos métodos dentro de guerras y conflictos modernos

Más recientemente, en el año 2016, con base en la doctrina del año 2000, la visión rusa toma fuerza para lograr definir lo que entenderían como "esfera de la información" (ciberespacio), siendo la "combinación de información, infraestructura de información, entidades involucradas en la recopilación, generación, distribución y uso de datos, así como un sistema para regular las relaciones públicas resultantes".[120]

[120] Nezavisimaya Gazeta ,President of Russia, "Ob utverzhdenii doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii [On Approving the Doctrine of Information Security of the Russian Federation]." Mayo 12, 2016, http://kremlin.ru/ acts/bank/41460/page/1 [En: Bilyana Lilly; Joe Cheravitch, "*The Past, Present, and Future of Russia's Cyber Strategy and Forces",* 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade, Tallinn, 2020, NATO CCDCOE Publications, 2020, p. 135.]

Y a su vez, los principios básicos de seguridad de la información (ciberseguridad):

> Los principios básicos sobre seguridad de la información internacional del Consejo de Seguridad de 2013 confirmaron este amplio entendimiento y la panoplia de amenazas relacionadas con la seguridad de la información que emanan del espacio cognitivo de ésta, impulsadas principalmente por actores extranjeros, y sus efectos sobre los valores sociales y la estabilidad. Consideraron que la tecnología de la información es un arma que puede usarse con fines políticos y militares para violar la soberanía y la integridad territorial de un Estado.[121] **(Consejo de Seguridad de la Federación Rusa 2013).**

A continuación, se presenta una lista de las principales amenazas y de respuestas de políticas contenidas dentro de los principales documentos sobre seguridad de la información desde la postura rusa.

[121] Security Council of the Russian Federation. 2013. "Osnovy gosudarstvennoy politiki Rossiyskoy Federatsii v oblasti mezhdunarodnoy informatsionnoy bezopasnosti na period do 2020 goda [Fundamentals of State Policy of the Russian Federation in the Field of International Information Security for the Period until 2020]." http://www.scrf.gov.ru/security/information/document114/. [En: Bilyana Lilly; Joe Cheravitch, "*The Past, Present, and Future of Russia's Cyber Strategy and Forces*", 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade, Tallinn, 2020, NATO CCDCOE Publications, 2020, p. 135.]

Tabla 6. Lista seleccionada de principales amenazas y respuestas de políticas recomendadas como se describe en los principales documentos de seguridad de la información de Rusia.

Documento	Amenazas		Recomendado (Respuesta política)
	Desde lo psicológico	**Desde lo técnico**	
Información Doctrina de Seguridad (Nezavisimaya Gazeta, 2000)	•Restricción irracional y excesiva del acceso a la información socialmente necesaria; uso ilegal de medios especiales de influencia. •Expulsar a las agencias de noticias y los medios de comunicación rusos del mercado de información nacional y aumentar la dependencia de las esferas espiritual, económica y política de la vida pública en Rusia de las estructuras de información extranjeras. •Una disminución en el potencial espiritual, moral y creativo de la población rusa.	•Desarrollo y distribución de programas que interfieren con el funcionamiento normal de la información y los sistemas de información y telecomunicaciones, incluidos los sistemas de protección de la información. •Riesgo de claves y medios de protección de información criptográfica. •Destrucción, daño o robo de máquinas y otros medios de almacenamiento.	•Introducción de enmiendas y adiciones a la legislación de la Federación Rusa que regula las relaciones en el espacio de la información para garantizar la seguridad de esta. •Aclarar la situación de las agencias de noticias, los medios y los periodistas extranjeros, así como de los inversores a la hora de atraer inversiones extranjeras para el desarrollo de la infraestructura de la información en Rusia; •Prioridad legislativa para el desarrollo de redes de comunicaciones nacionales, y la producción nacional de satélites de comunicaciones espaciales.
Vistas conceptuales sobre las Actividades de las Fuerzas Armadas en el Espacio Informativo (Ministerio de Defensa, 2011)	•Amenazas de carácter político en el espacio de la información.	•Uso generalizado de la tecnología informática en los sistemas de mando y control de tropas y armas.	•Las actividades de las Fuerzas Armadas de la Federación Rusa en el espacio de información se construyen con base en un conjunto de principios: legalidad, cooperación con Estados amigos y Organizaciones Internacionales; y contención y prevención de conflictos militares en el espacio de la información.

Convención para la Seguridad de la Información Internacional (Ministerio del Exterior Asuntos, 2011)	•Factores que crean un peligro para el individuo, la sociedad, el Estado y sus intereses en el espacio de la información. •Acciones en el espacio de la información para socavar los sistemas políticos, económicos y sociales de otro Estado, tratamiento psicológico de la población, desestabilización de la sociedad. •Utilizar la infraestructura de información para difundir información que incite a la enemistad étnica, racial e interconfesional, materiales escritos racistas y xenófobos.	•Impacto destructivo dirigido en el espacio de información sobre las estructuras críticas de otro Estado. •Contrarrestar el acceso a las últimas tecnologías de la información y la comunicación, creando condiciones para la dependencia tecnológica en el campo cibernético en detrimento de otros Estados. •Expansión de la información, adquisición del control sobre los recursos de información nacional de otro Estado.	Los Estados parte deben: •Mantener la paz y la seguridad internacionales y promover la estabilidad y el progreso económicos internacionales, el general bienestar de los pueblos y la cooperación internacional, libres de discriminación. •Abstenerse de desarrollar y adoptar planes y doctrinas que puedan provocar un aumento de las amenazas en el espacio de la información, así como provocar tensiones entre los Estados y el surgimiento de "guerras de la información". • Abstenerse de cualquier acción dirigida a la violación total o parcial de la integridad del espacio de información de otro Estado.
Principios básicos para la Política de Estado en Materia Internacional de Seguridad de información hasta 2020. (Seguridad Consejo, 2013)	•Llevar a cabo actos hostiles y de agresión destinados a desacreditar la soberanía, violar la integridad territorial de los Estados y representar una amenaza para la paz, la seguridad y la estabilidad estratégica internacionales. •Interferir en los asuntos internos de los Estados soberanos, perturbar el orden público, incitar a la hostilidad interétnica.	•Destruir elementos de la infraestructura de información crítica. •Delitos, incluidos los relacionados con el acceso ilegal a la información informática, con la creación, uso y distribución de programas informáticos maliciosos.	•Formación de un sistema de seguridad de la información internacional a nivel bilateral, multilateral, regional y mundial. •Crear condiciones para reducir el riesgo de utilizar las tecnologías de la información y la comunicación para actos hostiles y actos de agresión destinados a desacreditar la soberanía, violar la integridad territorial de los Estados y representar una amenaza para la paz, la seguridad y la estabilidad estratégica internacionales.

Seguridad de información Doctrina (Presidente de Rusia 2016)	• Uso creciente por parte de los servicios especiales de estados individuales de información e influencia psicológica con el fin de desestabilizar la situación política y social interna en varias regiones del mundo y socavar la soberanía y la integridad territorial. •Aumento de materiales en medios de comunicación extranjeros que contengan un mensaje que sesgue la evaluación de la política del gobierno de Rusia.	• Aumento en la escala y coordinación de ataques informáticos contra objetos de infraestructura de información crítica, aumento de las actividades de inteligencia de Estados extranjeros contra la Federación Rusa, así como un aumento en las amenazas en el uso de tecnologías de la información para causar daño a la integridad de la soberanía territorial, estabilidad política y social de la Federación.	•Disuasión estratégica y prevención de conflictos militares que puedan surgir como resultado del uso de la tecnología de la información; pronóstico, detección y evaluación de amenazas de información, incluidas amenazas a las Fuerzas Armadas de la Federación Rusa en el ámbito de la información. •Neutralización de información que pueda impactar psicológicamente, o que incluso esté destinada a socavar los cimientos históricos y las tradiciones patrióticas asociadas con la defensa de la Patria.

Fuente: **Bilyana Lilly; Joe Cheravitch**, *The Past, Present, and Future of Russia's Cyber Strategy and Forces,* 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade, Tallinn, 2020, NATO CCDCOE Publications, 2020, p. 8.

En el área legal, el Gobierno ruso expresa en la Ley Federal N°187-FZ sobre la seguridad de la infraestructura de información crítica de la Federación de Rusia, (julio de 2017), los principios básicos para garantizar la seguridad de dicha infraestructura; puntualiza los derechos, obligaciones y las responsabilidades de aquellos individuos que poseen instalaciones con infraestructura de carácter crítico, proveedores de comunicaciones y sistemas de información y comunicación que proporcionan interacción.[122]

Los elementos de la infraestructura de información crítica son:

- Sistemas de información.
- Redes de telecomunicaciones de las autoridades estatales.
- Sistemas y redes para la gestión de procesos tecnológicos que se utilizan en la defensa del Estado.
- Asistencia sanitaria.
- Transporte.
- Comunicación.

[122] S/a, *Rusia,* Ciberseguridad. Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas, WordPress. Disponible en: https://ciberseguridad.com/normativa/rusia/

- Finanzas.
- Energía.
- Industrias de combustible.
- Industria nuclear, aeroespacial, minería, metalmecánica y química.

Todas estas industrias e infraestructura se consideran críticas para el progreso y la estabilidad estatal, por lo que deben protegerse ante cualquier amenaza cibernética. La Ley de Seguridad de 2017 promovió la protección de la infraestructura crítica que se gesta con mayor fuerza desde 2013 con la Convención para la Seguridad de la Información Internacional, por lo tanto, significa que atender la ciberseguridad es atender a la seguridad integral del Estado ruso (o cualquier otro). La Federación Rusa enfatiza, a partir de ese momento en todos sus documentos oficiales, su concepción de amenaza por el lado psicológico y también por el lado técnico. Junto con los demás documentos que se presentan en la tabla, el panorama sobre el accionar ruso en ciberdefensa puede definirse como ofensivo y defensivo.

Cabe destacar que la apropiación e interiorización de los conceptos sobre el espacio de la información es notorio y relevante, así como el énfasis en los valores nacionales, sus intereses e integridad patriótica por sobre de todos los demás temas que puedan darse al hablar de la seguridad y defensa de la información rusa. No obstante, es interesante señalar que las referencias en la historia y legislación de este país sobre la ciberdefensa, tiene aproximadamente dos décadas; de manera contundente y formal, las bases que guían su accionar dentro del quinto dominio corresponden a una estructura que ha sido construida por las últimas tres administraciones, de las cuales destaca el presidente actual Vladimir Putin, quien ha sido Jefe de Estado desde el año 2000.

Si bien la idea anterior no se establece con la intención de minimizar la experiencia cibernética del Estado ruso, si denota que la atención al ciberespacio, siendo uno de los países más influyentes en la escena internacional, es reciente, por lo que mantiene su perfeccionamiento y alcance constante retomando lo que acontece en todos los dominios, además del quinto.

De acuerdo con esta doctrina, la guerra de la información consiste en operaciones cibernéticas y de información, siendo un elemento integral del conflicto moderno. Cuando se habla de la guerra de información, la doctrina oficial describe a

Rusia como un Estado que se apega a una postura defensiva en un entorno caracterizado por adversarios agresivos, aunque, en la práctica también forma parte de ellos.

La Doctrina de Seguridad de la Información de la Federación Rusa se basa en los siguientes principios **(President of the Russian Federation, 2000):**

- El cumplimiento de los derechos constitucionales y las libertades del ciudadano para utilizar la información: Hace referencia a las implicaciones que conlleva la preservación y el fortalecimiento de los valores morales de la sociedad y las tradiciones como el patriotismo, además de aumentar el potencial cultural y científico del país.
- Enfatiza transmitir información confiable al público ruso e internacional, acerca de la política estatal de la Federación Rusa y su posición oficial sobre los acontecimientos de importancia social. Esto se logra con permitir el acceso de los ciudadanos a los recursos de información del gobierno.
- La promoción de las tecnologías modernas de información: Impulsa la industria de la información (informática, telecomunicaciones e instalaciones de comunicaciones en particular) para asegurar la satisfacción de las necesidades del mercado nacional con productos propios, así como la entrada en el mercado mundial. Rusia debe ocupar una digna posición en el mundo, dentro de la industria microelectrónica e informática.[123]

En concordancia con las normas anteriormente presentadas, la Doctrina de la Seguridad de la Información de la Federación Rusa continúa con la línea de la protección, acceso a la información y cumplimiento a nivel interno, como primera instancia. Si bien, muchas han sido las críticas a los puntos que establece la doctrina en la última década, por los miembros de la sociedad civil debido a la incongruencia en la praxis y el discurso, en lo que respecta a la libertad de expresión, acceso a la información y transparencia mediática, no es menester de la presente investigación ahondar en ello, pero sí ofrece una invitación a hacer un análisis individual y colectivo de dicha cuestión en otros espacios académicos.

[123] Ministerio de Política Exterior de la Federación Rusa, *Doctrina de Seguridad de la Información*, Presidente de la Federación Rusa, 2000. En: Eduardo, Leiva. *"Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local"*, Revista Latinoamericana de Ingeniería de Software, Vol. 3, núm. 4, Argentina, 2015, pp. 161-176.

El **Dr. Andrew Foxall**, del Ministerio de Defesa del Reino Unido, encuentra que la forma en la que Rusia ha conducido su política exterior de guerra en la praxis, al menos en los eventos de los cuales destacan la invasión de Georgia (2008), la anexión de Crimea y la desestabilización de Ucrania (2014), se han caracterizado por la implementación de la ciberguerra junto con la guerra convencional, convirtiendo sus tácticas tradicionales en híbridas dentro de sus esquemas ofensivos y defensivos; lo que al mismo tiempo configura a la ciberguerra como una variable constante y como herramienta que resalta dentro de la política rusa[124].

Como un extra para salvaguardar su información y espacio cibernético, en 2019 se habilitó legalmente el proyecto de la internet soberana, conocido como *RuNet*, y ya se ha probado con éxito. *RuNet* permitiría que internet siga funcionando en el país, aunque reconduciendo todo el tráfico de datos a servidores nacionales controlados por autoridades estatales, filtrando así la decisión de lo que puede verse en internet o no.[125]

El objetivo del proyecto era, de hecho, tener un camino alternativo cuando Rusia percibiera amenazas a nivel cibernético. Aunque esta medida pueda ser criticada y dé paso a un debate e intercambio de opiniones, debe tomarse en cuenta como otra línea bajo la cual este país ha optado para incorporar la protección de sus intereses estatales en el quinto dominio.

En suma, la agenda rusa de ciberseguridad se encuentra articulada por la herencia tradicional y conservadora, que se ha distinguido por las líneas direccionales de corte soviético y que continúan intrínsecas a los valores que persigue la Federación para securitizar su ciberespacio.

Se debe destacar que, Rusia ha generado de manera autónoma su concepción alrededor de los elementos del ciberespacio distinguiéndolos de la visión occidental.

Es probable que la conceptualización rusa de la guerra de la información y las unidades que ejecutan estas operaciones impulsen y determinen la futura política y su estrategia cibernética. La noción, por ejemplo, de que Rusia se enfrenta a agresores que están utilizando las Tecnología de la Información y las Comunicaciones en evolución para socavar el potencial militar y la sociedad de Rusia, es casi seguro

---

[124] Andrew Foxall, "Putin´s Cyberwar: Russia´s Statecraft in the Fifth Domain", *Policy paper, England,* Russia Studies Centre, núm. 9, 2016, 15 pp.

[125] Manuel G. Pascual, "El Kremlin da el primer paso para aislar el internet ruso del resto del mundo", *El País*, Tecnología, España, marzo 2022. [En línea] https://elpais.com/tecnologia/2022-03-12/el-kremlin-da-el-primer-paso-para-aislar-el-internet-ruso-del-resto-del-mundo.html 98

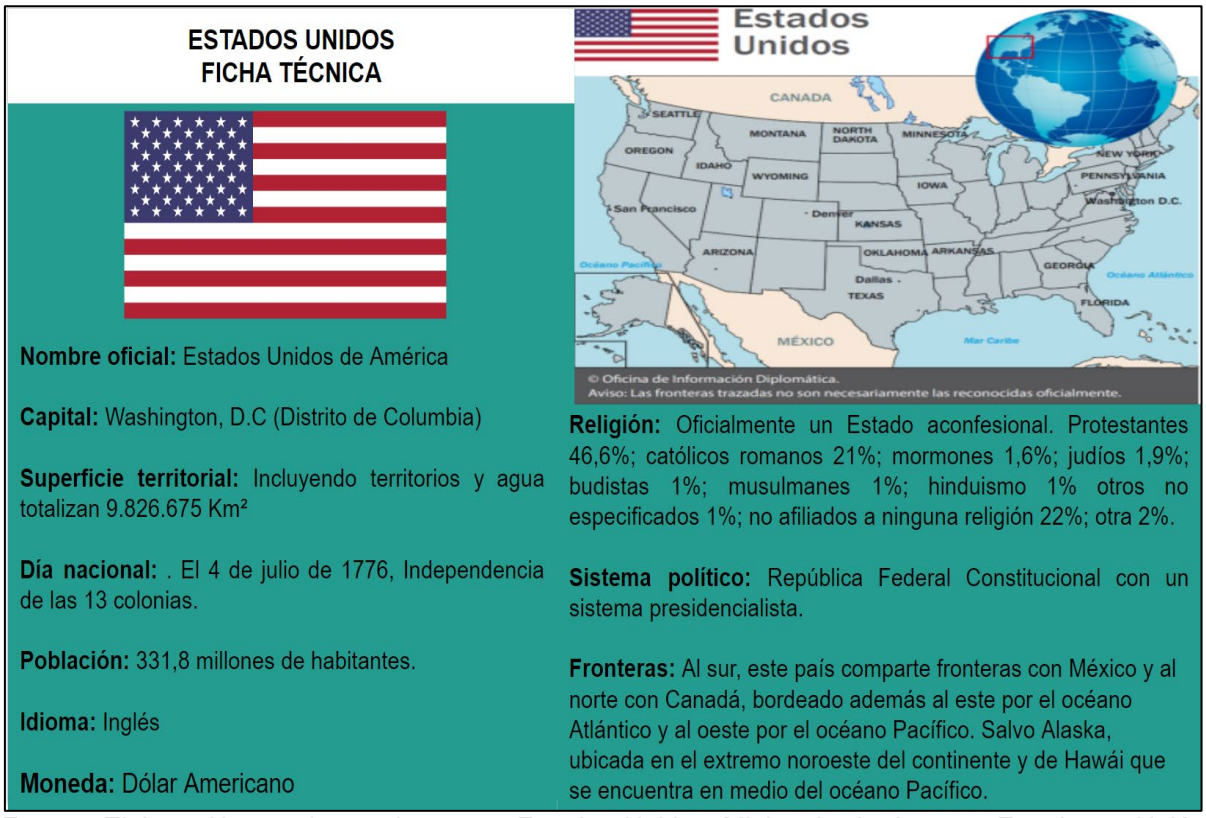
que perdurará en el futuro inmediato, por lo que el cuadro presentado en éste apartado muestra así la constante atención y actualización de las estrategias a las condiciones actuales que tienen lugar en el entorno cibernético, para poder respaldar de forma legal, a nivel nacional e internacional, el accionar ruso ante distintos factores que pretendan vulnerar su seguridad nacional desde el ciberespacio.

Finalmente, cabe señalar que, ante todo, en la Ley Federal sobre la Seguridad de la Infraestructura de Información Crítica de la Federación Rusa, se considera que la seguridad de la información crítica es fundamental para promover y garantizar la seguridad de los sectores clave que sostienen la estabilidad de la dinámica y la preservación del Estado ruso. Lo mencionado anteriormente es un ejemplo valioso de cómo Rusia expone al resto del mundo, a través de sus políticas de seguridad y ciberseguridad, la articulación entre seguridad nacional y ciberseguridad; es la evidencia de la necesidad imperativa de comprender que la ciberseguridad es la seguridad nacional en las demandas del siglo XXI y que se debe priorizar el estudio del quinto dominio en las actividades estatales de todo el mundo.

3.1.2 La agenda de ciberseguridad estadounidense.

Al igual que en el apartado anterior, para el caso de la agenda de ciberseguridad de Estados Unidos, se presentarán a continuación algunos datos básicos del país para ubicar al lector sobre el contexto estadounidense.

Figura 9. Datos básicos de Estados Unidos de América.



Fuente: Elaboración propia con base en: *Estados Unidos*, Ministerio de Asuntos Exteriores. Unión Europea y Cooperación, Oficina de Información Diplomática, marzo 2022, 23 pp.

Desde principios del siglo XX Estados Unidos emergió como una potencia de suma relevancia; fue al final de la Segunda Guerra Mundial que tomó su lugar como superpotencia global. A partir de los ataques del año 2001, comenzó a securitizar la agenda internacional, con enfrentamientos en diferentes zonas de Medio Oriente y algunas disputas políticas y económicas contra actores como Rusia, China o Corea del Norte.[126]

En el contexto estadounidense, la ciberseguridad comenzó a tomar relevancia por el auge económico de la Tercera Revolución Industrial. En primera instancia el

[126] Marco A. Lopátegui Torres; Mariana Corona Fragoso, "*Las amenazas a la ciberseguridad en América del Norte y la capacidad de respuesta regional: un análisis comparado institucional",* México, UNAM, octubre 2021.

Departamento de Seguridad Nacional de Estados Unidos, establecido por el presidente en turno, George W. Bush, en 2002, asumió la responsabilidad de la protección de la infraestructura de la Tecnología de la Información (TI) crucial para el país desde ese momento.

La concepción de ciberseguridad, por la parte estadounidense, la definió el Departamento de Defensa, entendiéndola en un primer momento como se cita a continuación:

> Es la prevención de daños para la protección y restauración de computadoras, sistemas electrónicos de comunicación, servicios de comunicación electrónica, comunicaciones alámbricas y comunicación electrónica, incluyendo información contenida en ellos, para asegurar su disponibilidad, integridad, autenticidad, confidencialidad y no repudio.[127]

La definición anterior, expone que la concepción estadounidense centra su atención en la protección a la infraestructura de sistemas tecnológicos, infraestructura crítica, y específicamente en prevenir la violación de la información contenida en distintos dispositivos, o redes de almacenamiento de datos relevantes. Así mismo, la concepción de ciberseguridad no solo se encuentra definida de manera textual o limitada a lo que comprende la cita presentada, sino que se va complementando al paso del tiempo a través de estrategias sobre políticas públicas y de política exterior; como la presencia regional e internacional con la creación conjunta de documentos, protocolos, informes, tratados que orientan la ciberseguridad como área relevante en las agendas y debates para el bienestar global. Es así como la concepción estadounidense de ciberseguridad se va perfeccionando y redefiniendo constantemente.

Actualmente la Agencia de Seguridad, Ciberseguridad e Infraestructura de Estados Unidos, (CISA) por sus siglas en inglés, agrega: “La ciberseguridad es el arte de proteger redes, dispositivos y datos del acceso no autorizado o uso delictivo y la práctica de garantizar la confidencialidad, integridad y disponibilidad de la información”.

Estados Unidos de manera interna, generalmente aborda la ciberseguridad a través de estatutos, regulaciones y requisitos de su industria privada específicos del sector. A nivel federal, numerosas agencias imponen estándares de ciberseguridad a través de una variedad de mecanismos regulatorios y de aplicación.

---

[127] U.S. Office of the Chairma*, The Joint Chiefs Of Staff. Department of Defense Dictionary of Military and Associated Terms* (JP 1-02), Washington, CJC, 2015.

> En primera instancia, el Departamento de Seguridad Nacional estadounidense es el encargado del sistema de respuesta ante incidentes cibernéticos, brinda asistencia a entidades potencialmente impactadas, analiza el impacto potencial en la infraestructura crítica, investiga a los responsables de los ataques en conjunto con las fuerzas del orden público y coordina la respuesta nacional ante incidentes cibernéticos; colabora con otras agencias federales y locales en misiones cibernéticas complementarias, así como con propietarios y operadores del sector para garantizar una mayor unidad de esfuerzos y una respuesta de alcance nacional a los incidentes cibernéticos.[128]

Asimismo, existen distintas instituciones e iniciativas que complementan lo dispuesto por el Departamento de Seguridad Nacional en el ámbito cibernético, específicamente se enlistan a continuación:

- **Ley de mejora de la ciberseguridad de 2014.**

  Con el objetivo de fortalecer la investigación en temas sobre el ciberespacio, mejorar la ciberseguridad y el desarrollo de ésta; la ley permite la asociación y cooperación entre sector público y privado para su ejecución, así como la promoción de la conciencia pública para la seguridad y buenas prácticas en el ciberespacio.[129]

- **Ley de Protección de Avance de 2015.**

  Hace una modificación a la Ley de Seguridad Nacional de 2002, para habilitar al Departamento de Seguridad Nacional y el Centro de Integración de Comunicaciones (NCCIC), que dé inclusión como representantes no federales, a los gobiernos tribales, centros de análisis y entidades privadas, lo cual permite una mejor promoción de la ley y su contenido, así como la participación informada de más sectores.[130]

- **Cyber Command (USCYBERCOM).**

  Se transforma de forma paralela con los planes del Pentágono para consolidar la fuerza cibernética de Estados Unidos, así como los requisitos para la seguridad y defensa. Los tres ejes principales que orientan sus actividades son: (1) la C*yber National Mission Force,* con el propósito de evitar ataques cibernéticos a la infraestructura crítica, (2) *Cyber Combat Mission Force,*

[128] Marco L.; Mariana C.; "*Las amenazas a la ciberseguridad en América del Norte y la capacidad de respuesta regional: un análisis comparado institucion*al", Amenazas a la seguridad en el siglo XXI, en el marco del Proyecto PAPIIT IN307018, octubre 2021, p 15.
[129] Ibid, p. 15
[130] Ibid, p. 15

responsable de coordinar las operaciones en el extranjero con objetivos militares que se suscitaron en o a través del ciberespacio, y (3) *Cyber Protection Force,* enfocada en la defensa de la infraestructura de las TIC dependientes del Pentágono.[131]

- **Ley de la Agencia de Seguridad de Infraestructura y Ciberseguridad, 2018.**

  Atiende de manera específica la coordinación de defensa (especializada) de la infraestructura crítica estadounidense de los ataques cibernéticos y físicos.[132]

- **Cybersecurity and Infrastructure Security Agency (CISA)**

  A través de la Agencia se ha promovido el intercambio perfeccionado de la información sobre amenazas a la ciberseguridad y para defenderse de ciberamenazas se gestiona, a nivel gubernamental, y también con socios privados. La Ley de la Agencia de Seguridad de Infraestructura y Ciberseguridad de 2018 que nace junto con el Centro Nacional de Integración de Comunicaciones y Seguridad Cibernética (NCCIC); desempeña un papel importante para el acceso del gobierno a cualquier aspecto relacionado con la seguridad informática por medio de capacidades de respuesta ante ciberataques, y para garantizar que todos los sitios gubernamentales (web.gov) permanezcan seguros.[133]

- **Ley de Mejora de la Ciberseguridad del IoT (Internet of Things), 2020.**

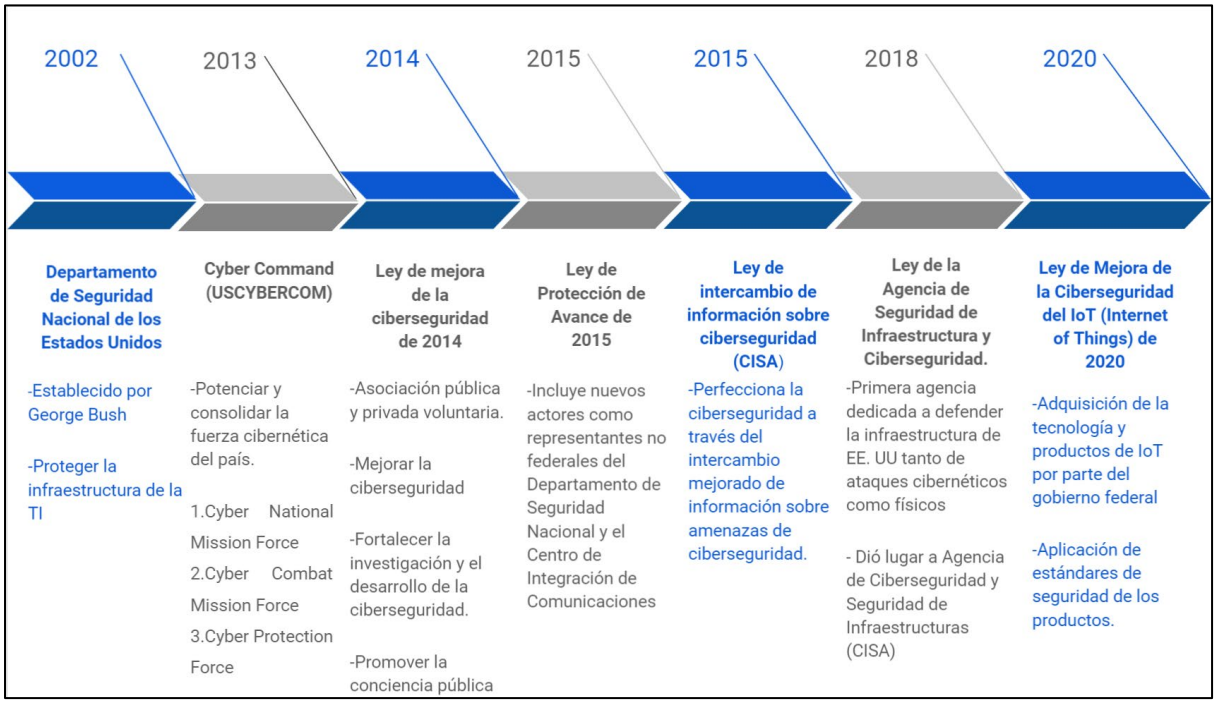
  Al reconocer que la ciberseguridad involucra el uso de todo dispositivo con conexión a internet, lo cual representa una oportunidad para implementación de prácticas que vulneren la estabilidad cibernética, es que ésta ley pone énfasis en los requisitos, limitantes y prohibiciones para la adquisición de tecnología y productos de IoT; sobre todo aquellos destinados al uso de servidores públicos, equipos que su uso sea dentro de instituciones gubernamentales con información de carácter nacional o clasificada. Los fabricantes de los dispositivos deben cumplir con los estándares de seguridad si no quieren perder los contratos de adquisición celebrados con el gobierno, tal es el caso de priorizar la seguridad de los dispositivos por encima de la velocidad y precio de comercialización; de igual modo la Ley establece normas

[131] Ibid., p.16.
[132] Ibid., p.16.
[133] Ibid., p.16.

voluntarias aplicables a empresas relacionadas con la infraestructura crítica a través del Instituto Nacional de Estándares y Tecnología (NIST), con un marco de seguridad cibernética que instaura mejores prácticas de búsqueda para gestionar y reducir riesgos cibernéticos en las empresas estadounidense, o no estadounidenses, pero que se encuentren dentro del territorio.[134]

A continuación, se presenta una línea del tiempo que resume la información descrita en los párrafos anteriores:

Figura 10. Evolución de la ciberseguridad en Estados Unidos



Fuente: Elaboración propia en; **Marco L.; Mariana C.**, *Las amenazas a la ciberseguridad en América del Norte y la capacidad de respuesta regional: un análisis comparado institucional*, Amenazas a la seguridad en el siglo XXI, en el marco del Proyecto PAPIIT IN307018 octubre 2021, p 19.

A partir del desglose de algunos ejes principales descritos con anterioridad, se presenta que la valoración estadounidense de ciberseguridad se sostiene manteniendo en primer lugar a Estados Unidos, "*America First*", lo que significa que sus intereses nacionales se ubican por encima de los intereses (económicos/políticos/sociales) de otros países y que sus ventajas tecnológicas no deben ser cuestionadas.[135]

[134] Ibid., p.17
[135] Zheng, Li, "*Different Values but Similar Visions for Cyberspace*", Retrieved, China-US Focus Magazine, 16 de enero 2018. Disponible en: https://www.chinausfocus.com/peace-security/different-values-but-similar-visions-for-cyberspace

Asimismo, destacan diferentes elementos en torno a la agenda de ciberseguridad estadounidense. En primer lugar, hay que señalar que Estados Unidos ha desarrollado con fuerza en las últimas dos décadas normas, leyes, reformas, etc. que principalmente velan por la seguridad de la información contenida en sus sistemas digitales. Lo anterior, se realiza de manera conjunta con el sector privado; una característica importante que en la búsqueda de securitizar su ciberespacio, apela a la homogeneidad en dicha cooperación con el objetivo de no ver interrumpida la estabilidad de la dinámica ciberespacial estadounidense por factores terroristas, robo de datos, actividades criminales, control de infraestructura crítica, etc., lo que se traduce, al mismo tiempo, en un obstáculo para llevar a cabo satisfactoriamente sus metas para el desarrollo nacional e internacional.

En suma, se puede comprender que las políticas de ciberseguridad y ciberdefensa tienen una línea de acción interna y externa;

> [...] Por un lado, la defensa de los sistemas nacionales internos recae en una mancuerna de acción entre el sector privado y público, dada la importancia del desarrollo comercial e industrial que deposita el país para su economía, además de la creación de departamentos que atienden y vigilen las vulnerabilidades cibernéticas a las cuales el país se encuentra expuesto, sí como la promoción de la investigación en torno al tema de la seguridad cibernética. Por otro lado la regulación en torno a la adquisición de tecnología del exterior, bajo la aplicación de estándares de seguridad de los productos que asegura el estado de preservación y control del ciberespacio desde el ingreso al país es un ejemplo de las precauciones que el Estado norteamericano tiene en consideración para su política de ciberseguridad externa, además de la inversión económica que delega a fondos, organizaciones e instituciones internacionales como la OTAN, el Fondo de Modernización Económica, a la Unión Internacional de Telecomunicaciones, etc.[136]

Con base en la última idea, el gobierno estadounidense complementa sus líneas de ciberseguridad cooperando con diversos organismos internacionales en el área específica de seguridad informática y ciberespacial, algunos de ellos ya mencionados y descritos en su quehacer y dinámica. (Véase apartado 2.2).

De igual manera, la interconexión que asoma la lectura de sus distintos órganos, normas y protocolos, subraya la articulación y comunicación que el país ha puesto en marcha entre las instituciones, agencias, departamentos y actores partícipes de salvaguardar la seguridad cibernética nacional, por medio del

[136] Op. Cit., Marco L.; Mariana C

intercambio de datos eficiente y efectivo ante cualquier evento que implique una ciberamenaza.

Se debe destacar, el interés de Estados Unidos al reconocer la educación como elemento clave para promover su seguridad en el quinto dominio; una propuesta implícita, al menos en sus legislaciones internas, que invitan a replicar en ejercicio de manera global como una estrategia preventiva y cooperativa con la sociedad civil.

3.2 El conflicto a través del mundo cibernético. Confrontación ruso-estadounidense.

Muchos han sido los escenarios a lo largo de la historia en los que convergen Estados Unidos y Rusia como actores principales. El conflicto entre ambos países, alimentado por su estatus de grandes superpotencias geopolíticas, la divergencia entre Occidente y Oriente, entre el sistema capitalista y el sistema socialista, ha representado mundialmente una balanza de contrapesos y de choques constantes que han llamado la atención en su relación. Es fundamental entender la cronología y los eventos que históricamente han tenido lugar de forma “física” para contextualizar y analizar el panorama actual de ambos, tanto en el ciberespacio, así como dentro de las tensiones existentes dentro del mismo.

El evento por excelencia de tensión entre ambos actores fue la Guerra Fría que comprendió el período entre 1945 a 1989; se distinguió por ser un enfrentamiento político, ideológico, económico y cultural de dos bloques de países liderados por Estados Unidos y, en ese momento, por la URSS.

Algunas de las principales características que pervivieron durante varias décadas fueron:

- Sin ser un enfrentamiento armado directo, había conflicto permanente implícito.
- Fuerte escalada armamentista, existía una preocupación y amenaza constante de destrucción mutua asegurada; las armas nucleares con capacidad de destrucción global fueron un tema relevante.
- Cada uno de los bloques, capitalista y socialista, se organizó mediante tratados de cooperación, ayuda mutua y apoyo militar. El bloque occidental integró la OTAN y el bloque oriental, el Pacto de Varsovia y el Consejo de Ayuda Mutua Económica (COMECON).

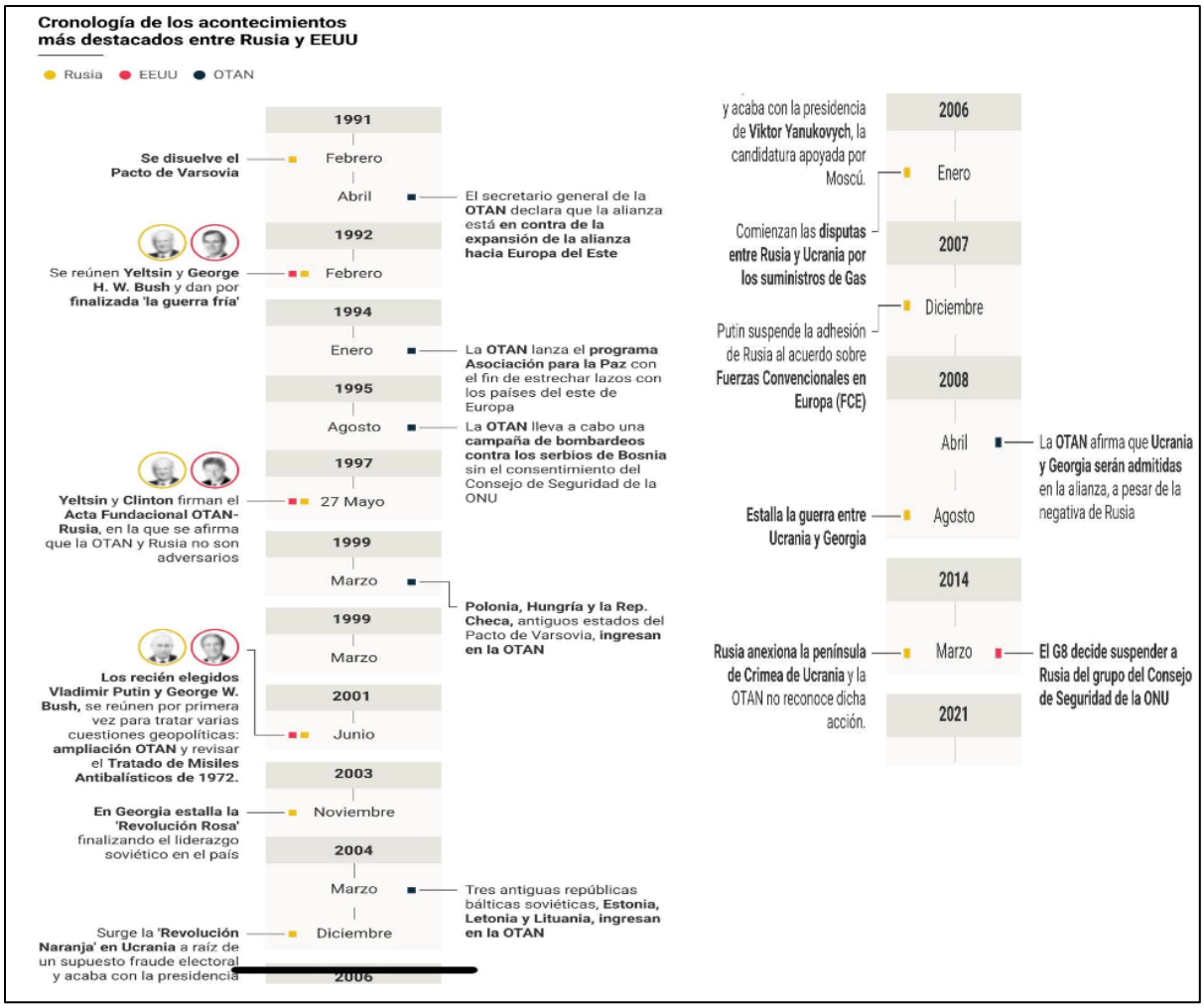
- El momento de máxima tensión fue denominada como la “Crisis de los misiles” en Cuba (1962), que desencadenó un fuerte temor a que la guerra nuclear fuera una realidad próxima.
- A partir del enfrentamiento de lógica política, se derivaron otras áreas de competencia como la ciencia, la tecnología y la cultura. La carrera espacial por la conquista y exploración del espacio exterior fue la más destacada y en ella ambos bloques invirtieron grandes sumas de dinero. [137]

Hacía la década de 1990 la Guerra Fría se dio por finalizada con la caída del Muro de Berlín (1989) y la posterior desaparición de la Unión Soviética (1991). En febrero de 1992 Boris Yeltsin y George H.W Bush se reunieron y dan por finalizada su rivalidad, formalmente. Desde entonces, el cambio ideológico y algunas acciones militares por parte de ambas naciones han mantenido la tensión entre sí. A su vez la era de la posguerra se ha distinguido por la dominación de la globalización en el sistema-mundo. Lo anterior ha dado paso a la posibilidad de la comercialización de la Internet, el crecimiento en las telefonías móviles y la incorporación de la red como un espacio de dinámicas político-sociales, lo cual ha traspolado dichos cambios ideológicos y de acciones militares a ocupar el espacio cibernético.

En la siguiente imagen se ilustran algunos de los momentos de relevancia en la relación bilateral Rusia- Estados Unidos, al finalizar la Guerra Fría.

[137] National Geographic, *¿Qué fue la Guerra Fría?*, National Geographic Society, noviembre 2022. Disponible en: https://www.nationalgeographicla.com/historia/2022/11/que-fue-la-guerra-fria

Figura 11. Cronología de los acontecimientos más destacados en la relación Rusia-Estados Unidos.



Fuente: **Rocío Márquez**, *Cronología de la relación entre Rusia y Estados Unidos: la Guerra Fría que no acaba,* El Confidencial, España, febrero 2022. Disponible en: https://www.elconfidencial.com/mundo/2022-02-24/cronologia-rusia-estados-unidos-guerra-fria_3368345/

Entre las características de un ciberataque, detalladas en el primer capítulo de esta investigación, se retoma el del anonimato; que la autoría sea confirmada de ser rusa o estadounidense es muy complicado lograrlo, sin embargo, hay casos que han podido afirmarse con total certeza. Con base en la aclaración anterior, a continuación, se presentan algunos de los ciberconflictos en los que históricamente ambos países han participado, enriqueciendo así la panorámica del estatus de su relación en el ámbito ciberespacial.

Tabla 7. Ciberataques a Estados Unidos y Rusia.

Ciberataques a Estados Unidos	Ciberataques a Rusia
2008. "Operación *Buckshot Yankee*". Ataque malicioso al Departamento de Defensa de Estados Unidos. Se trató de un gusano informático que tenía el objetivo de escanear computadoras en busca de datos, dar acceso al sistema y al control remoto del mismo. Se sospechaba que los piratas informáticos rusos estaban detrás de esto porque habían usado el mismo código que compuso ciberataques anteriores como "agent.btz".	2017. Washington irrumpe en la red eléctrica rusa insertando algunos virus para activarlos en caso de algún conflicto.
2014. Robo de datos confidenciales a los principales bancos estadounidenses (Bank of America, Regions Bank TD Bank). Se estima que 76 millones de hogares y 7 millones de pequeñas empresas pudieron tener sus datos comprometidos.	2019- Servicios especiales de EE. UU intensifican ciberataques para penetrar y perjudicar la infraestructura, especialmente de los sectores: transporte, energía y bancaria.
2015. El sistema de correo electrónico no clasificado del Estado Mayor del Conjunto del Pentágono de EE. UU fue objeto de un ataque cibernético sofisticado. 4,000 miembros del personal militar y civil se vieron afectados; el sistema se cerró y mantuvo inactivo y desconectado durante casi dos semanas.	
2016. El presidente Barack Obama ordena la expulsión de 35 diplomáticos rusos por ciberataques. Dos equipos de piratería del servicio de inteligencia ruso son señalados de infiltrar al Partido Demócrata, alterando el proceso electoral.	
2017. Planta Nuclear "Wolf Creek" en Kansas, recibe un ciberataque para inmiscuirse en sus sistemas de control.	
2018. El FBI y el Departamento de Seguridad Nacional reportaron una serie de ataques informáticos a instalaciones estadounidenses (entidades federales, empresas del sector eléctrico, nuclear, comercial, agua, aviación de manufactura crítica del país.	
2020. Ciberataques y ciberespionaje al Departamento de Estado, del Tesoro, del Comercio, de Seguridad Nacional y a la Agencia Nuclear. Denominado como "Solar Winds Cyberattack" por ser la empresa desde donde entró el *malware* al *software.*	

Fuente: **Bilyana Lilly & Joe Cheravitch**, The Past, Present, and Future of Russia's Cyber Strategy and Forces, Tallinn, 2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade, © NATO CCDCOE Publications, 2020, pp 8.

La notable diferencia que se observa en la tabla anterior corresponde a considerar dos aspectos relevantes; por un lado, la gran discrepancia entre la cantidad de casos de ciberataques registrados en contra de EE. UU en contraste con los perpetrados contra Rusia, y por el otro, el papel que Rusia sostiene desde hace al menos 30 años como uno de los principales países desde donde provienen los incidentes. Rusia se ha instalado fuera del alcance de los incidentes cibernéticos debido, principalmente, a que buena parte de los atacantes residen en este país o temen represalias por parte del gobierno de Vladímir Putin, el cual a su vez se le ha encontrado estrechamente relacionado con grupos de *crackers (Nation-state groups)* los cuales presuntamente siguen indicaciones del gobierno para ejecutar masivamente ataques cibernéticos a los enemigos del Estado ruso con gran capacidad para perpetrar la estabilidad cibernética; el más emblemático de ellos conocido como *Cozy Bear/APT 29/Nobelium:*

> Llevan años poniendo contra las cuerdas a gobiernos, partidos políticos y empresas de medio mundo. Su lista de operaciones (conocidas) es larga. Tan larga que a servicios de inteligencia y empresas de ciberseguridad les ha costado años encontrar un hilo conductor entre todas ellas. Por eso se les conoce por una decena de nombres distintos. Incluso, en algunos casos se tardan meses (o incluso años) en saber que fueron ellos quienes se encontraban detrás de un ciberataque de gran envergadura.[138]

Que Moscú cuente abiertamente, o no, con dicho cuerpo (amplio, especializado, militarizado y altamente jerarquizado) de colaboradores, con distintas divisiones operativas que desarrollan sus tareas en áreas como la política, la energía, la diplomacia o el sector de las telecomunicaciones, puede dar con más facilidad otra razón por la cual Rusia no parece sufrir tantos ciberataques como lo hace Estados Unidos, ya que así como tiene un gran grupo ofensivo, es igualmente defensivo tomando en cuenta las habilidades que los *hackers* y *crackers* tienen al desarrollar con base en el objetivo perseguido. Lo anterior está perfectamente respaldado por el avance y perfeccionamiento paralelo de sus políticas públicas y doctrinas de seguridad y ciberseguridad nacionales. Incluso no puede pasarse por alto el restringido acceso a la información relativa a la seguridad de Rusia.

No obstante, es sustancial observar cómo la dinámica de confrontación entre ambos sigue siendo constante. Si bien la tabla y la información hasta ahora

[138] Daniel J. Ollero, “El peligroso grupo de hackers (y espías) que pone contra las cuerdas a gobiernos de medio mundo”, EL MUNDO, Madrid, España, junio 2021. Disponible en: https://www.elmundo.es/tecnologia/2021/06/02/60b0f3d4fdddffaa818b45a9.html

documentada podrían hacer parecer obvia la conclusión de que Estados Unidos aparentemente no contrataca a la Federación Rusa cibernéticamente, en respuesta a los ataques que ha sufrido y/o intentado infiltrarse dentro de sus sistemas, existen diversos estudios que muestran en tiempo real que la idea anterior podría no ser del todo certera.

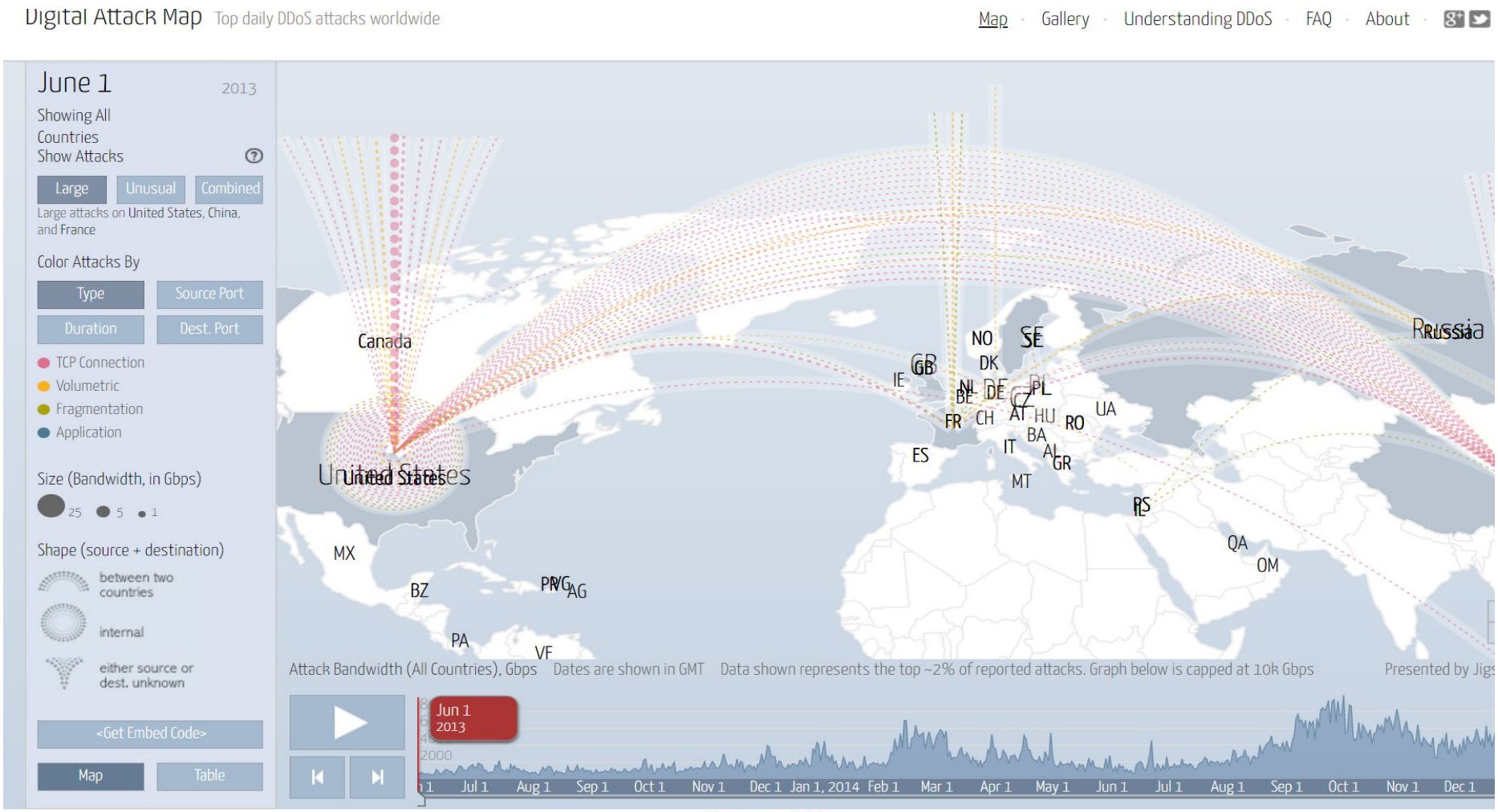
Actualmente, existe una amplia variedad de mapas interactivos que muestran ciberataques en tiempo real, que permiten observar casos de países en específico, algunos de ellos son:

- *Digital Attack Map:* se concentra en los ataques DDoS diarios en todo el mundo
- *FireEye:* se especializa en las amenazas cibernéticas en tiempo real en los principales sectores industriales por país y muestra al máximo atacante en cada uno.
- *Kaspersky:* Muestra el ataque en tiempo real y sus diversos sistemas de origen
- *Threat Cloud by Check Point:* Revisa los principales países de origen y destino de las amenazas en la nube.
- *Akamai:* Mapa regional, se concentra en la descripción del tráfico de red.
- *Bitdefender:* Ataques relacionados con correo no deseado, infección y ataque para robo de información.

Aunque existen muchos más, los anteriormente enlistados cuentan con el respaldo de diversas instituciones dedicadas a la ciberseguridad y se concentran en los tipos de ataque más frecuentes y riesgosos.

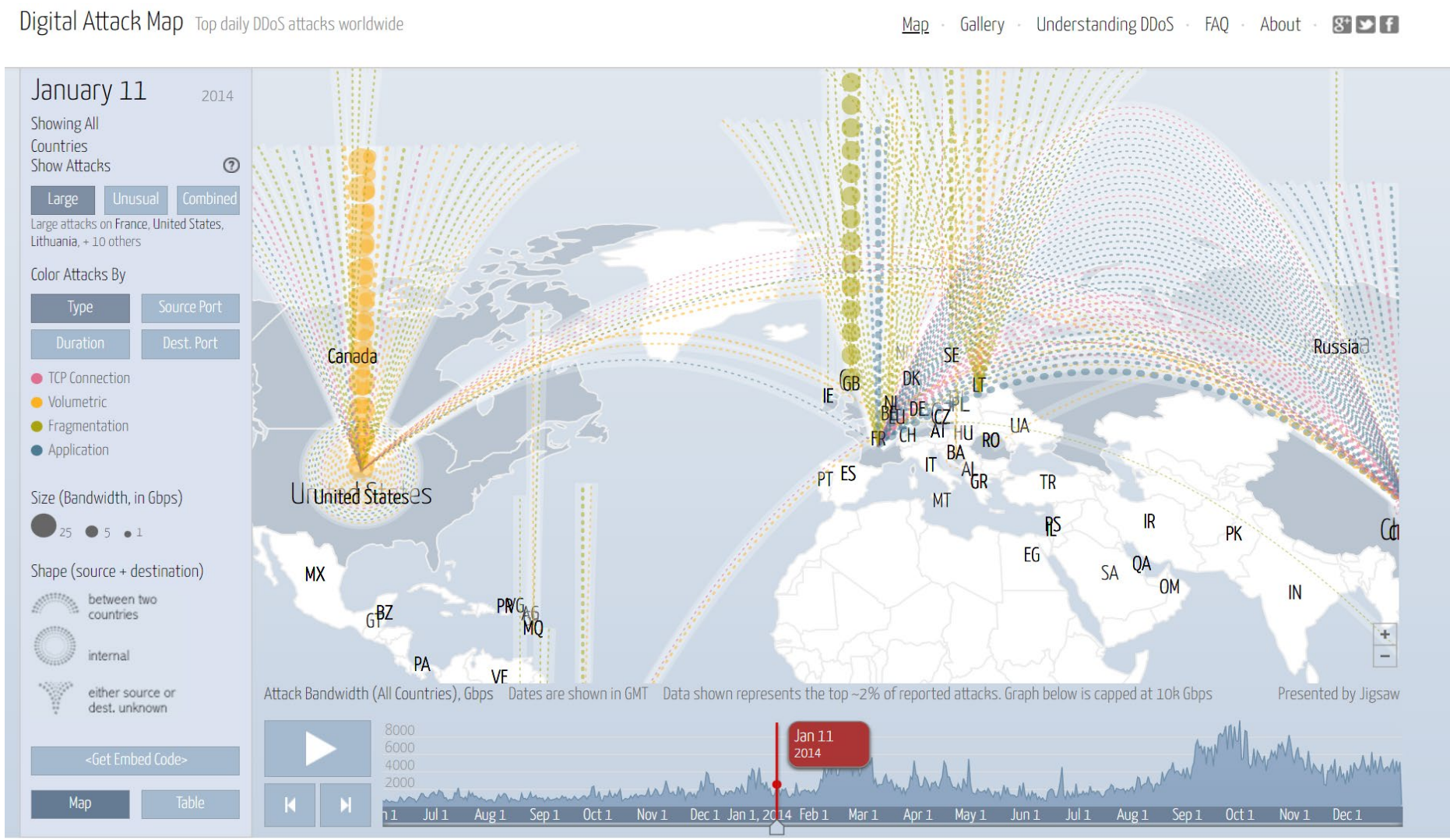
Para objeto de la investigación, el *Digital Attack Map* es el que mejor ilustra los ciberataques en la relación Rusia-Estados Unidos, ya que como se expone a continuación, guarda el registro por año de los ciberataques entre ambos (recibidos y realizados), dando así paso al análisis del estudio de caso.

Figura 12. Ciberataques Rusia- Estados Unidos 2013



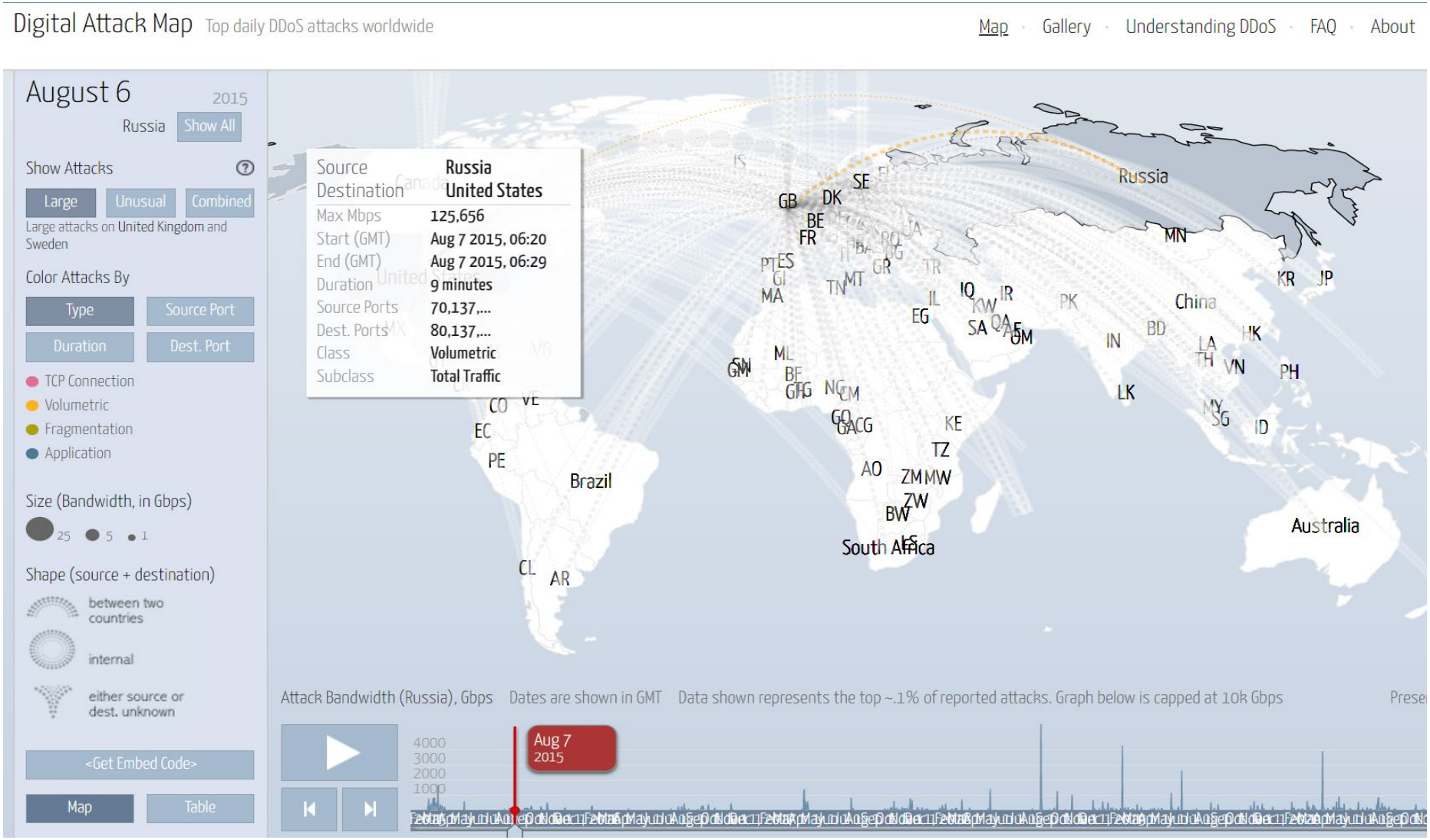
Fuente: Google Ideas, Digital Attack Map, DDoS data 2020, Arbor Networks, Inc.

Figura 13. Ciberataques Rusia-Estados Unidos 2014.



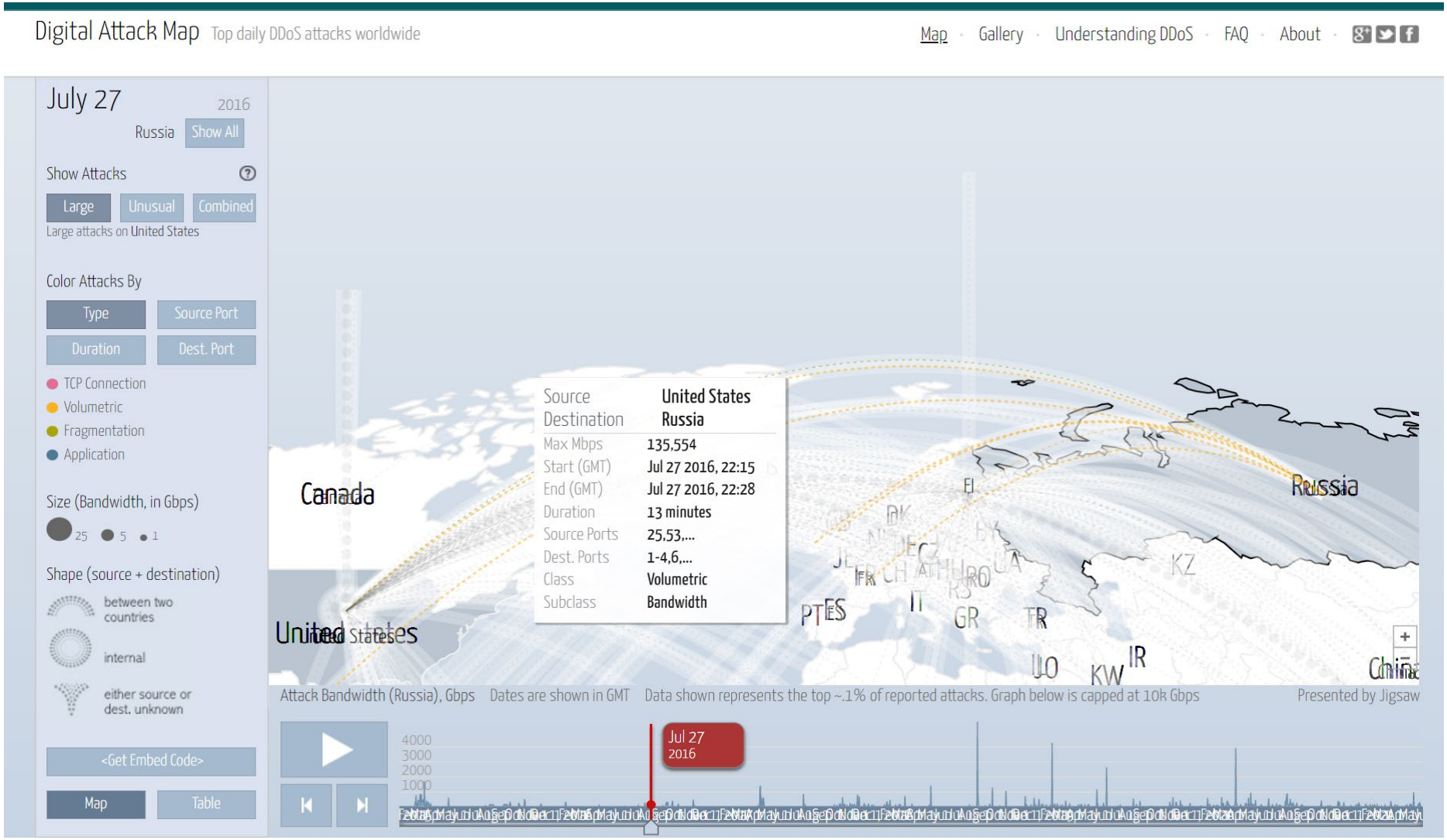
Fuente: Google Ideas, Digital Attack Map, DDoS data 2020, Arbor Networks, Inc.

Figura 14. Ciberataques Rusia- Estados Unidos 2015



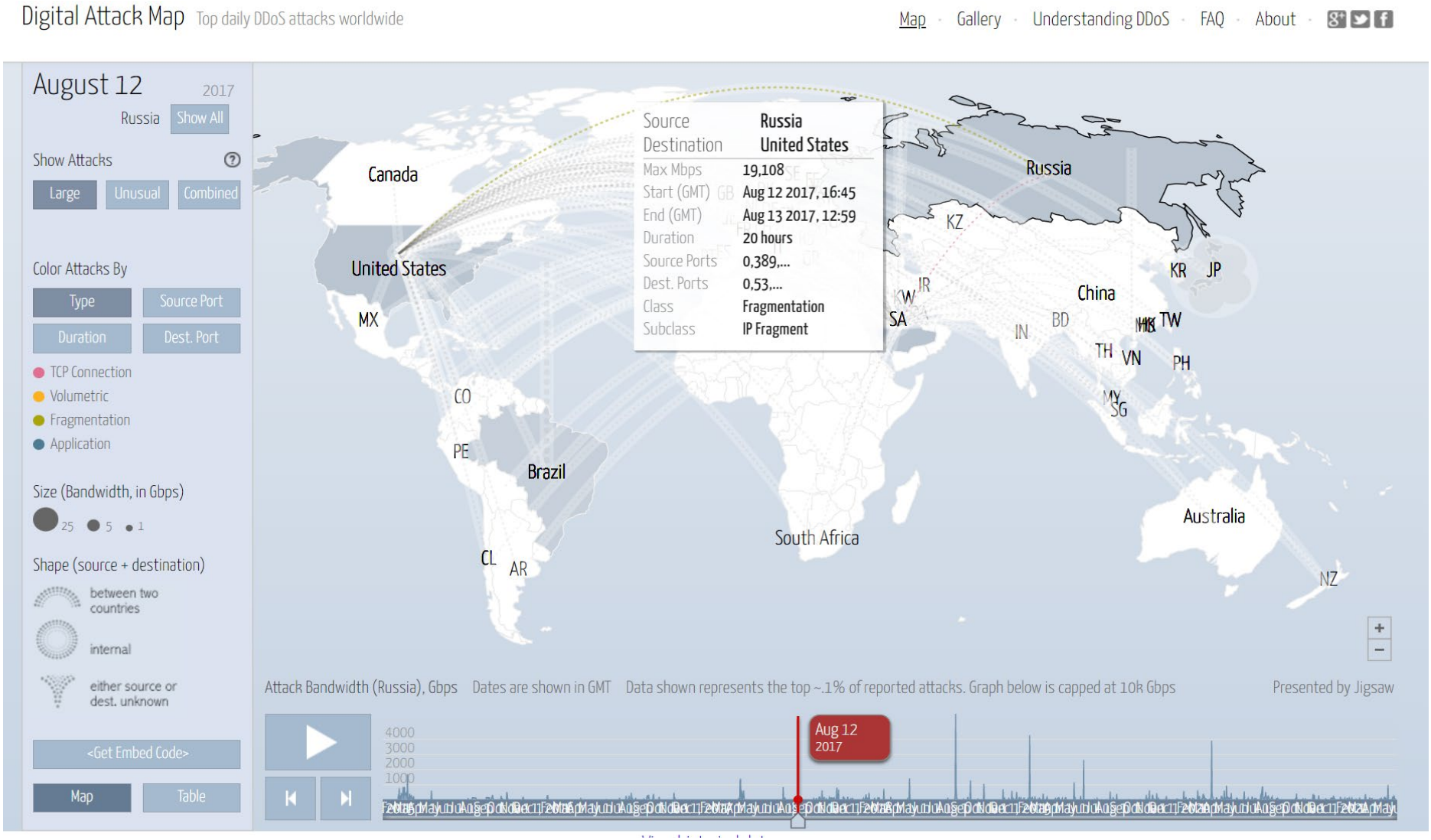
Fuente: Google Ideas, Digital Attack Map, DDoS data 2020, Arbor Networks, Inc.

Figura 15. Ciberataques Rusia- Estados Unidos 2016



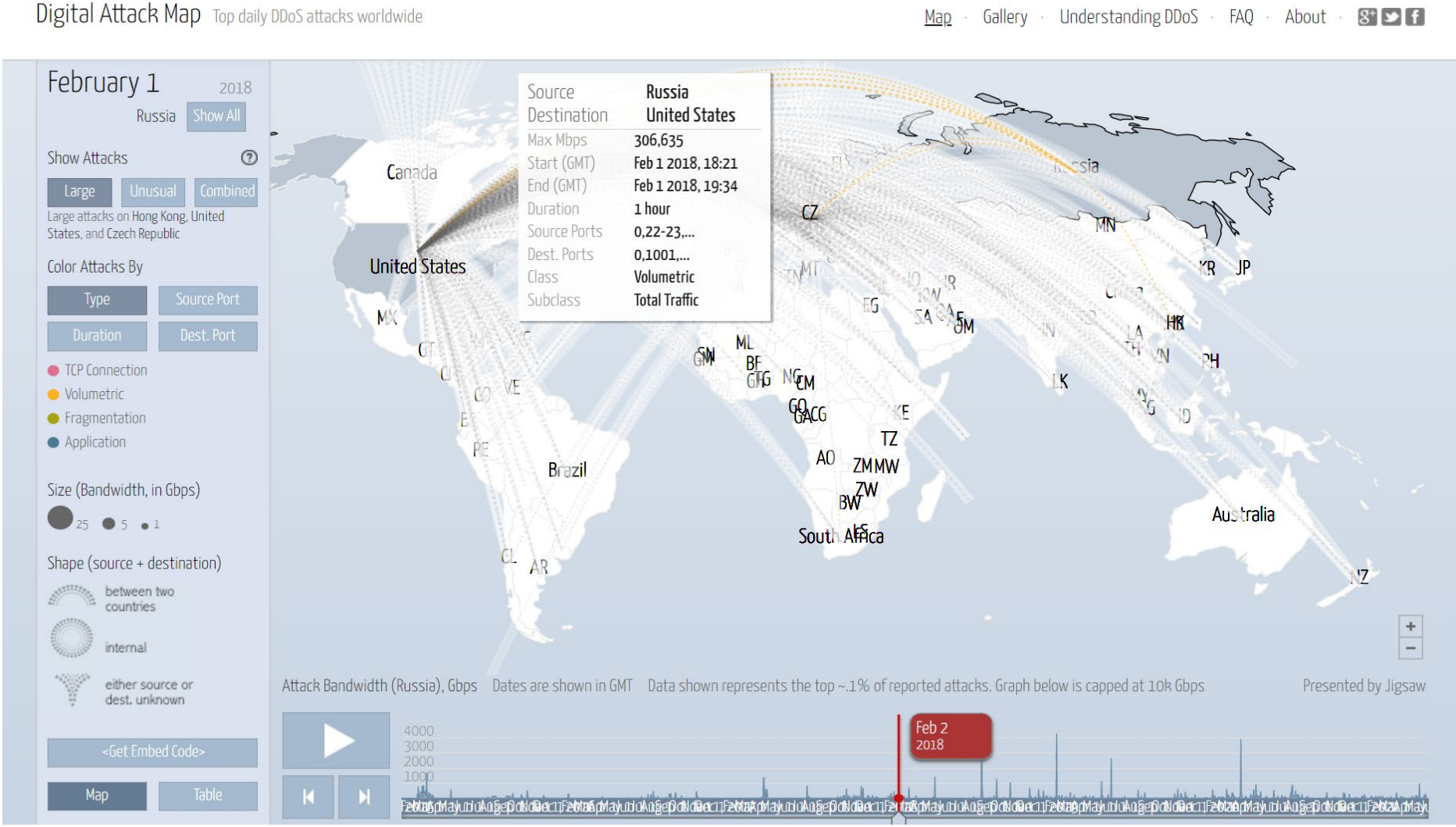
Fuente: Google Ideas, Digital Attack Map, DDoS data 2020, Arbor Networks, Inc.

Figura 16. Ciberataques Rusia- Estados Unidos 2017



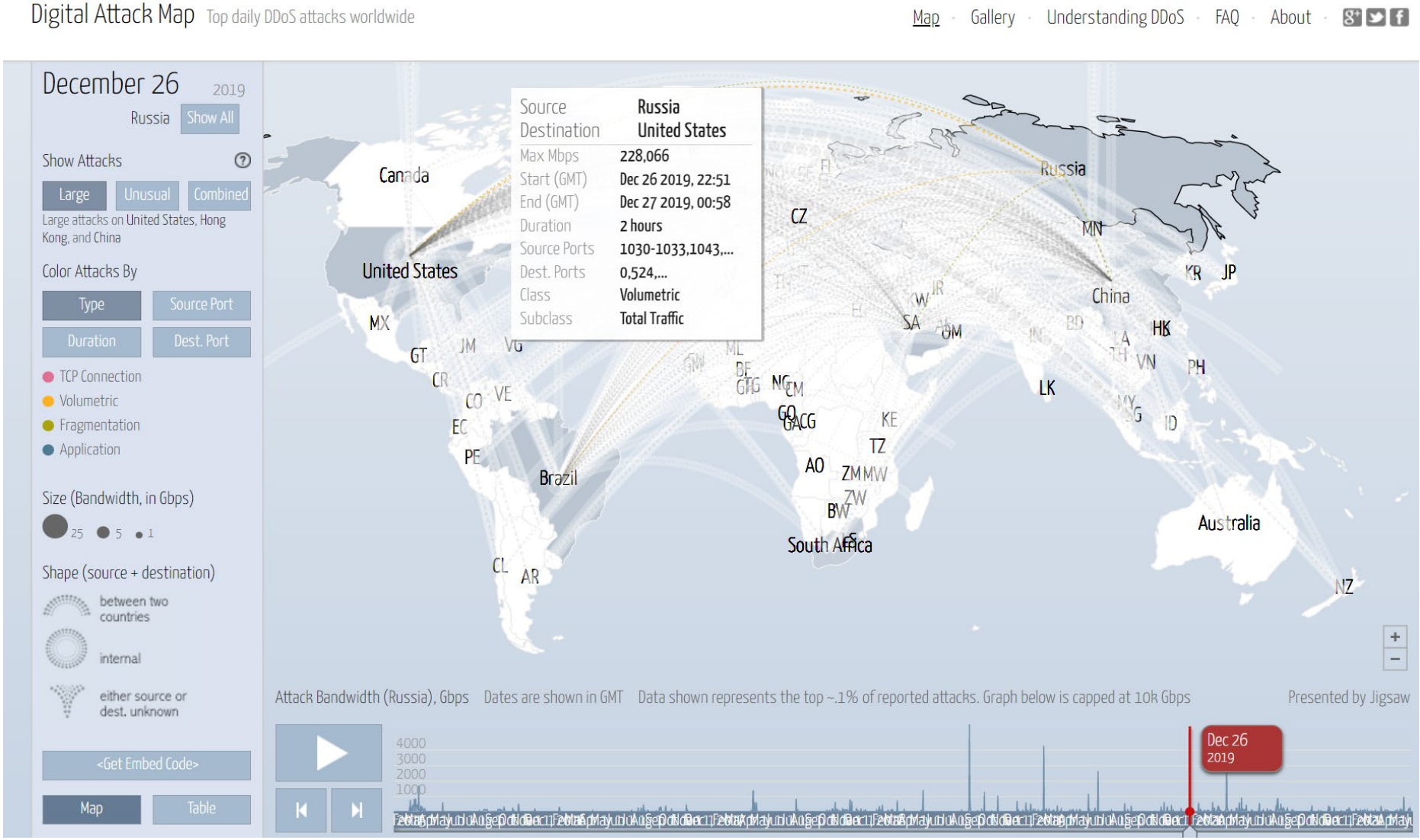
Fuente: Google Ideas, Digital Attack Map, DDoS data 2020, Arbor Networks, Inc.

Figura 17. Ciberataques Rusia- Estados Unidos 2018



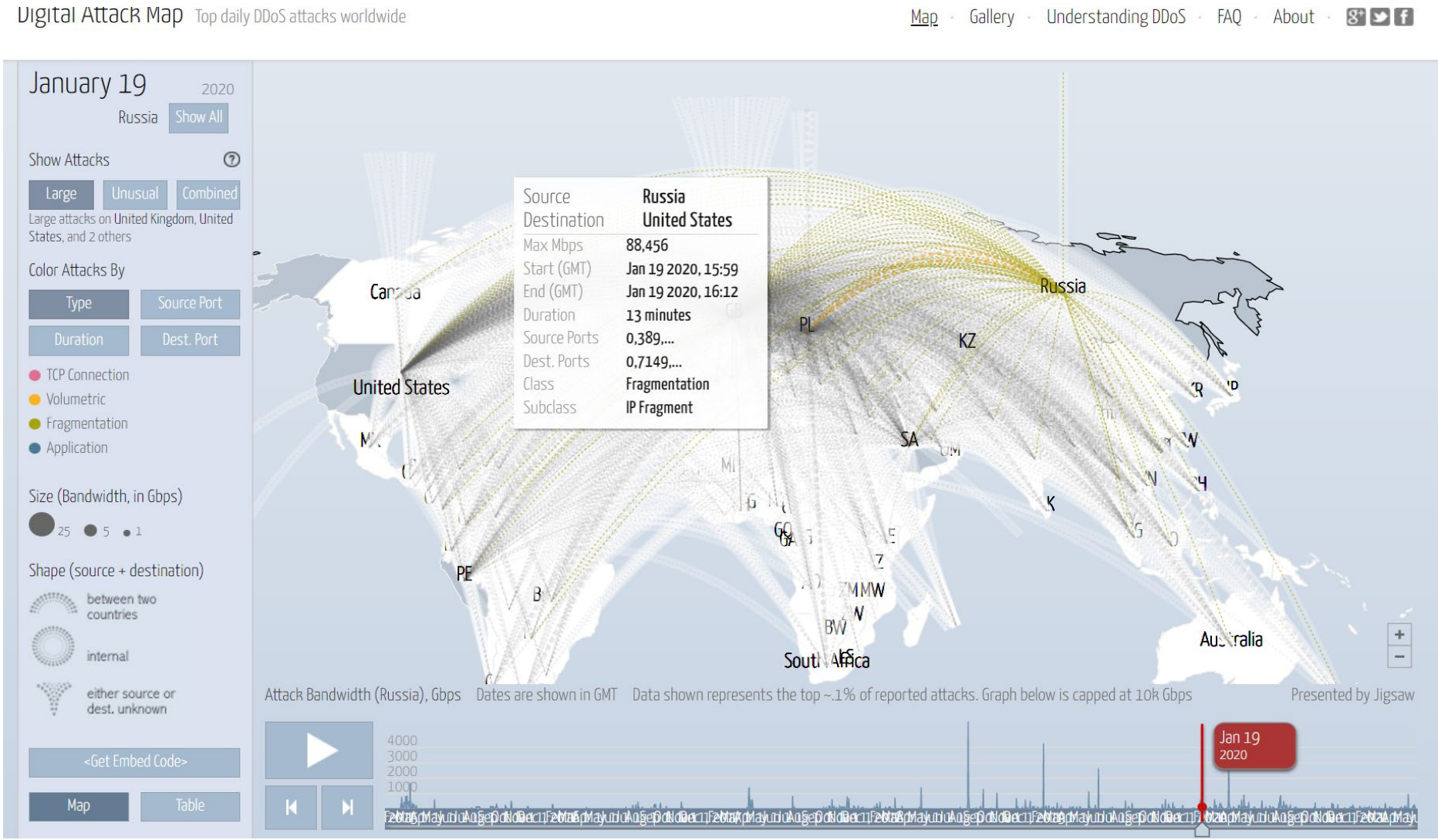
Fuente: Google Ideas, Digital Attack Map, DDoS data 2020, Arbor Networks, Inc.

Figura 18. Ciberataques Rusia- Estados Unidos 2019



Fuente: Google Ideas, Digital Attack Map, DDoS data 2020, Arbor Networks, Inc.

Figura 19. Ciberataques Rusia- Estados Unidos 2020



Fuente: Google Ideas, Digital Attack Map, DDoS data 2020, Arbor Networks, Inc.

Cada una de las imágenes corresponde a los ataques en tiempo real durante el año que se muestra en la esquina superior izquierda. Esto indica de manera gráfica que durante al menos la última década el Estado estadounidense y el Estado ruso han ejercido y recibido ciberataques uno del otro de forma constante. El código de color en el mapa muestra el nivel de riesgo/peligro; el color verde, es para aquellos ciberataques de "fragmentación" lo cual quiere decir que corresponde a *DDoS* (*Distributed Denial of Service*) que afectan los sistemas de control de infraestructuras críticas con mayor facilidad y frecuencia, y el amarillo para los volumétricos, que indican un gran bombardeo de estos ciberataques constantemente.

Frente a la pregunta: ¿Qué indican en conjunto las imágenes?, se puede mencionar que aportan distintas pruebas:

1. Cada año durante los 365 días, tanto Rusia como Estados Unidos, reciben miles de ciberataques que entran dentro de diversas clasificaciones lo cual nos habla de un conflicto constante en el ciberespacio.
2. En paralelo con los ciberataques más importantes (mencionados anteriormente en la tabla), el *Digital Attack Map* también los identifica como puntos altos de tensión dentro de la gráfica temporal y reflejados en los flujos de intercambio en el mapamundi; fortaleciendo así la evidencia de que fueron lanzados los ciberataques desde uno u otro país con dirección a su contraparte. Ejemplo de esos puntos altos de tensión es la imagen correspondiente a 2015 cuando se acusa de empezar las interferencias al partido demócrata por parte de Rusia, el *RussiaGate*, y luego en 2016 año en el que presuntamente el gobierno estadounidense infiltra virus y ciberataques para adentrarse en la red eléctrica y activarlos en algún momento de necesidad; este caso, incluso, lo detecta el *DigitaMap,* pero hasta 2017 se hace pública dicha información y se puede así hacer la correlación de manera retroactiva.
3. Retomando la característica del anonimato y discreción que los ataques cibernéticos tienen, es que el mapa nos muestra aquellos que pueden o no hacerse totalmente visibles en la realidad material pero que han tenido lugar y han sido detectados por la tecnología del mapa. Sin embargo, sí da el referente del

punto geográfico dentro del que se orquestan, para dar pauta a demostrar el flujo de ataques entre los actores involucrados.

4. El mapa también permite ver los ataques no solamente entre EE. UU y Rusia, sino también de otros países que sean aliados de éstos; más visiblemente de Rusia hacia miembros de la Unión Europea, OTAN, G7, G8, etc.

No pasa desapercibido el hecho de que Rusia sea propiamente el actor del que emanan muchísimos ciberataques, no solo a Estados Unidos, pero también a otros países; y aunque no es parte esencial de los objetivos de la investigación, nos permite tener una idea general respecto a la capacidad para realizar ataques cibernéticos en una gran diversidad de países/objetivos.

Con base en las evidencias documentadas y la información sobre la relación bilateral ruso-estadounidense, es que pueden señalarse dos supuestos:

1. En el ciberespacio, la relación de Rusia y Estados Unidos encuentra nuevos elementos a considerar para su implementación en áreas de competencia. Esta reformulación habilita la forma en la que crean y ejercen su política en el quinto dominio con su contraparte, lo cuál también es una búsqueda por la obtención del poder en este espacio. Lo anterior, para Rusia es una oportunidad única para recuperar su posicionamiento en la escena internacional, y para Estados Unidos una oportunidad de reafirmar su influencia en la misma.
2. Debido al perfeccionamiento de las herramientas de innovación tecnológica y la información digitalizada, la confrontación ruso-estadounidense en el ciberespacio, encuentra en la ciberguerra y su gran abanico de agresiones cibernéticas como un canal de enfrentamiento o como un complemento de las prácticas bélicas tradicionales, lo que lleva a considerar un híbrido que va tomando fuerza como alternativas cada vez más recurrentes en los momentos de tensión entre ambos actores.

Si bien los reportes de ciberataques actualmente son más constantes, no han sido formalmente retomados ni publicados con la misma frecuencia con la que estos ocurren, tampoco tratados bajo la trascendencia que pueden llegar a tener en el mundo material. La explicación puede ser, por un lado, que es una estrategia para poder seguir ejerciendo

el ciberpoder con un bajo perfil que no represente una exposición o crítica ante la sociedad internacional. Por el otro lado, eso no exenta que los Estados sepan de la existencia, el riesgo y el significado político que ejercen los ciberataques y, así, tengan un posicionamiento ante ellos.

Cabe destacar que el cuarto punto, está respaldado por el hecho de que miembros de la OTAN son países europeos, los cuales también reciben ciberataques de forma constante. En capítulos anteriores se hizo mención del Convenio del Consejo de Europa de Budapest, el cual contiene el siguiente dato importante:

> Rusia es el miembro más prominente del Consejo que no ha firmado el tratado y Japón no lo ha ratificado todavía. Si bien la Convención se está promoviendo por muchos países europeos, para los Estados Unidos se ve como la mejor opción para asegurar un acuerdo internacional sobre la lucha contra la ciberdelincuencia. [139]

Lo anterior conduce a señalar que también el conflicto cibernético entre ambos debe tomar en cuenta los grupos y organizaciones de los cuales forman parte, tanto EE. UU como Rusia respectivamente ya que, en un escenario de confrontación más fuerte, tendría mayor peso y relevancia su articulación en el conflicto.

Al respecto, también se debe señalar que lo anterior puede responder a la visión pesimista de los preceptos realistas y neorrealistas, respecto a la cooperación internacional y la idealización de esta. Lo anterior se ilustra con la cita anterior; la falta de firma y ratificación de Rusia y Japón respectivamente, así como el aporte poco equitativo de todos los demás miembros y en cuanto a sus capacidades de ciberseguridad de forma individual.

La reconfiguración del concepto que diversos países tienen sobre la guerra o conflicto, actualmente se han visto enriquecidos por la incorporación de elementos cibernéticos, tales como ciberataques o ciberguerra como un híbrido de las estrategias militares de seguridad y defensa. Rusia y Estados Unidos han retomado con fuerza esta reconfiguración posicionándose, después de la caída del Muro de Berlín y el consecuente acomodo que sufrió el escenario internacional, como dos actores predominantes en las relaciones dentro del ciberespacio, con la singularidad característica de ser contrapartes uno del otro. No es un hecho aislado que las Agendas de Seguridad Nacional, de ambos

[139] Op. Cit., Eduardo Leiva, p. 167.

países, cambien sustancialmente al incorporar la ciberguerra y las amenazas cibernéticas en sus protocolos, así como en la creación de dependencias que específicamente atiendan los temas de seguridad en el ciberespacio, y en su relación con otras naciones.

3.3 La relación cibernética ruso-estadounidense actual y posibles escenarios futuros.

Analizar la relación actual entre Rusia y Estados Unidos, debe hacerse con la reserva de no abordarla de forma extremista. Por un lado, se debe entender que el contexto que rodea la interacción entre ambas partes es herencia de fuertes diferencias ideológicas, políticas y sociales, e incluso por ser un referente paradigmático y un parteaguas histórico para todo el mundo. Al retomar los roces que ha tenido dicha relación y que fueron descritos en el apartado anterior, se puede enfatizar que la relación actual involucra elementos en el espacio terrestre, marítimo, aéreo, espacial, y ahora, también, el contexto cibernético de las interacciones entre Washington y Moscú. Como se ha visto, las relaciones entre ambas naciones no son siempre estables y/o sencillas de regular.

No puede iniciarse este apartado sin la consideración de que, la dinámica bilateral también ha comprendido esfuerzos diplomáticos y de cooperación para mantener un balance dentro de la búsqueda del poder de ambos actores con sus respectivas diferencias; es así que lo anterior se establece con la intención de observar ambos aspectos para analizar de forma más equitativa el estatus actual de la relación en general dentro y fuera del ciberespacio, pero también la prospectiva que emane de ambas consideraciones en escenarios futuros.

Las relaciones entre ambos actores decayeron frente al retorno de Vladimir Putin al Kremlin en 2012 debido a su declaración en torno a que los manifestantes que se posicionaron en contra de su regreso al poder habían sido enviados por Hilary Clinton.

En el año 2013 Edward Snowden (consultor tecnológico estadounidense), develó documentos clasificados al gobierno estadounidense, y al cual Putin dio asilo político negándose a las solicitudes de Obama para extraditarlo; situación que generó la cancelación de una cumbre que se había programado para un encuentro diplomático entre los dos.

Recientemente también han ocurrido momentos en los que la cooperación bilateral ha tenido éxito: un referente fue el periodo posterior a los atentados del 9/11, pues Rusia apoyó a Estados Unidos durante la primera etapa de la guerra con Afganistán, al dotarlo de información sobre las acciones bélicas de dicho país en la región de Medio Oriente, y la cual había sido recabada por los sistemas de inteligencia ruso durante aproximadamente diez años de su presencia dentro del país.

Otro ejemplo se suscita entre 2008 y 2012, cuando ambos países cooperaron entre sí para el control de armas en Irán y Afganistán bajo la administración de Barack Obama y Dmitri Medvédev.

Lamentablemente, la presunta injerencia de Moscú en las elecciones presidenciales de Estados Unidos en 2016, y los presuntos intentos de afectar la campaña electoral en 2020, son algunos de los temas que han dirigido e incrementado la atención en Rusia en los últimos años, (no sucedía desde 1950), generando tensión y confusión.

> La interferencia cibernética rusa en las elecciones estadounidenses de 2016 fue el golpe decisivo. Conforme se detalla en el informe de 2019 elaborado por Robert Mueller, una "fábrica de troles" de San Petersburgo trabajaba las 24 horas con el propósito de utilizar las redes sociales para exacerbar la polarización política de la sociedad estadounidense, sembrar dudas en ella en cuanto a la legitimidad de su propia democracia y favorecer a Donald Trump por sobre Hillary Clinton. Asimismo, Rusia intentó acceder a máquinas de votación en algunos estados, lo que aumenta las posibilidades de que su objetivo fuera modificar los resultados de futuras elecciones. La injerencia electoral mediante las redes sociales ha continuado en el ciclo comicial de 2020.[140]

Las tensiones entre Rusia y Estados Unidos se han incrementado por el inicio del conflicto en el sudeste de Ucrania, el apoyo abiertamente expresado a Nicolás Maduro en Venezuela, la anexión de Crimea a su territorio, así como su influencia en la guerra civil en Siria. Algunas reacciones han sido, en primera instancia, que Estados Unidos y sus aliados han optado por imponer sanciones económicas y expulsar a diplomáticos rusos de su territorio, no obstante, los vínculos entre ambos países han pasado a ser

[140] Angela S., *"¿A qué se debe que las relaciones entre Estados Unidos y Rusia sean tan difíciles?"*, Policy 2020 brookings, Vitales para votantes, septiembre 2020. Disponible en: https://www.brookings.edu/es/policy2020/votervital/a-que-se-debe-que-las-relaciones-entre-estados-unidos-y-rusia-sean-tan-dificiles/

mayormente contenciosos, debido a la capacidad de uno y otro para coartar sus intereses nacionales.

Asimismo, debido a su condición de superpotencias nucleares, los dos tienen la responsabilidad de mantener ante cualquier escenario, la estabilidad de sus relaciones; desalentar la proliferación de armas químico-biológicas, etc., y, además, cooperar frente al interés que todos los Estados demandan para enfrentar el cambio climático, el terrorismo, y por supuesto, la pandemia por COVID-19.

A pesar de que la cooperación en temas de interés global abre la puerta para el equilibrio entre las tensiones existentes entre ambos actores, al mismo tiempo proyecta nuevas áreas de competencia. Debido a los efectos por la pandemia COVID-19, el robo de datos, la información e incremento en la contienda por generar una vacuna ante la enfermedad y sus variantes, ha potencializado los ciberataques, virus, *malwares*, *phishing*, etc., entre empresas privadas, Estados, y organizaciones que pertenezcan, o no, a EE. UU y Rusia, específicamente, a pesar de que ya haya otros países involucrados en esta dinámica.

Con base en lo anterior, algunos escenarios futuros en la relación cibernética ruso-estadounidense podrían ser:

- Perfeccionamiento y reformas de ambos países a sus Estrategias de Ciberseguridad y Ciberdefensa que den pauta a imponer una mayor presencia en el ciberespacio, y que demuestre las capacidades de cada uno.
- El endurecimiento de las sanciones económicas impuestas por la UE y la OTAN a Rusia, podrían en consecuencia limitar aún más el intercambio comercial ruso, y afectar la economía del país.
- Estados Unidos podría intentar retomar los ejes principales del “Tratado de Limitación de Armas Estratégicas” (SALT II) que incluye la reducción del armamento nuclear con miras de no caer en una carrera armamentista, ya que actualmente se ve alimentada por la capacidad cibernética de ambos, facilitando así un escenario de vulnerabilidad que sería muy delicado en un escenario de confrontación.

- Rusia, por su parte, podría intentar delimitar y controlar el espacio cibernético en el que se mueve para tener un mejor manejo y vigilancia de aquellos canales que puedan ser vulnerables para penetrar en sus sistemas informáticos y de relevancia nacional.
- De generarse una confrontación entre ambos actores o donde participen en apoyo de algún otro Estado, ambos podrían implementar y/o combinar ciberataques como parte de sus estrategias bélicas.
- Un escenario de negociación también sería factible como una alternativa para la plenitud de los procesos electorales estadounidenses, y la liberación de sanciones económicas para Rusia, siempre y cuando no acontezca algún otro suceso dentro del periodo de negociación que pudiera poner en riesgo la intención de llegar a un acuerdo entre ambas partes, logrando un efecto contrario.

Conclusiones del capítulo.

El recorrido entre las agendas de ciberseguridad de Rusia y Estados Unidos es un claro ejemplo de las diferencias heredadas desde la Guerra Fría, y de las ideologías políticas que cada uno perseguía y aún persigue. La marcada diferencia entre la interpretación que cada Estado da a los conceptos de ciberseguridad empieza por señalar la apropiación de sus concepciones y el manejo de ellas, estableciendo así una visión que dista de homogeneizar la percepción de Oriente con la de Occidente, alrededor del quinto dominio.

Rusia es dentro de su agenda, basto en su diversidad de áreas cibernéticas a las que presta atención, pero al mismo tiempo permisivo en exponer lo que entenderá como ataque o amenaza cibernética y, lo que, en consecuencia, el Estado ruso podría desplegar cibernéticamente para neutralizar, contrarrestar y, de ser el caso, devolver el ataque. A su vez, es particular que la manipulación psicológica (correspondiente a la Primera Generación de la ciberguerra) se encuentre presente dentro de las consideradas ciberamenazas, ya que refleja, directa o indirectamente, lo que Rusia propiamente implementa y/o espera, considerando su papel como uno de los Estados con mayor

señalamiento por la Sociedad Internacional de ser autor de un sin número de ciberataques a lo largo del tiempo.

Por su parte Estados Unidos, se ha encargado de crear un red perfectamente interconectada entre sus instituciones gubernamentales; la estrategia enmarca una organización lineal en cooperación para la ciberseguridad a través de comandos de seguridad cibernética, agencias nacionales que son respaldadas por las leyes en torno a la temática, pero también con el sector privado y civil, siendo una particularidad importante que EE.UU incorpora como forma de atender y entender a la ciberseguridad íntegramente involucrando a diversas dependencias y niveles de la sociedad estadounidense.

El estudio de caso entre estos dos actores arroja elementos valiosos para dar seguimiento y entender la relación que sostienen en el contexto del siglo XXI. Reconocer la herencia que les antecede sienta las bases de las diferencias que marcan la dinámica actual en el ciberespacio. Fundamentalmente, la transición (paulatina hasta el momento) del conflicto al ciberespacio, relativamente “maquillado” por las ventajas de discreción de los ciberataques, ha beneficiado a ambos países al tener acceso a un canal alterno ya sea para ejercer presión, interferir actividad del contrario, para persuadir y condicionar la actividad del otro y, por supuesto, para atacar la infraestructura crítica, a las instituciones etc., que pudieran resultar importantes para los objetivos de uno u otro.

La información que el *Digital Attack Map* proporciona, sintetiza las pruebas necesarias para sustentar que la confrontación en el ciberespacio es una realidad presente desde que la Guerra Fría “tradicional” tuvo lugar. A lo largo de las últimas dos décadas ha sido constante el uso de ciberamenazas y ciberataques entre ambos actores, independientemente de los acontecimientos que han tenido lugar en la realidad material; con mayor o menor intensidad, pero siempre constante por ambas partes. Debido al pasado histórico, las fuertes y contrarias ideologías y políticas que han condicionado el comportamiento de diversos actores internacionales, es que parecería obvio que tanto Rusia como Estados Unidos hubiesen buscado nuevos espacios para continuar con la competencia que implícitamente está presente en diversas áreas de desarrollo e influencia. No obstante, el ciberespacio ha representado más que un espacio de competencia, sino que se ha fortalecido y escala a un nivel mayor, sobre todo en la

diversidad y en el grado de daños que posibilita alcanzar: La oportunidad de llegar a dañar la infraestructura crítica habla de una herramienta altamente poderosa para desestabilizar sectores clave de un Estado, y en consecuencia la pérdida de recursos, economía, población civil, etc., dañando su posición en el mundo también.

Un aspecto sustancial de este apartado es el paralelismo existente entre el *DigitalMap* y la tabla realizada por el Foro Económico Internacional; ya que son instrumentos elaborados por dos instituciones diferentes, y aun así, al contrastar su información, reflejan que coinciden de manera cualitativa y cuantitativa en los momentos clave de tensión política entre ambos actores. Lo anterior, proyecta tanto la escalada de riesgos cibernéticos que comprometen la infraestructura crítica, como el postulado de afirmar que los ciberataques son un medio cada vez más empleado para vulnerar a otros actores en la búsqueda del poder y/o la disuasión.

Finalmente, en lo que concierne a la relación cibernética actual, es de carácter sumamente delicado. Ambos actores tienen una idea general de la capacidad que uno y otro pueden poseer para perpetrar sistemas de relevancia nacional, si en determinado momento se tiene alguna diferencia política, y en concordancia con ello reconocen e implementan cada vez más los canales cibernéticos como espacios de confrontación y componentes importantes de coerción, disuasión y persuasión. Así pues, resulta razonable que las Estrategias de Ciberseguridad y Seguridad Nacional se enfoquen hacia el perfeccionamiento de sus protocolos en el carácter ofensivo y defensivo, considerando importante trasladar su visión e influencia con sus aliados y grupos internacionales que apoyen su posicionamiento para coordinar esfuerzos conjuntos. Que la estabilidad cibernética se mantenga, depende de la negociación diplomática, y de qué conflictos que se gesten en la realidad material no escalen en gravedad para que los ciberataques tomen fuerza como herramientas disuasivas y que perjudiquen la estabilidad estatal rusa o estadounidense.

La relación que Washington y Moscú en la actualidad, particularmente en la esfera cibernética, puntualizan el legado histórico que ha marcado y definido el vínculo entre naciones. Hablar sobre el final de dicha dinámica llena de roces, tensión y competencia sería utópico e incierto, si se toma en cuenta la posición aún hegemónica de ambos países, su zona de influencia y la cada vez más acelerada tecnologización; por lo tal

motivos es necesario dar seguimiento al análisis y estudio no solo de la relación Rusia-Estados Unidos, sino también de otros nexos y actores que van apareciendo con fuerza en el escenario cibernético internacional, para así involucrar el enfoque de Relaciones Internacionales en un espacio cada vez más concurrido.

Sin embargo, también es importante puntualizar que lo anterior se afirma con base en la publicación de documentos y acciones oficiales, aunque en la praxis y trayectoria no-oficial, dentro de este país se han desarrollado prácticas defensivas y ofensivas en otros niveles en momentos anteriores a las fechas en que las estrategias nacionales gubernamentales se han presentado.

Conclusiones

El tratamiento de toda la información a lo largo de este trabajo logró cubrir los objetivos de investigación que en síntesis giraron en torno a: 1) Explicar la influencia que ha tenido la incorporación de las tecnologías de la información y comunicación en el conflicto internacional y el tránsito de los conflictos internacionales a la cibernética en las confrontaciones interestatales; 2) Analizar cómo se construyen y constituyen las agendas de ciberseguridad en Estados Unidos y Rusia, retomando los objetivos e intereses que persiguen en su contenido y aplicación, al igual que los efectos que tiene el tener una agenda de esta naturaleza en la seguridad de dichos países; y 3) Estudiar el conflicto en modalidad de ciberguerra no declarada entre Estados Unidos y la Federación Rusa como una constante, a pesar de la existencia de otros actores internacionales.

La investigación realizada determina que la ciberguerra ha cobrado relevancia bélica en las últimas décadas debido a su bajo costo, precisión, rapidez, letalidad, y capacidad para vulnerar la infraestructura crítica de los Estados. En este sentido, la ciberseguridad es el pilar fundamental en el cual yace el entendimiento y la atención a la seguridad nacional de los Estados como parte de los elementos contextuales en los que se sitúa el mundo, como los bitcoins, inteligencia artificial, digitalización de la información y el almacenamiento de datos.

Se observó que la tecnología por sí misma no ha jugado un papel bueno, o malo, pero tampoco neutral; su presencia influye en la modificación de las concepciones,

dinámicas y comportamiento, en este caso, de los actores internacionales, en la era de la información y las comunicaciones.

En esta línea, la apertura de un amplio abanico de herramientas y vías cibernéticas ha colisionado las prácticas sociopolíticas internacionales, y en menester de esta investigación, incluye las confrontaciones interestatales entendidas desde el nivel de disuasión, hasta el nivel de ataque a infraestructura crítica en un escenario beligerante.

La imbricación de los aspectos de ciberguerra y ciberseguridad en los diversos documentos de seguridad de los países de todo el mundo, son una muestra vigente del alza en las escenas de conflicto cibernético. Independientemente del contexto que condiciona a cada país, valorar lo cibernético como un tópico que no puede ser descartado, dado que el ciberespacio no conoce fronteras, condiciones económicas, o sociales, ningún actor o Estado puede deslindarse de estar en algún aspecto involucrado, dentro de lo que acontece dentro de él y que lo coloca en una posición vulnerable al mismo tiempo.

No obstante, la construcción y constitución de las Agendas de Seguridad Nacional, no en todos los países retoma a la ciberguerra y ciberseguridad de forma directa o al menos dentro de sus objetivos principales para mantener la seguridad integral, lo cual deja una brecha importante por cubrir, considerando que el no atender primordialmente este aspecto en el contexto actual, es no atender de manera sustancial la seguridad nacional.

La transferencia de muchos aspectos de relevancia estatal a la red y la interconexión de datos ha generado que también los temas principales de las Agendas de Seguridad Nacional como economía, hidrocarburos, comercio, transporte etc., se encuentren en canales cibernéticos accesibles que los ponen en riesgo, por lo tanto, priorizar la ciberseguridad es priorizar la Seguridad Nacional de cualquier país.

Paralelamente, es imperativo mencionar que, aunque muchos Estados presuman de tener una Estrategia de Ciberseguridad, esta autora deja la invitación a analizar la calidad, y lo productivas que dichas estrategias son; no es desconocido que México a pesar de tener la Estrategia de Ciberseguridad de 2017, aún se encuentra con carencias muy fuertes en el aspecto de seguridad cibernética, en sus protocolos, en las instancias

que la norman y ejecutan, y por supuesto en sus prácticas. Como es el caso de nuestro país, existen muchos otros con estatus similares.

Se exhorta a ejercer presión para perfeccionar las legislaciones y ciber-legislaciones en aras de la protección del Estado, instituciones y sociedad civil en el marco hipertecnológico, ya que es cada vez más necesario para mantener la seguridad íntegra de las sociedades.

La ciberguerra no declarada abiertamente (y/o pasiva) actual, entre Estados Unidos y la Federación Rusa, atiende a una constante tensión dentro del espacio cibernético, que aun cuando muchos otros actores ya tienen presencia en él, la relación entre estos dos nunca se ha detenido. Además, el reflejo que los ciberataques responden paralelamente a lo que acontece en los escenarios materiales internacionales, y fortalece la idea de que el ciberespacio es actualmente otra área que posibilita la confrontación con elementos que configuran nuevas formas de interacción y conflicto que las esperadas en los espacios tradicionales.

En este sentido es que la hipótesis planteada para esta investigación se cumple, ya que la tensión entre Rusia y Estados Unidos prevalece en el quinto dominio a través de dinámicas de confrontación que se han desplazado al ámbito ciberespacial, hecho que se puede apreciar en la rearticulación de sus agendas de seguridad más recientes, aunque con la reserva de ser todavía un área con un largo trayecto por perfeccionar de manera individual y colectiva. Sin embargo, debido al contexto actual, se preveía que se pondría un particular énfasis en el conflicto cibernético dentro de dichos documentos estatales de seguridad, lo que, al concluir esta investigación, no logramos afirmar, ya que aún es ambiguo el tratamiento de este eje en contraste con otras áreas a nivel Estatal e internacional. Además de que cada vez los países han optado por limitar el acceso a dicha información, lo cual también podría deberse al conocimiento del riesgo que podría implicar, en el contexto ciberespacial, facilitar dichos datos.

Por último, no sólo los Estados tienen la tarea de enfocar y actualizar su visión en torno a los temas cibernéticos, también lo tienen los espacios de producción del conocimiento como lo es la Universidad Nacional Autónoma de México, en este caso, la disciplina de Relaciones Internacionales para que sus egresados tengan una formación actualizada en temas que ya son parte de su propio contexto. Asimismo, se hace

extensivo en diferentes carreras dentro de las cuales el estudio del ciberespacio deberá ser considerado para la formación del profesionista que constituye parte de la sociedad global actual.

Como internacionalistas, debemos aunar por incluir el estudio del quinto dominio como producto y productor de dinámicas sociales, políticas y económicas que influyen en la realidad social que analizamos. Debemos atender dicha realidad en todos sus niveles para dotar de actualidad, la manera en que los egresados de esta universidad comprendemos y estudiamos las relaciones internacionales. Paulatinamente, lo que acontezca en el ciberespacio tendrá que tomarse en cuenta dentro de las teorías, investigaciones y coyunturas de la disciplina, lo cual es menester de la UNAM impulsar en concordancia con su misión de ofrecer una educación de calidad y a la vanguardia de los acontecimientos actuales.

Bibliografía.

- ABAD-QUINTANAL, G.: "*El concepto de seguridad: su transformación*", Revista Comillas de Relaciones Internacionales, Madrid, Universidad Pontificia Comillas, Departamento de Relaciones Internacionales, diciembre 2015, [En línea]:https://www.researchgate.net/publication/291140394_El_concepto_de_seguridad_su_transformacion
- AGNU: *Resolución 68/243.* "*Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional"*, aprobada por la Asamblea General el 27 de diciembre de 2013 en el marco del 68° período de sesiones, publicado por Naciones Unidas el 9 de enero de 2014, A /RES/68/243.
- ÁLVAREZ, Y.: "*La ciberguerra: un futuro muy presente",* Directos rtve noticias, 2013. [En línea]: https://www.rtve.es/noticias/20130616/ciberguerra-futuro-muy-presente/68932 2.shtml.
- ASTIÉ, B. W.: *"Seguridad internacional y diplomacia para la salud global"*, *Revista Mexicana de Política Exterior,* México, núm. 102, septiembre-diciembre 2014, 141-171 pp.
- BRADLEY, K. A.; "*Anatomy of Cyberterrorism Is America Vulnerable"*. United States, Air War College. Air University, 2003. p. 4.
- BARACK, F.: *"¿Puede un ataque cibernético causar una guerra EE. UU.-Rusia?",* The San Diego Union Tribute (en español), Estados Unidos, febrero 2022. [En línea]: https://www.sandiegouniontribune.com/en-espanol/noticias/story/2022-02-14/puede-un-ataque-cibernetico-causar-una-guerra-eeuu-rusia
- BELLAMY, C.: "*The evolution of modern land warfare: Theory and practice",* Londres: Routledge, 2015.
- BILYANA, L.: Cheravitch, J.; *"The Past, Present, and Future of Russia's Cyber Strategy and Forces",* 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade, Tallinn, NATO CCDCOE Publications, 2020, pp. 5-6.
- BONILLA, A.: *"Rusia: Fortalezas y debilidades"*, Revista Problemas del Desarrollo, México, UNAM, Instituto de Investigaciones Económicas, 2012, vol. 43, núm. 171.
- CALVO, G. R. C.: *"Política de Defensa de Japón",* Documento de opinión, Instituto Español de Estudios Estratégicos, España, octubre, 2020, pp. 3-5.

- CALVO, L. A.: Conferencia presentada en el Encuentro Internacional de Seguridad de la Información (ENISE), citado por EGUSKIÑE L. I.: *"Ciberguerra, los Escenarios de Confrontación"*, *Documentos de Opinión*, España, Instituto español de estudios estratégicos, 2014, p. 16.
- CANO, J.:" Ciberseguridad *y ciberdefensa: dos tendencias emergentes en un contexto global".* Colombia, Sistemas Asociación colombiana de ingenieros de sistemas, 2011, 119, 4.
- CARO, M. J.; *"Nuevo concepto de ciberdefernsa de la OTAN"*, Documento informativo del IEEE 09/2011, Instituto Español de Estudios Estratégicos, Ministerio de la Defensa, marzo 2011. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7271583
- CASAR, C. J.R.: (Dir.), *"El ciberespacio. Nuevo escenario de confrontación, México"*, Anuario Mexicano de Derecho Internacional, México, 2014, vol. XIV, 863-868 pp.
- CASASÚS, R.M. y Serrano A. S.: "*La efectividad de la intervención humanitaria en los conflictos armados internacionales del siglo XX y XXI"* (tesis). México, Puebla, Universidad de las Américas. 2016. [En línea]: http://catarina.udlap.mx/u_dl_a/tales/documentos/lde/casasus_ruz_m/
- CARRILLO, C.L. y Deisy P. Vargas C.: "*Ciberguerra: descripción de estrategias políticas internacionales y algunos planteamientos jurídicos para afrontarla",* Bogotá, Universidad Militar Nueva Granada, Facultad de Derecho, 2016, 114 pp.
- CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL; Gabinete de Estrategia Militar, *"Los ámbitos no terrestres en la guerra futura: Espacio",* Monografías del CESEDEN, España-Argentina, núm. 128, 2012.
- CIBERSEGURIDAD GLOBAL, "Expertos reportan una mejora en la ciberseguridad en el mundo", El siglo de Torreón, México, 30 de junio de 2021. [En línea]: https://www.elsiglodetorreon.com.mx/noticia/2021/expertos-reportan-una-mejora-en-la-ciberseguridad-en-el-mundo.html
- CISA Cybersecurity & Infrastructure Security Agency. *Security Tip (ST04-001) What is cybersecurity?* Estados Unidos, noviembre 2019. [En línea]:https://www.cisa.gov/uscert/ncas/tips/ST04-

001#:~:text=Cybersecurity%20is%20the%20art%20of,integrity%2C%20and%20availability%20of%20information. [Consulta: 21 de junio de 2022]

- COLLE, R.: “Internet: un cuerpo enfermo y un campo de batalla”, *Revista Latina de Comunicación Social*, Junio 2000. [En línea]: http://www.ull.es/publicaciones/latina/aa2000qjn/91colle.htm [Consulta: 2 de marzo de 2021].
- COLOM P. G.; “La evolución de la Estrategia de Seguridad Israelí (I)”, *Boletín de Información*, España, Ministerio de la Defensa, 2009, núm. 309, pp. 67-80. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3061967
- COMNINOS. A.: *Una Agenda de Ciberseguridad para la sociedad civil: ¿Qué hay en juego?,* España, Asociación para el Progreso de las Comunicaciones, Temas emergentes, 2013. 11 pp.
- CS, *Resoluciones del Consejo de Seguridad de la ONU*. Organización de las Naciones Unidas. [En línea]: https://www.un.org/securitycouncil/es/content/resolutions [Consulta: 15 de mayo 2022].
- Consejo Europeo, *Ciberseguridad: cómo combate la UE las amenazas cibernéticas,* Consejo de la Unión Europea. Consejo Europeo, abril 2022. [En línea] https://www.consilium.europa.eu/es/policies/cybersecurity/ [Consulta: 15 de mayo de 2022].
- Council of Europe, “Convenio sobre la ciberdelincuencia”, *Serie de Tratados europeos*. Budapest, núm. 185, 23 de noviembre 2001 [En línea para descargar]: https://www.oas.org/en/sla/dil/treaties_agreements.asp https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- DARBY, C. y SEWALL, S.: *Las guerras de la innovación La ventaja tecnológica erosiva de Estados Unidos*, de Foreign Affairs, 2021. [En línea]: https://www.foreignaffairs.com/articles/united-states/2021-02-10/technology-innovation-wars?utm_medium=email_notifications&utm_source=reg_confirmation&utm_campaign=reg_guestpass [Consulta: 20 de febrero 2021]
- DEPARTAMENTO DEL PRIMER MINISTRO; Gabinete, *Prioridades de inteligencia y Seguridad Nacional,* Nueva Zelanda, 2018, Disponible en:

https://dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security-and-intelligence-priorities

- DERBYSHIRE, Y.: Márquez, R.; "Cronología de la relación entre Rusia y Estados Unidos: la Guerra Fría que no acaba", *El Confidencial*, España, febrero 2022. Disponible en: https://www.elconfidencial.com/mundo/2022-02-24/cronologia-rusia-estados-unidos-guerra-fria_3368345/
- DESQBRE*: Unidad 1. Módulo 3. Los cinco objetivos para la UE en 2020, Introducción a la estrategia Europa 2020 y H2020,* España, Fundación Andaluza para la divulgación de la innovación y el conocimiento*,* 2019.
- El ciberataque de escala mundial y "dimensión nunca antes vista" que afectó a instituciones y empresas de unos 150 países, *BBC NEWS*, Sección "Mundo", mayo 2017. [En línea]: https://www.bbc.com/mundo/noticias-39903218 [Consulta: 17 de mayo 2022].
- ECHEVERRI, M. L. M.: *La relación de la ciberguerra con la guerra interestatal Clásica: estudio de caso Estonia, Georgia e Irán* (tesis). Bogotá, Universidad Militar Nueva Granada, 2016. [En línea]: https://repository.unimilitar.edu.co/bitstream/handle/10654/15363/EcheverriMart%C3%ADnezLauraMilena2016.pdf?sequence=2 [Consulta: 20 de febrero 2021]
- ECHEVERRÍA J. C.: "Las Prioridades Estratégicas de Irán", *Revista General de Marina,* España, Armada de la Defensa Española, Año 2020, Vol. 279, diciembre 2020, pp. 925-933.
- FATTON, L.: "Japan's Space Program: Shifting Away from Non-Offensive Purposes?", *Asie Visions*, Nº115, IFRI, July 2020.
- FEDERACIÓN RUSA, *Estrategia de Seguridad Nacional de la Federación Rusa*, 31 de diciembre de 2015, Texto original. [En línea]: dhttp://static.kremlin.ru/media/events/files/ru/l8iXkR8XLAtxeilX7JK3XXy6Y0AsHD5v.pdf
- FERRERO, JULIO A.: "La ciberguerra. Génesis, y evolución", *Revista General de Marina,* Madrid, España, Ministerio de Defensa, Vol. 264, enero-febrero 2013, 200 pp.

- FERRERO, MARIANO J.: *"La ciberguerra en el marco de la preocupación por la seguridad internacional en las sociedades hiperconectadas contemporáneas"*, *Serie Estudios*, Chile, Biblioteca del Congreso Nacional de Chile, marzo 2015, núm., 02-15, 20 pp.
- FOJÓN, E. y HERNÁNDEZ, A.: "Riesgos del ciberespacio", *Estudios de Política Exterior*, 2014. [En línea]: https://www.politicaexterior.com/basicospolext-riesgos-del-ciberespacio/ [Consulta: 2 de marzo de 2021]
- FONSECA, E. y PEDORMO, L.: "El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra". *Revista de la ESG*, No. 588, 2014,17 pp.
- FORBES STAFF, *"*OTAN ve a Rusia responsable de ciberataque a EU y apoya sanciones", *Forbes México, Internacional*, abril 2021. [En línea]: https://www.forbes.com.mx/otan-rusia-responsable-ciberataque-eu-sanciones/ [Consulta: 25 de julio de 2022].
- FOXALL, A.; "Putin´s Cyberwar: Russia´s Statecraft in the Fifth Domain", *Policy paper,* England, Russia Studies Centre, 2016, núm. 9. 15 pp.
- FRETT, N.: ¿Qué es un ciberataque? *AUDITOOL; Red Global de Conocimientos en Auditoría y Control Interno*, 2015 [En línea]: https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque [Consulta: 22 de febrero de 2021].
- GAITÁN R. A.; *Ciberguerra: La consolidación de un nuevo poder en las relaciones internacionales contemporáneas*. Bogotá: Universidad de Santo Tomás, 2018, 209 pp.
- GAITÁN R. A.; "La ciberguerra y sus generaciones: un enfoque para comprender la incidencia de las TIC en la guerra regular", *Revista Científica de Estudios en Seguridad y Defensa,* España, Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacionales, Vol. 7, núm. 13, 2012, pp. 1-2.
- GASPERIN, R.: "Adolescencia y ciberespacio", *Revista OEI, Monografías virtuales: ciudadanía, democracia y valores y sociedades plurales*. Línea temática: Valores y TICs, Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura, 2005, núm. 5.
- GIBSON, W.: *Neuromance*r, Nueva York, United States. Ace Books, 1984, 352 pp.

- GILES, K.: *Handbook of Russian information warfare*. Roma: NATO Defence College, 2016. [En línea]: http://www.ndc.nato.int/download/downloads.php?icode=506
- GOBIERNO DE AUSTRALIA; Departamento del Primer Ministro y Gabinete, *Estrategia para la Seguridad Nacional de Australia*, Australia, 2013, [En línea]: https://www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf
- GOBIERNO DE EGIPTO: *Fundamentos de la Política Egipcia*, Egipto, Servicio de información estatal, 2019, Disponible en: https://www.sis.gov.eg/section/0/52?lang=en-us
- GOBIERNO DE ESPAÑA, CONSEJO DE SEGURIDAD NACIONAL, *Estrategia de Seguridad Nacional. Un proyecto compartido de todos y para todos*, España, Presidencia del Gobierno, 2017, 128 pp. [En línea]: https://www.defensa.gob.es/Galerias/defensadocs/Estrategia_Seguriad_Nacional_2017.pdf
- GOBIERNO DE MÉXICO: *Estrategia Nacional de Seguridad Pública* (Resumen del documento presentado por el Presidente de la República al Senado de la República) 2019-2024. [En línea]: https://www.dof.gob.mx/nota_detalle.php?codigo=5560463&fecha=16/05/2019 [Consulta: 25 de julio de 2022].
- GOBIERNO DE PAPÚA NUEVA GUINEA: *Política de Seguridad Nacional, Capítulo 6, Metas y estrategia de implementación de la política,* Papúa Nueva Guinea, 2013. [En línea]: https://www.aspistrategist.org.au/wp-content/uploads/2014/08/2013-PNG-National-Security-Policy.pdf Traducción del inglés al español realizada por Mariana Corona Fragoso.
- GOBIERNO DE LA REPÚBLICA POPULAR CHINA: "Ley de Seguridad Nacional de la República Popular China (Orden del Presidente No. 29), Xinhua, China", *Agencia de noticias*, 2015. Disponible en: http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm?fbclid=IwAR0MVdm5gjVFplGrVExHMSdjZyDD37tkd_4n_cCLEz5v_Z9P1FOLkT6dCMI
- GÓMEZ LL. D. A.: *Análisis del ciberataque para la seguridad de los estados y su incidencia en la transformación del status quo: Stuxnet el virus informático,*

Bogotá, Colombia, Universidad Colegio Mayor de Nuestra Señora del Rosario, Facultad de Relaciones Internacionales, 2017.

- GOOGLE IDEAS, Digital Attack Map, DDoS data 2020, Arbor Networks, Inc.
- GUTIÉRREZ, L. A.: "Evolución de la tecnología militar y "su impacto" en España", *Cuadernos de Estrategia*, España, 1995, p 85.
- HENRY, R. y Peartree C. E, *"Military theory and information warfare"*, Parameters, Center for Strategic & International Studies, 28, 1998, 121-135 p.
- HERNÁNDEZ, S.: "La teoría del realismo estructuralista y las interacciones entre los estados en el escenario internacional", *Revista Venezolana de Análisis de Coyuntura,* Venezuela, 2008.
- HIGUERA, J.: ¿Ciberguerra ó Ciber-seguridad?, *Tecnología Militar*, Vol. 35 ISSUE, 2013, núm. 3.
- HIPERDERECHOS: "Una breve historia de la ciberseguridad importada", *Derechos Digitales. Derechos Humanos y Tecnología en América Latina*, Chile, julio 2018. Disponible en: https://www.derechosdigitales.org/12329/una-breve-historia-de-la-ciberseguridad-importada/
- ICA Sistemas y Seguridad: *Los 9 tipos de ciberataque que deberías conocer*, España, Grupo ICA. Información y Comunicación Avanzada, s.a., [En línea]: https://www.grupoica.com/blog/-/blogs/9-tipos-ciberataque-debes-conocer [Consulta: 17 de mayo de 2022].
- IBARRA, V. y NIEVES, M.: "La seguridad internacional determinada por un mundo on-line: el Estado ante el desafío del terrorismo y la ciberseguridad", *Memorias del VIII Congreso de Relaciones Internacionales*, Argentina, Universidad Nacional de la Plata, 2016. [En línea]: http://sedici.unlp.edu.ar/handle/10915/58156 [Consulta: 21 febrero 2021]
- Information Systems Audit and Control Association: Ciberseguridad. *Newsletter.* 24 de noviembre 2017. [En línea]: *https://www.interempresas.net/Ciberseguridad/Articulos/204693-Ciberseguridad.html*
- INTERNATIONAL: *Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales,* LAWi, 20 de abril de 2018. [En línea]

https://leyderecho.org/convencion-de-la-union-africana-sobre-ciberseguridad-y-proteccion-de-datos-personales/ [Consulta: 15 de mayo de 2022].

- INTERNATIONAL TELECOMMUNICATION UNION; Global Cybersecurity: Index 2020 [en línea], 155 pp., Switzerland., 2021.
- INTERNATIONAL TELECOMUNICATIONS UNION, "Countries ramp up cybersecurity strategies", Press Release ITU, 29 de junio de 2021. Disponible en: https://www.itu.int/en/mediacentre/Pages/pr06-2021-global-cybersecurity-index-fourth-edition.aspx
- KÁNDIKO, U.L.: "¿Qué países son los mejores en ciberseguridad?", *CXOCommunity Latam*, 2020 [En línea]: https://www.cxo-community.com/2017/07/que-paises-son-mejores-en-ciberse guridad.html [Consulta: 23 de octubre de 2020].
- KASPERSKY-GREAT: "Gauss: Troyano bancario se utiliza en el espionaje cibernético gubernamental", *SECURELIST- Kaspersky*, Rusia, Kaspersky Company Account, 13 de agosto de 2012. [En línea] http://www.viruslist.com/sp/weblog?weblogid=208188666 [Consulta: 15 de mayo de 2022].
- KEOHANE, R. y Nye, J.: *Poder e Interdependencia,* 3ra edición. Nueva York: Longman, 2000.
- LA VARGUARDÍA, "*El G7 adopta un marco común para prevenir ciberataques al sector financiero",* LA VANGUARDÍA*,* Sección Economía, G7 Finanzas, Barcelona, España, 12 octubre 2016. Disponible en: https://www.lavanguardia.com/politica/20161012/41937750211/el-g7-adopta-un-marco-comun-para-prevenir-ciberataques-al-sector-financiero.html
- LEIVA E., *"Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local"*, Revista Latinoamericana de Ingeniería de Software, Vol. 3, núm. 4, Argentina, 2015, pp. 161-176.
- LEIVA V. R.: La ciberguerra; sus impactos y sus desafíos. Cap.1. Aparece la ciberguerra, Chile, Centro de Estudios Estratégicos de la Academia de la Guerra. Ejército de Chile, 2018.

- LEJARZA I. E.: *Ciberguerra, los escenarios de confrontación*, España, Instituto Español de Estudios Estratégicos, 2014, 20 pp.
- LI: Z Different Values but Similar Visions for Cyberspace, Retrieved, China-US *Focus Magazine,* 16 de enero 2018. Disponible en: https://www.chinausfocus.com/peace-security/different-values-but-similar-visions-for-cyberspace
- Lilly B. & Cheravitch J.: *The Past, Present, and Future of Russia's Cyber Strategy and Forces,* Tallinn, 2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade,© NATO CCDCOE Publications, 2020, pp 27.
- LOPÁTEGUI T. M. A.; Corona F. M.: *"Las amenazas a la ciberseguridad en América del Norte y la capacidad de respuesta regional: un análisis comparado institucional*", Amenazas a la seguridad en el siglo XXI, en el marco del Proyecto PAPIIT IN307018, México, UNAM, octubre 2021.
- *Los 5 mayores ciberataques de la historia*, Reino Unido, Deloitte. [En línea]: https://www2.deloitte.com/es/es/pages/risk/articles/los-cinco-mayores-ciberataques-de-la-historia.html [Consulta: 17 de mayo de 2022].
- Manotas, V.M.C. y Irina Burgaentzle J.: Las Guerras Cibernéticas en el Derecho Internacional Humanitario: Aplicación de los Principios Rectores del Derecho Internacional Humanitario, *LAW Review*, Ecuador, USFQ, Vol. 8, No. 1, mayo de 2021, pp. 71-86. [En línea]: https://revistas.usfq.edu.ec/index.php/lawreview/article/view/2162/3036 [Consulta: 4 de mayo de 2021].
- McGUINNESS, D.: Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país, Sección "Mundo", *BBC NEWS,* mayo 2017. [En línea]: https://www.bbc.com/mundo/noticias-39800133 [Consulta: 17 de mayo 2022].
- MILOSEVICH-JUARISTI M.: *Mapa de la presencia e influenciade Rusia en el mundo desde el año 2000*, Real Instituto elcano, Futuro de Europa, noviembre 2020. [En línea]: https://www.realinstitutoelcano.org/documento-de-trabajo/mapa-de-la-presencia-e-influencia-de-rusia-en-el-mundo-desde-el-ano-2000/ [Consulta: 25 de julio 2022].

- MINISTERIO DE ASUNTOS EXTERIORES. Unión Europea y Cooperación, Oficina de Información Diplomática: *Estados Unidos*, marzo 2022, 23 pp.
- MINISTERIO DE ASUNTOS EXTERIORES. Unión Europea y Cooperación, Oficina de Información Diplomática: *Rusia,* abril 2021, p.20.
- MINISTERIO DE LA DEFENSA DE FRANCIA: *Guerra Cibernética*. Le Livre blanc sur la défense et la sécurité nationale., XXXIII Curso de Defensa Nacional, CESEDEN, 2013.
- MINISTERIO DE DEFENSA DE LA REPÚBLICA DE INDONESIA: *Libro Blanco de Defensa, Capítulo 4 Política, estratégica y manejo de la Defensa Nacional,* Indonesia, 2015. [En línea]: https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIA-DEFENCE-WHITE-PAPER-ENGLISH-VERSION.pdf (Traducción del inglés al español realizada por Mariana Corona Fragoso)
- MINISTERIO DE LA DEFENSA DE LA REPÚBLICA DE KENIA: *Libro Blanco de la Defensa*, Kenia, 2017. [En línea]: https://mod.go.ke/download/national-defence-policy/
- MIRA MILOSEVICH, en S/A, *Cómo Putin logró restaurar el estatus de Rusia como potencia global tras el colapso de la URSS hace 30 años*, BBC News, Mundo, diciembre 2021. [En línea]: https://www.bbc.com/mundo/noticias-internacional-59671737
- MIZRAHI, D.: Joe Biden vs Vladimir Putin: cómo y por qué va a crecer el conflicto entre Estados Unidos y Rusia con el cambio de mando en Washington, *INFOBAE,* E.E.U.U, diciembre 2020. [En línea]: https://www.infobae.com/america/eeuu/2020/12/26/joe-biden-vs-vladimir-putin-como-y-por-que-va-a-crecer-el-conflicto-entre-estados-unidos-y-rusia-con-el-cambio-de-mando-en-washington/ [Consulta: 25 de julio 2022].
- MONAGHAN, A.: *The New Russian Foreign Policy Concept: Evolving Continuity,* Londrés, Chatham House, abril 2013,8 pp. [En línea]: https://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0413pp_monaghan.pdf [Consulta: 19 de mayo 2022].
- MI5, The Threats: Cyber. Reino Unido, https://www.mi5.gov.uk/cyber

- NAVARRETE F.; "*Los ámbitos no terrestres en la guerra futura: Espacio",* Anu. Mex Der. Inter. España-Argentina, Monografías del CESEDEN, vol. 14, 2014. pp. 869-874. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542014000100028&lng=es&nrm=iso
- NEZAVISIMAYA GAZETA, President of Russia, "Ob utverzhdenii doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii [On Approving the Doctrine of Information Security of the Russian Federation]." Mayo12, 2016, http://kremlin.ru/ acts/bank/41460/page/1
- NIETO M. I.: *Las relaciones Estados Unidos- Rusia en la era Trump,* Madrid, Universidad Complutense de Madrid, Revista UNISCI Journal No. 48, octubre 2018.
- NOVOSTI, RIA: *"Diez acontecimientos internacionales más importantes para Rusia en 2007", Sputnik News*, enero 2008. [En línea]: https://sputniknews.lat/20080102/94167528.html.
- Nye, S. J.: "*Cyber Power,* United States, Belfer Center for Science and International Affairs", Harvard Kennedy School, 2010.
- OLLERO D., J.*, "El peligroso grupo de hackers (y espías) que pone contra las cuerdas a gobiernos de medio mundo",* EL MUNDO, Madrid, España, junio 2021. [En línea]: https://www.elmundo.es/tecnologia/2021/06/02/60b0f3d4fdddffaa818b45a9.html
- ORGANIZACIÓN DE LAS NACIONES UNIDAS: "*Asamblea General Plenaria".* [En línea]: https://www.un.org/es/ga/sessions/regular.shtml
- ORGANIZACIÓN DE LAS NACIONES UNIDAS; Consejo de Seguridad: "*Resoluciones del Consejo de Seguridad de la ONU*. Naciones Unidas". [En línea]: https://www.un.org/securitycouncil/es/content/resolutions
- ORGANIZACIÓN DE LOS ESTADOS AMERICANOS: "*Programa de Ciberseguridad"*, Comité Interamericano contra el Terrorismo. [En línea] https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp [Consulta: 15 de mayo de 2022].

- ORTEGA, R.: "El ciberespacio, nuevo escenario de confrontaciones*", América Latina en movimiento*, 2020 [En línea]: https://www.alainet.org/es/articulo/210027.
- PANKOV. N.: "*Los objetivos de ExPetr son empresas importantes", Kaspersky Daily,* junio 2017. [En línea]: https://www.kaspersky.es/blog/expetr-for-b2b/13617/.
- PASCUAL, M.G.: *"El Kremlin da el primer paso para aislar el internet ruso del resto del mundo", El País,* Tecnología, España, marzo 2022. [En línea] https://elpais.com/tecnologia/2022-03-12/el-kremlin-da-el-primer-paso-para-aislar-el-internet-ruso-del-resto-del-mundo.html
- PÉREZ DE LÓPEZ C.: "*El poder de todas las rusias: la influencia de la identidad eslava y la identidad contrastiva sobre la política exterior de la Federación Rusa*". (Tesis Profesional). Recuperada de: Universidad Pontificia Comillas de Madrid, 2015. [En línea]: https://repositorio.comillas.
- PÉREZ, S. G.; *"Hacia una tecnología socialmente significativa"*, *en* SANTOS, M. J. y De Gortari, R. (coords.) *"Computadoras e Internet en la biblioteca pública mexicana",* México, UNAM, IIS- Pearson 2009, 30 pp.
- PODER EJECUTIVO; Ministerio de Defensa de Uruguay: *"Propuesta de Política de Defensa Nacional, Decreto N°371/020"*, Diario Oficial, Montevideo, Uruguay, Centro de Información Oficial, núm. 30 599, 7 de enero de 2021. [En línea]: https://www.impo.com.uy/bases/decretos-originales/371-2020
- RAMÍREZ M. D.: *"La visión internacional de la ciberseguridad",* Documento informativo, España, Instituto Español de Estudios Estratégicos, 2015, núm. 02. [En línea]: www.ieee.es/Galerias/fichero/docs_informativos /2015/DIEEEI02-2015_VisionInternacional_Ciberseguridad_DRM.pdf
- Rand Corporation (s.f.) "*Cyber Warfare",* RAND Corporation. [En línea]: http://www.rand.org/topics/cyber-warfare.html
- Real Academia Española: "*Diccionario de la lengua española,* 2021". [En línea]: https://dle.rae.es/guerra
- REGUERA, J.: "*Aspectos legales del ciberespacio. La Ciberguerra y el Derecho Internacional Humanitario"*, España, Grupo de Estudios de Seguridad Internacional, 2015. [En línea]

http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario.

- REYNA R. D.; Olivera G. D. A.: *"Las amenazas cibernéticas, 10 Temas de Ciberseguridad"*. Veracruz, México, Editorial Universidad de Xalapa, 2017, pp. 49-72.
- RIZZI, A.*: "¿Quién tiene más ciberpoder? Una radiografía de las capacidades de EE UU, China, Rusia y otras potencias*", El País, Sección "Internacional", enero 2022, [En línea]: https://elpais.com/internacional/2022-01-30/quien-tiene-mas-ciberpoder-una-radiografia-de-las-capacidades-de-ee-uu-china-rusia-y-otras-potencias.html.
- RODRÍGUEZ S. L. G.: *"Antiguas y nuevas amenazas a la seguridad de América Latina",* Revista Bien Común, México, Vol. XIII No. 152, 2007, pp. 15-18.
- RODRÍGUEZ, T.: "*Los usos de la teoría de la guerra de Carl von Clausewtiz en el concepto de lo político de Carl Schmitt. A propósito de la guerra como continuación de la política por otros medios"*, en: IPAR E.; Tonkonoff, S.: *Teoría, política y sociedad: reflexiones críticas desde América Latina*. Argentina-Estados Unidos, CLACSO, 2018, 831 pp.
- ROMERO, G. J.: *"Conceptualización de una Estrategia de Ciberseguridad para la Seguridad Nacional de México"*. Revista Internacional de Ciencias Sociales y Humanidades, México, Universidad Autónoma de Tamaulipas, 2018, vol. XXVIII, núm. 2.
- RUBIO, R.: "*Las Relaciones Internacionales en el Tránsito al Siglo XXI".* Cuadernos de la Escuela Diplomática de España, Madrid, Ministerio de Asuntos Exteriores y de Comunicación, Escuela Diplomática de España, 2011, 44 pp. [En línea]: http://www.rafarubio.es/wp-content/uploads/ciberdiplomaciaintro.pdf
- SÁEZ, C. L.: "*La Ciberguerra en los Conflictos Modernos"*, Santiago, Chile, Fuerza Aérea Chile, 2012, FACH, 2012.
- SAMPAIO, F. "*Ciberguerra: guerra eletrônica e informacional, um novo desafio estratégico".* Organização para Estudos Científicos (OEC). Escola Superior de Geopolítica e Estratégia. Porto Alegre, Brasil, 2001.
- SBARAGLIA G.*, "Ciberguerra: la guerra cibernética entre Estados. Casos famosos",* Cesena, Italia, FlashStart Internet Protection, marzo 2022. [En línea]:

https://flashstart.com/es/ciberguerra-la-guerra-cibernetica-entre-estados-casos-famosos/.

- SÁNCHEZ, G.: *"El ciberespionaje".* Derecom, Nueva Época, 2013, núm. 13, marzo-mayo, 115 p. [En línea para descarga]: https://www.academia.edu/7414397/El_ciberespionaje.
- SÁNCHEZ, G.: *"Los Estados y la Ciberguerra",* Revista Boletín de Información, España, Universidad Complutense de Madrid, 2010, núm. 317, pp. 63-76 pp. [En línea para descarga]: https://dialnet.unirioja.es/servlet/articulo?codigo=3745519
- SCOTT, D.: "*Applegate, The Dawn of Kinetic Cyber"*. 5th International Conference on Cyber Conflict, Tallin, Estonia, Publicaciones del CCD COE de la OTAN, 2013, p 5. [En línea]: https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf
- SILES I.: "*Cibernética y sociedad de la información: el retorno de un sueño eterno"*, Signo y Pensamiento, 2007, 26 (50), pp. 84-99.
- SMITH, G. S.; *"Recognizing and preparing loss estimates from cyber-attacks.",* Information Systems Security, 2004, Vol.12 (Issue 6), pp. 46-57.
- SNOW J. *"Top 5 de los ciberataques más memorables"*, Kaspersky, noviembre 2018. Disponible en: https://goo.su/LRZF42.
- SORENSEN, M.; *"Manual of International Law"*, New York: St. Martin's Press, 1998, 771 pp.
- STENT. A.: *"¿A qué se debe que las relaciones entre Estados Unidos y Rusia sean tan difíciles?"*, Policy 2020 brookings, Vitales para votantes, septiembre 2020. [En línea]: https://www.brookings.edu/es/policy2020/votervital/a-que-se-debe-que-las-relaciones-entre-estados-unidos-y-rusia-sean-tan-dificiles/
- SWEDISH ARMED FORCES: [En línea]: https://www.forsvarsmakten.se/en/
- S/A: *"La ciberguerra ruso-estadounidense acaba de empezar"*, *Deutsche Welle*, Sección Mundo, marzo 2019. [En línea]: https://www.dw.com/es/la-ciberguerra-ruso-estadounidense-acaba-de-empezar/a-47748659.
- TORRES, S. M.: *"Los Dilemas Estratégicos de la Ciberguerra",* Revista Ejército, España, núm. 839, marzo 2011, pp. 14-19.

- TORRES, W. C.: "*Las teorías tradicionales de las Relaciones Internacionales",* Centro Iberoamericano de Estudios Internacionales, México, 2017. [En línea]: https://fundacioncibei.org/teorias-tradicionales-relaciones-internacionales/.
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, "*Global Cybersecurity Index 2020"*, Ginebra Suiza, 2021, 155 pp. [En línea]: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
- UNITED STATES GOVERNMENT, "*National Security Strategy of the United States of America, United States of America"*, diciembre 2017. 68 pp., [En línea]: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2017/NSS-Final-12-18-2017-0905.pdf
- U.S. OFFICE OF THE CHAIRMAN OFS*, "The Joint Chiefs of Staff. Department of Defense Dictionary of Military and Associated Terms"* (JP 1-02), Washington, CJC, 2015.
- USI, EE.: *"2007: acontecimientos que movieron el mundo"*, Made ForMinds, 2019. [En línea]: https://www.dw.com/es/2007-acontecimientos-que-movieron-el-mundo/a-3025 878-0.
- VARGAS, S.: *"Guerra Cibernética: la nueva amenaza"*, La Jornada, México, julio 2013. [En línea]: https://www.jornada.com.mx/2013/07/05/opinion/018a2pol.
- VÉLEZ, C.: *"Ciberguerra",* Gaceta del Instituto de Ingeniería. México,UNAM, Vol. 1. Núm. 118, 2016, 24 pp. [En línea]: http://gacetaii.iingen.unam.mx/GacetaII/index.php/gii/article/view/2166/2103.
- VILLAESCUSA, S.: "*Ensayo sobre vulnerabilidad cibernética"*, CISDE Observatorio, 2016. [En línea]: https://observatorio.cisde.es/archivo/18718/#:~:text=En%20las%20%C3%BAltimas%20tres%20d%C3%A9cadas,%C3%A1mbito%20de%20hostilidades%3A%20el%20 ciberespacio.
- WALTZ, K.: *"El hombre, el Estado y la guerra"*, *Revista Académica de Relaciones Internacionales*, México, núm. 6 abril de 2007, UAM-AEDRI.
- WIENER, N. "*Cibernética o el control y comunicación en animales y máquinas".* Barcelona Tusquets, 1998. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5206500

Anexos.

1) Estrategia de Seguridad Nacional de la Federación Rusa 2021. Disponible en: https://paulofilho.net.br/wp-content/uploads/2021/10/National_Security_Strategy_of_the_Russia.pdf
2) Estrategia de Seguridad Nacional de los Estados Unidos de América 2021- Disponible en: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf