Revista Política y Estrategia
Nº 139, (2022)

Editada por: **Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) Chile**.

Lugar de edición: Santiago, Chile

Dirección web:
http://www.politicayestrategia.cl

ISSN versión digital: 0719-8027

ISSN versión impresa: 0716-7415

DOI: https://doi.org/10.26797/rpye.vi139.996

Para citar este artículo / To cite this article: MOTTA, Gustavo Jorge L.: “La Estrategia Nacional Cibernética Británica (2022-2025)”.

Revista Política y Estrategia N° 139. 2022. pp. 111-126

DOI: https://doi.org/10.26797/rpye.vi139.996

Si desea publicar en Política y Estrategia, puede consultar en este enlace las Normas para los autores:

To publish in the journal go to this link:

http://politicayestrategia.cl/index.php/rpye/about/submissions#authorGuidelines

LA ESTRATEGIA NACIONAL CIBERNÉTICA BRITÁNICA (2022-2025)∞

GUSTAVO JORGE L. MOTTA*

RESUMEN

En la actualidad la seguridad en el ciberdominio pasó a ser un área de naturaleza estratégica nacional y, a decir de importantes especialistas, es el componente más sensible de la seguridad estatal. En consecuencia, muchos países han desarrollado estrategias de ciberseguridad nacional con el propósito de brindar un contexto seguro en el ciberespacio. Gran Bretaña ha publicado en diciembre de 2021 una nueva estrategia cibernética mucho más activa, integradora y multidimensional que provee elementos claves para el estudio de este dominio, discernir su evolución y entender el conflicto en un entorno cada vez más complicado e incierto.

Palabras clave: *Ciberdominio; dominio cibernético; ciberseguridad; Estrategia Nacional Cibernética; ciberpoder.*

THE BRITISH NATIONAL CYBER STRATEGY (2022-2025)

ABSTRACT

Currently, the security in the cyber domain has become an area of a strategic nature at the national level and, according to important specialists, the most sensitive component of state security. Consequently, many countries have developed national cybersecurity strategies in order to provide a secure environment in the cyberspace. In December 2021, Great Britain published a new, much more active, integrated and multidimensional cyber strategy that provides key elements for the study of this domain, discern its evolution and understand the conflict in an increasingly more complicated and uncertain environment.

Key words: *Cyber domain; cyber domain; cybersecurity; National Cyber Strategy; cyberpower.*

---

* Magíster en Estudios Estratégicos por la Escuela de Guerra Naval (UNDEF) y Licenciado en Estrategia y Organización por el Instituto de Enseñanza Superior del Ejército. Posee un Diploma en Gestión Gerencial del Instituto Tecnológico de Buenos Aires (ITBA). Oficial de Estado Mayor del Ejército Argentino. Es Co-Director de la Maestría en Estrategia Militar de la Escuela de Guerra Conjunta de las Fuerzas Armadas, donde también se desempeña como Profesor y Jefe de Cátedra de la Materia Tareas de la Estrategia Militar. gjlmotta@hotmail.com ORCID: https://orcid.org/0000-0002-3776-3146

∞ Fecha de recepción: 090522 - Fecha de aceptación: 230522.

A ESTRATÉGIA CIBERNÉTICA NACIONAL BRITÂNICA (2022-2025)

RESUMO

Atualmente, a segurança no domínio cibernético tornou-se uma área de natureza estratégica nacional e, segundo importantes especialistas, é a componente mais sensível da segurança do Estado. Consequentemente, muitos países desenvolveram estratégias nacionais de segurança cibernética para fornecer um ambiente seguro no ciberespaço. Em dezembro de 2021, a Grã-Bretanha publicou uma nova estratégia cibernética muito mais ativa, inclusiva e multidimensional que fornece elementos-chave para o estudo desse domínio, discernindo sua evolução e entendendo o conflito em um ambiente cada vez mais complicado e incerto.

Palavras-chave: *Domínio cibernético; domínio cibernético; cíber segurança; Estratégia Cibernética Nacional; ciberpoder.*

Introducción

Los adelantos en materia de Tecnología de la Información son reveladores. Mientras las infraestructuras digitales más crecen, más vulnerables son los Estados, las sociedades y las personas. Los riesgos de fraude, espionaje, robo, daño o destrucción de propiedad intelectual o física en el ciberdominio son mayores y la confidencialidad, integridad y disponibilidad de sistemas, infraestructuras y datos, están amenazados en forma permanente[1].

La creciente integración y transversalidad en el área de la tecnología de la información ofrece claras ventajas, pero expone a Estados y sociedades a un elevado riesgo de incidentes de ciberseguridad[2].

Si bien la seguridad informática ha mantenido su raíz y características eminentemente técnicas, en la actualidad pasó a ser un área de naturaleza estratégica en el nivel nacional; es decir, un área asociada a los objetivos y seguridad del Estado.

Porque el ciberespacio no reconoce fronteras ni jurisdicciones y ha ampliado la superficie de exposición a los ataques, generando una necesidad tangible de protección. Nada ni nadie escapan a la influencia del ciberdominio. Operar en forma confiable y segura se ha convertido en algo esencial para los estados, las sociedades y las personas.

1 Guide to Developing a National Cybersecurity Strategy 2nd Edition – Strategic engagement in cybersecurity. Creative Commons Attribution-NonCommercial 3.0 IGO (CC BY-NC 3.0 IGO). p. 12.

2 Los incidentes de este tipo deberían entenderse como eventos inesperados o no deseados que pueden comprometer operaciones de cualquier naturaleza, provocando una pérdida o uso indebido de información o la interrupción parcial o total de los sistemas.

Este dominio es un "facilitador clave para la economía, la sociedad y el gobierno" y, por esa razón, la ciberseguridad "debería ser de alta prioridad"[3].

En esa misma línea, el general De Vergara sostiene que la seguridad informática es hoy el componente más sensible de la seguridad estatal porque su afectación puede tener efectos devastadores contra la seguridad de un Estado, equiparable a un ataque nuclear[4].

En consecuencia, muchos países en mayor o menor medida[5] han desarrollado estrategias de ciberseguridad nacional con el propósito de brindar un contexto seguro para el aprovechamiento del ciberespacio por parte de las personas y organizaciones públicas y privadas.

La Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés[6]), organismo especializado de la ONU encargado de regular las telecomunicaciones a nivel internacional, explica que las *estrategias de ciberseguridad* se suelen desarrollar en uno o más documentos dedicados a este dominio, o bien, ser parte integral de la estrategia de seguridad nacional o de aquella del sector de Tecnologías de la Información y las Comunicaciones[7] de un país.

El presente trabajo busca resaltar la importancia de este tipo de estrategias y recalcar la necesidad de un creciente protagonismo en los escenarios de cooperación y competencia actuales. Para ello, se ha optado por desarrollar en forma sintética los lineamientos seguidos en la materia por uno de los países más avanzados. Nos referimos a Gran Bretaña, la cual el pasado 15 de diciembre de 2021 ha publicado una nueva versión de la estrategia cibernética para el período 2022 a 2025 y que, unos meses antes, había publicado una nueva revisión estratégica de tipo "integrada" que incluye aspectos del dominio cibernético.

La elección de este país no ha sido casual por cuanto, para el Índice Global de Ciberseguridad (en inglés Global Cybersecurity Index 2020 - GCI 2020), Gran Bretaña se encuen-

---

3 International Telecommunication Union (ITU). (2021). Global Cybersecurity Index 2020. p. 1. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

4 DE VERGARA, E. (2017). Estrategia: el camino. Buenos Aires, Argentina: Editorial Universitaria del Ejército. p. 437.

5 Existen numerosos antecedentes en la región. Se sugiere ver la contribución académica Operaciones Militares Cibernéticas en https://esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-49.pdf. Algunos documentos son: en el caso de la Argentina, el 24 de mayo de 2019, la Secretaría de Gobierno de Modernización emitió la Resolución N° 829/2019 que establece una Estrategia Nacional de Ciberseguridad y crea la Unidad Ejecutiva del Comité de Ciberseguridad. Ver https://www.marval.com/publicacion/estrategia-nacional-de-ciberseguridad-de-la-republica-argentina-13372. En Chile, en abril de 2017, el Gobierno de la expresidenta Bachelet dio a conocer la Política de Ciberseguridad 2017-2022 y, en Brasil, en mayo de 2015, el Gabinete de Seguridad del Gobierno presentó la Estrategia de Seguridad de la Información y las Comunicaciones y de Seguridad Cibernética de la Administración Pública Federal 2015-2018

6 International Telecommunication Union (ITU). Loc. Cit.

7 Ver Global Cybersecurity Index 2020 en https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

tra a la vanguardia del desarrollo de la ciberseguridad. Ocupa el segundo puesto a nivel global (con 99,54 puntos[8]), seguido por Estonia con 99,48 puntos[9].

En síntesis, el estudio del caso británico permite, por un lado, apreciar la forma en que este tipo de estrategias se integra en forma creciente desde el más alto nivel y, a la vez, destacar algunas perspectivas modernas que seguramente marcarán un derrotero de interés para otros actores estratégicos estatales.

El trabajo incluye una introducción (esta sección), un desarrollo donde se resumen los aspectos del dominio cibernético de la Revisión Integrada británica de marzo de 2021 y, luego, se tratan los contenidos más salientes de la nueva estrategia cibernética de diciembre de 2021. Finalmente, se elaboran breves reflexiones. Los niveles de análisis serán el descriptivo y el explicativo.

La Revisión Integrada de Seguridad, Defensa, Desarrollo y Política Exterior británica 2021 y el dominio cibernético

A principios de 2021 Gran Bretaña presentó la Revisión Integrada de Seguridad, Defensa, Desarrollo y Política Exterior, titulada "Gran Bretaña global en una era competitiva, la Revisión Integrada de Seguridad, Defensa, Desarrollo y Política Exterior"[10].

El documento identifica en extrema síntesis el rol global que se busca alcanzar y las acciones a emprender para la presente década. Los aspectos relacionados con el ciberespacio (en sus diferentes menciones y variantes: "ciberpoder", "ciberespacio", "ciberseguridad", "cibercapacidad", "ciberriesgo", "ciberestrategia", "ciberdefensa", "cibercrimen", "ciberataque", "ciberfuerza", etc.,) se mencionan en más de 130 oportunidades, lo cual refleja su relevancia actual y la integración con el resto de las estrategias sectoriales.

Para el 2030, Gran Bretaña busca afianzar la meta "de superpotencia científica y tecnológica"…"redoblando el compromiso asumido en materia de investigación y desarrollo", fortaleciendo la red global de asociaciones, mejorando las capacidades disponibles y "estableciendo al Reino Unido como centro global digital, de servicios y datos"[11].

La adaptación a un mundo más competitivo requiere de un enfoque integrado[12] y la ciberseguridad es vista por los británicos como la base del ciberpoder y adonde se integra toda la gama de capacidades en un esfuerzo abarcativo y trasversal.

El "Marco Estratégico" de la Revisión responde a la visión que sobre las tendencias prevalecientes en el contexto internacional sirven de base para la elaboración de futuras

8 Igualado por Arabia Saudita. En Europa, Gran Bretaña ocupa el primer puesto, seguido por Estonia y luego por España con 98,52 puntos (International Telecommunication Union (ITU), 2021, p. 30).

9 Ver International Telecommunications Union (ITU). (2021). Global Cybersecurity Index 2020. p 25. Recuperado el 5 de enero de 2022, de ITU Publications: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

10 En inglés Global Britain in a Competitive Age, the Integrated Review of Security, Defence, Development and Foreign Policy.

11 Ibid. Op. Cit. p. 4.

12 Whole-of-cyber approach en inglés.

políticas en forma integrada[13]. No provee estrategias nacionales o regionales con un riguroso detalle, pero fija líneas y acciones prioritarias de fundamento flexible[14] .

Por otra parte, el "Marco Estratégico" sigue las decisiones referidas a los gastos a realizar y que fueran incluidas en la Revisión 2020. Aquí se incluyen varias iniciativas a las que se asignan fondos en forma concreta. Este es el caso del Programa Nacional de Ciberseguridad al que se destina una cifra de 305 millones de libras en inversión continua para el período 2021-2022 con el propósito de financiar proyectos intergubernamentales y transformadores de seguridad cibernética que apoyen áreas del gobierno, el sector privado y la sociedad en general.

Los cuatro objetivos generales establecidos por la revisión se apoyan mutuamente. Se desarrollan en secciones separadas y refieren a:

- "Mantener la ventaja estratégica a través de la ciencia y la tecnología"[15], como elemento integral para la seguridad y como poder cibernético global.
- Dar "forma al orden internacional abierto del futuro"[16].
- "Fortalecer la seguridad y la defensa en el interior y en el exterior"[17], con aliados y socios para abordar los desafíos a la seguridad en el ámbito físico y en el ciberdominio.
- "Desarrollar la resiliencia en el país y en el extranjero"[18] reconociendo que no es posible predecir o prevenir todos los riesgos a la seguridad y prosperidad y, por ello, se busca mejorar las capacidades relacionadas con la anticipación, respuesta y restablecimiento.

Respecto del primer objetivo, "Mantener la ventaja estratégica a través de la ciencia y la tecnología", la revisión sostiene que la competencia entre Estados ha crecido y que la Ciencia y Tecnología (en adelante CyT) incrementará su importancia como una "arena de competición sistemática"[19].

> En los años por venir, los países que establezcan un rol de liderazgo en tecnologías críticas y emergentes estarán en el primer plano del liderazgo global[20].

Por esta razón, el Reino Unido fija la necesidad de adoptar un enfoque activo hacia la "construcción y sostenimiento de una ventaja competitiva en CyT". En este ordenamiento, su primer objetivo es "hacer crecer el poder científico y tecnológico…en la búsqueda de la

13 Global Britain in a competitive Age. Op. Cit. p 18.

14 Ibid.

15 Ibid. p. 35.

16 Ibid. p. 44.

17 Ibid. p. 69.

18 Ibid. p. 87.

19 Ibid. p. 35.

20 Ibid.

ventaja estratégica", mediante un "esfuerzo de todo el Reino Unido". El gobierno crea el entorno propicio para el desarrollo de un próspero ecosistema de ciencia y tecnología[21].

Las acciones que se priorizarán incluyen la construcción de una base exitosa de CyT, liberar el potencial del ecosistema de datos y CyT, la protección de la propiedad intelectual y la investigación sensible, la mejora de la habilidad para identificar, construir y usar las capacidades estratégicas en CyT, la adopción de un enfoque colaborativo gobierno, ciencia y sector privado y la construcción de una potente y variada red de asociaciones[22].

Durante la última década, Gran Bretaña se ha convertido en una potencia cibernética mediante el diseño y construcción de capacidades defensivas y ofensivas de vanguardia y un liderazgo en el sector de ciberseguridad. El segundo objetivo particular en el área refiere a "consolidar la posición del Reino Unido como un ciberpoder responsable y democrático con capacidad de proteger y promover nuestros intereses en, y a través del ciberespacio"[23].

El ciberpoder es, según el documento, la habilidad de proteger y promover los intereses nacionales en y a través del ciberespacio. Nuevamente enfatiza el "enfoque de toda la nación" para el logro de la ciberestrategia y la integración de la industria, la academia y la ciudadanía en general a quienes le asigna un rol destacado en materia de ciberseguridad[24].

Además de asociar el ciberpoder a la defensa y seguridad, es un facilitador del crecimiento económico, de los negocios, la productividad, la innovación y la creación de trabajo. Ello genera "nuevas formas de protección de nuestros intereses, permitiendo detectar, disuadir e interrumpir las acciones de nuestros adversarios en el ciberespacio"[25]. Al respecto, debería tenerse en cuenta que, desde el año 2011, el gobierno británico ha aplicado una ambiciosa estrategia sostenida por inversiones concretas para lograr el liderazgo mundial en el campo cibernético.

Para fortalecer la seguridad y la defensa en el interior y el exterior, se han desarrollado algunas capacidades cibernéticas de vanguardia, que no se limitan al establecimiento del Centro Nacional de Seguridad Cibernética (NCSC) y la Fuerza Cibernética Nacional (NCF), creada en 2020, sino que este objetivo abarca el desarrollo de un próspero sector de ciberseguridad con más de 1.200 empresas y 43.000 puestos de trabajo calificados[26].

La seguridad cibernética es la base actual de un poder integral cibernético y fue el enfoque principal de la estrategia británica hasta 2021. La estrategia cibernética considera "la gama completa" de capacidades y, por esa razón, ha impulsado la formación de un grupo ministerial con el fin de lograr una mayor cohesión en la toma de decisiones cibernéticas en todo el gobierno[27].

21 Ibid.

22 Ibid. pp. 36 a 38.

23 Ibid. p. 35.

24 Ibid. p. 40.

25 Ibid.

26 Ibid.

27 Ibid.

Las acciones o políticas prioritarias que se observan en la revisión integrada son las siguientes[28]:

- "El fortalecimiento del ecosistema cibernético del Reino Unido, permitiendo un enfoque de toda la nación".
- "La construcción de un Reino Unido digital resistente y próspero" donde los ciudadanos estén protegidos y se disponga de capacidad de resistir y recuperarse de ataques cibernéticos.
- La ventaja en el ámbito de "las tecnologías vitales para el poder cibernético" (microprocesadores, diseño de sistemas seguros, tecnologías cuánticas y nuevas formas de transmisión de datos).
- "La puesta en marcha de marcos normativos y jurídicos de vanguardia" en tecnología digital.
- "La promoción de un ciberespacio libre, abierto, pacífico y seguro".
- "La detección, interrupción y disuasión" de los adversarios mediante la construcción de un "sistemas sin fisuras" que integre en forma creativa y permanente los recursos disponibles de tipo diplomático, militar, de inteligencia, económicos, legales, la comunicación estratégica y el empleo de la nueva Fuerza Cibernética Nacional (NCF), para imponer costos a los adversarios y negar su capacidad para dañar los intereses del Reino Unido.

La NCF posee la capacidad de conducir operaciones cibernéticas ofensivas"para apoyar las prioridades de seguridad nacional". Para ello, integra la defensa y las capacidades de inteligencia en forma responsable y dentro del derecho y el derecho internacional[29].

Un párrafo aparte merece el lugar asignado a la capacidad militar la cual debe permitir operar en forma integrada "en los cinco dominios a nivel operacional[30]. La diplomacia, fuerzas armadas y los organismos de seguridad e inteligencia son medios esenciales en cualquier estrategia nacional. Para el gobierno británico "serán los más innovadores y efectivos para su tamaño en el mundo" y caracterizados por su agilidad, "velocidad de acción e integración digital"[31].

El cuarto objetivo referido a la resiliencia refleja la necesidad de mejorar la capacidad de anticipación, prevención, respuesta y recuperación o restablecimiento en todos los sectores y convoca al trabajo transversal ante riesgos que afecten "nuestra seguridad y prosperidad" incluyendo los fenómenos naturales o amenazas "como los ciberataques"[32].

En síntesis, se observa que el campo cibernético está planeado desde el máximo nivel de la estrategia, es trasversal a todos los demás sectores, busca el rol de "poder Ciber-

28 Ibid.

29 Ibid. p. 42 .

30 Ibid. p. 7.

31 Ibid.

32 Ibid. pp. 18 y 19.

nético responsable y democrático"[33], a través de un enfoque integrador de toda la nación y ha concebido y diseñado capacidades que van más allá de la seguridad y defensa, con el objeto de sostener una ventaja estratégica con un fuerte desarrollo de la CyT, la industria y la dirección del gobierno.

La Estrategia Cibernética Nacional 2022 - Pioneros en un futuro cibernético con todo el Reino Unido[34]

La Estrategia Cibernética 2022 es un documento de 130 páginas afín a la Revisión integrada 2021. A diferencia de la Estrategia de Ciberseguridad Nacional del período 2016-2021[35] posee un enfoque más integral, multidimensional y activo que advierte que el dominio cibernético es "…una forma de proteger y promover" los "intereses en un ambiente reformado por la tecnología"[36]; ubica en el centro de la estrategia al "concepto de ciberpoder"[37] porque el foco en la ciberseguridad no era suficiente y se requería de una acción del gobierno[38].

El informe destaca siete tecnologías clave[39] que se listan más abajo y que "serán críticas para el poder cibernético"…y "debemos ser capaces de anticipar, evaluar y actuar sobre estos desarrollos"[40].

1. Tecnología 5G y 6G, y otras formas emergentes de transmisión de datos.
2. Inteligencia Artificial (IA), incluida la necesidad de proteger los sistemas de IA y el potencial del uso de IA para mejorar la seguridad cibernética en una amplia gama de aplicaciones, como el monitoreo de redes.
3. La tecnología *Blockchain* y sus aplicaciones, como las criptomonedas y las finanzas descentralizadas

33 Gobierno de Gran Bretaña - Global Britain in a competitive age. 2021. Global Britain in a competitive age The Integrated Review of Security,Defence, Development and Foreign Policy. Government of the United Kingdom. [En línea] marzo de 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.

34 En inglés National Cyber Strategy 2022 - Pioneering a cyber future with the whole of the UK.

35 National Cyber Security Strategy 2016 to 2021. Desarrollaba el plan del gobierno para hacer un país seguro y resiliente en el ciberespacio.

36 Gobierno de Gran Bretaña - NCS. 2021. National Cyber Strategy 2022 Pioneering a cyber future with the whole of the UK. Gobierno del Reino Unido. [En línea] 15 de diciembre de 2021. [Citado el: 30 de diciembre de 2021.] https://www.gov.uk/government/publications/national-cyber-strategy-2022

37 BEECROFT, N. (17 de diciembre de 2021). The UK's Cyber Strategy Is No Longer Just About Security. Recuperado el 30 de enero de 2022, de Carneggie Endowment for International Peace: https://carnegieendowment.org/2021/12/17/uk-s-cyber-strategy-is-no-longer-just-about-security-pub-86037

38 Ibid.

39 TARGETT, E. (2021). 10 key insights into UK's bullish new national cybersecurity strategy. Recuperado el 19 de enero de 2022, de The Stack: https://thestack.technology/uks-2022-national-cyber-security-strategy/

40 National Cyber Strategy 2022. Op. Cit. p. 80.

4. Semiconductores, chips de microprocesador, arquitectura de microprocesador y su cadena de suministros, diseño y proceso de fabricación.

5. Autenticación criptográfica, incluida la gestión de acceso e identidad y productos criptográficos de alta seguridad.

6. Internet de las cosas y tecnologías utilizadas en entornos de consumo, empresariales, industriales y físicos, como lugares conectados.

7. Tecnologías cuánticas, incluida la computación cuántica, la detección cuántica y la criptografía poscuántica.

Identifica cinco dimensiones alineadas con los pilares de la estrategia cibernética, vinculando fines y medios y concibiendo capacidades dedicadas en todos los componentes del poder nacional[41], incluyendo:

- Las personas, conocimientos, habilidades, estructuras y asociaciones como base del poder cibernético,
- La capacidad de proteger activos a través de la ciberseguridad y la resiliencia,
- Las capacidades técnicas e industriales en tecnologías cibernéticas clave,
- La influencia global, las relaciones y estándares éticos para dar forma a reglas y normas en el ciberespacio de acuerdo a los intereses y promoción de la seguridad y estabilidad internacional.
- La capacidad de actuar en el ciberespacio para apoyar la seguridad nacional, el bienestar económico y la prevención del delito, contemplando la realización de operaciones cibernéticas, sea, para obtener una ventaja estratégica, cumplir con la ley o aplicar sanciones en el dominio.

La estrategia británica del dominio cibernético menciona claramente que, sobre la base del abordaje estratégico actual –es decir la estrategia 2016-2021– se buscará adaptar, mejorar y expandir los esfuerzos donde sea necesario.

Está presentada con una introducción y dos partes principales. La primera, trata el contexto y la respuesta de nivel nacional y, la segunda, consiste en su implementación.

Los cinco pilares y objetivos de la Estrategia Nacional Cibernética británica, que se agregan más abajo, están referidos al fortalecimiento del ecosistema cibernético, la resiliencia cibernética, la ventaja tecnológica, el liderazgo global y el enfrentamiento de amenazas[42]:

41 Ibid. p. 20.

42 Ibid. p. 13.

Tabla 01
Cinco pilares y objetivos de la Estrategia Nacional Cibernética británica

Pilar 1	Fortalecer el ecosistema cibernético	**Objetivo 1:** Endurecer las estructuras, asociaciones y redes necesarias para apoyar una perspectiva de toda la sociedad hacia el dominio cibernético. **Objetivo 2:** Aumentar y expandir las ciberhabilidades de las nación en cada nivel, incluyendo la diversidad profesional de nivel mundial que inspire y equipe el talento futuro. **Objetivo 3:** Fomentar el crecimiento de un sector ciber y de ciberseguridad sostenible, innovador e internacionalmente competitivo, entregando calidad de productos y servicios, que satisfacen las necesidades de gobierno y de una economía más amplia.
Pilar 2	Construir un entorno digital próspero y resiliente en el país	**Objetivo 1:** Mejorar el entendimiento del ciberriesgo para impulsar una acción más efectiva sobre la ciberseguridad y resiliencia. **Objetivo 2:** Prevenir y resistir ciberataques en forma más efectiva mejorando el manejo del ciberriesgo dentro de las organizaciones británicas y proveyendo mayor protección a los ciudadanos. **Objetivo 3:** Fortalecer la resiliencia a nivel nacional y organizacional para preparar, responder y recuperarse de los ciberataques.
Pilar 3	Tomar la delantera en tecnologías vitales para el poder cibernético	**Objetivo 1:** Mejorar la habilidad para anticipar, evaluar, anticipar y actuar sobre los desarrollos de CyT más vitales al ciberpoder. **Objetivo 2.:** Adoptar y sostener una ventaja soberana y aliada en tecnologías de seguridad críticas al ciberespacio. **Objetivo 2a.**: Preservar un resiliente y robusto sector nacional cripto (*cripto-key* en inglés[43]) que satisfaga las necesidades del gobierno, aliados y socios y que haya mitigado en forma apropiada los riesgos más significativos incluyendo las amenazas de los adversarios más capaces. **Objetivo 3:** Asegurar la próxima generación de tecnologías e infraestructuras conectadas, mitigando los riesgos de ciberseguridad ligados a la dependencia de los mercados globales y asegurando que los usuarios tengan acceso a un abastecimiento confiable y diverso. **Objetivo 4:** Trabajar con la comunidad interesada para conformar el desarrollo de estándares técnico digitales globales en áreas prioritarias que más signifiquen para el mantenimiento de nuestros valores democráticos, aseguren la ciberseguridad y el avance de la ventaja estratégica en CyT.

43 Crypt-Key refiere al uso de la criptografía para proteger información crítica y servicios.

Pilar 4	Avanzar hacia el liderazgo global e influencia global	**Objetivo 1:** Fortalecer la ciberseguridad y resiliencia de socios internacionales e incrementar la acción colectiva para interrumpir y disuadir adversarios. **Objetivo 2:** Dar forma a la gobernanza global para promover un ciberespacio libre, pacífico y seguro. **Objetivo 3:** Aprovechar y exportar las propias capacidades y pericia ciber para impulsar la ventaja estratégica y promover una política exterior más amplia e intereses de prosperidad.
Pilar 5	Detectar, interrumpir y disuadir adversarios	**Objetivo 1:** Detectar, investigar y compartir información sobre Estados, criminales y otros ciberactores maliciosos y actividades para proteger Gran Bretaña, sus intereses y ciudadanos. **Objetivo 2:** Disuadir e interrumpir Estados, criminales y otros ciberactores maliciosos y actividades para proteger Gran Bretaña, sus intereses y ciudadanos. **Objetivo 3:** Actuar en y a través del ciberespacio para apoyar la seguridad nacional y prevenir y detectar casos criminales serios.

Según el sitio web "*The Stack*", la estrategia 2022 "es un recordatorio de que el dominio cibernético no existe en el vacío" porque integra las estrategias industriales, las de seguridad nacional, las habilidades y capacidades a obtener y da "una declaración de intenciones cada vez más activas e intervencionistas"[44] que asigna la módica suma de 2.600 millones de libras esterlinas (3.458 mil millones de USD) en tres años[45].

Señala la necesidad de invertir para obtener una mejora rápida y radical de toda la seguridad cibernética del gobierno y establecer estándares claros para las áreas que lo integran, focalizando en la infraestructura de TI:

Las funciones críticas del Gobierno serán endurecidas en forma significativa contra los ciberataques[46]

Por otra parte, refleja un "enfoque más ambicioso y proactivo" para mantener una creciente participación en la tecnología crítica con el apoyo de la base industrial nacional y el desarrollo de planes para "actuar cada vez más en sentido ascendente en nombre de todos los usuarios de Internet en el Reino Unido", tanto a nivel nacional como internacional[47].

44 TARGETT, E. (2021). Loc. Cit.

45 National Cyber Strategy 2022. Op. Cit. p. 35. A esa suma deben agregarse las inversiones en otros programas ya iniciados.

46 Ibid. p. 35.

47 Ibid.

Otras de las características salientes de la estrategia del ciberdominio 2022, que la diferencian de la anterior[48], son la introducción del concepto "esfuerzo comprehensivo de toda la sociedad dentro y fuera del gobierno" (en inglés whole-of-society-effort), el incremento de la ciberseguridad, el mantenimiento de la ventaja tecnológica y el desarrollo de campañas más integradas y compatibles con el propósito de interrumpir y disuadir a los adversarios.

Dentro de un creciente y disputado entorno competitivo en el que interactúan actores estatales democráticos y autocráticos[49] y no estatales[50], la estrategia introduce el llamado "autoritarismo digital" donde el foco estará en forma creciente en el ciberespacio:

> La libertad global en internet está disminuyendo globalmente como visión de espacio compartido que apoya el intercambio del conocimiento y bienes entre sociedades abiertas que corren el riesgo de verse amenazadas[51].

Una vez más la estrategia presentada eleva la perspectiva desde un problema de expertos de índole técnico a uno de naturaleza estratégica nacional. De allí, el enfoque comprehensivo que busca desarrollar todos los recursos de base industrial en áreas donde «la dependencia de fuentes de suministro no aliadas plantea riesgos de seguridad inaceptables» y enfatiza la necesidad de un liderazgo internacional más activo[52].

La estrategia 2016-2021 sostenía que la defensa y la seguridad comienzan con una aceptable disuasión aplicable a todos los dominios incluyendo lógicamente al dominio cibernético y que se debían construir alianzas globales y promover la aplicación de la ley internacional en el ciberespacio[53]. La nueva estrategia señala que a pesar de varios esfuerzos en este sentido[54] este enfoque «todavía no parece haber alterado fundamentalmente el cálculo de riesgo para los atacantes»[55] y que se buscará elevar los costos de los ataques[56].

De acuerdo con el párrafo 170 y siguientes, el modo de acción adoptado cambiará hacia una campaña más integrada y sostenida que emplee toda la escala de capacidades disponibles para imponer costos a los adversarios, persigan e interrumpan a los eventuales perpetradores y disuadan futuros ataques.

---

48 Ibid.

49 La estrategia llama explícitamente a China y Rusia como "competidores sistémicos".

50 National Cyber Strategy 2022. Op. Cit. p. 30.

51 Ibid. p. 23.

52 Ibid. p. 82.

53 Gobierno de Gran Bretaña. (2016). NATIONAL CYBER SECURITY STRATEGY 2016-2021. (G. d. Bretaña, Ed.) Recuperado el enero de 2022, de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

54 Por ejemplo las acciones para contrarrestar con los aliados el costo de la actividad hostil en 2020 cuando se produjeron los ataques a SolarWinds y Microsoft Exchange.

55 National Cyber Strategy 2022. Op. Cit. p. 25.

56 Ibid. pp. 36, 93 y 96.

Algunos elementos que serán centrales hacia el logro de este fin[57]:

- Por un lado el continuo desarrollo de la NCF para conducir ciberoperaciones ofensivas,
- Luego las campañas elaboradas a medida a través de todo el gobierno para hacer frente a las amenazas que se presenten,
- El empleo de la política exterior, el componente militar, las fuerzas policiales, de inteligencia y herramientas económicas, jurídicas y de comunicación estratégica,
- El desarrollo de nuevas inversiones para posibilitar a las fuerzas de seguridad la continuación de investigaciones a un paso y ritmo que permita mantener la ventaja.
- El intercambio de datos a través del gobierno y la industria

En síntesis, como señala Beecroft, esta última estrategia cibernética tiene un enfoque más asertivo ante una evaluación del contexto futuro riesgoso y confrontativo, destacando que las "capacidades técnicas están superando la comprensión de los países sobre cómo aprovechar las herramientas cibernéticas de manera más efectiva, lo que es una combinación peligrosa"[58].

Finalmente, contiene un interesante énfasis en el desarrollo de los recursos humanos: la palabra "habilidades" es mencionada 48 veces y se compromete a la expansión de los programas de capacitación para satisfacer las necesidades crecientes de personal con perfiles adecuados y la adopción de otras medidas como, por ejemplo, la relacionada a los programas en los institutos tecnológicos y el financiamiento de "campos de entrenamiento" en ciberseguridad[59].

Reflexiones finales

Las estrategias de seguridad y defensa de los países reflejan los ambientes particulares en que se encuentran para el período en que se elaboran. Es más, toda estrategia de seguridad, o de defensa y, en este caso particular, la del dominio cibernético, deben reflejar una conciencia estratégica respecto de su propia situación de seguridad. Reconocer cuándo y cómo adaptarse es imprescindible para una sabia y prudente dirigencia.

Acertar en los fines, modos y medios a concebir, desarrollar e implementar, refleja el fin último de la estrategia en un ambiente que parece enrarecerse y ser cada día más competitivo; porque en los conflictos, crisis y guerras no hay espacios para los segundos puestos.

Para la cultura estratégica, es bien sabido que las comunidades estratégicas piensan y se comportan de manera diferenciada respecto de cuestiones estratégicas asociadas a la

57 Ibid. p. 100

58 BEECROFT, N. Loc. Cit.

59 TARGETT, E. Loc. Cit.

defensa y seguridad del Estado. Este es el caso de la nueva estrategia cibernética británica que se ve renovada, integrada, más activa y multidimensional.

Las estrategias del ciberdominio del mundo actual, de las cuales solo se ha tratado la británica, proporcionan elementos sustanciales a la hora de estudiar y profundizar los nuevos contextos y caminos que la curva de aprendizaje va mostrando con proyección hacia un incierto y complejo futuro.

En función de ello, es crucial que en los propios contextos nacionales se den pasos precisos y renovados para concretar estrategias desde el máximo nivel y con amplia e integrada participación.

REFERENCIAS BIBLIOGRÁFICAS

BALLESTEROS, Miguel Angel. 2016. En busca de una Estrategia de Seguridad Nacional. s.l. : Ministerio de Defensa, 2016.

BEECROFT, Nick. 2021. The UK's Cyber Strategy Is No Longer Just About Security. Carneggie Endowment for International Peace. [En línea] 17 de diciembre de 2021. [Citado el: 30 de enero de 2022.] https://carnegieendowment.org/2021/12/17/uk-s-cyber-strategy-is-no-longer-just-about-security-pub-86037

BOONE Bartholomees Jr., J, y otros. 2006. U.S. Army War College Guide to National Security Policy and Strategy. 2nd Edition revised and expanded. Carlisle : U.S. Army War College, 2006.

Council of Europe (CoE),Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security. 2021. Guide to Developing a National Cybersecurity Strategy 2nd Edition – Strategic engagement in cybersecurity. [En línea] 2021. [Citado el: 30 de enero de 2022.] https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf

DE VERGARA, Evergisto. 2012. Estrategia, métodos y rutinas. Buenos Aires : Editorial Universitaria del Ejército, 2012.

DE VERGARA, Evergisto. 2017. Estrategia: el camino. Buenos Aires : Editorial Universitaria del Ejército, 2017.

DREW, Dennis y SNOW, Donald. 2006. Making Twenty First-Century Strategy - An introduction to modern National Security processes and problems. Maxwell : Air University Press, 2006.

FRISCHKNECHT, Federico, y otros. 1995. Lógica, teoría y práctica de la estrategia. Buenos Aires : Escuela de Guerra Naval. Armada Argentina, 1995.

Geopolitics of the 2015 British Defense White Paper and Its Historical Predecessors. Chapman, Bert. 2016. [ed.] Purdue University. 2, 2016, Geopolitics, History, and International Relations, Vol. 8, pp. 42-63.

Gobierno de Gran Bretaña - NCS. 2021. National Cyber Strategy 2022 Pioneering a cyber future with the whole of the UK. Gobierno del Reino Unido. [En línea] 15 de diciembre de 2021. [Citado el: 30 de diciembre de 2021.] https://www.gov.uk/government/publications/national-cyber-strategy-2022

Gobierno de Gran Bretaña - Global Britain in a competitive age. 2021. Global Britain in a competitive age The Integrated Review of Security,Defence, Development and Foreign Policy. Government of the United Kingdom. [En línea] marzo de 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

Gobierno de Gran Bretaña - NCS. 2021. National Cyber Strategy 2022 Pioneering a cyber future with the whole of the UK. Gobierno del Reino Unido. [En línea] 15 de diciembre de 2021. [Citado el: 30 de diciembre de 2021.] https://www.gov.uk/government/publications/national-cyber-strategy-2022

Gobierno de Gran Bretaña. 2016. NATIONAL CYBER SECURITY STRATEGY 2016-2021. [En línea] 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

International Telecommunication Union (ITU). 2021. Global Cybersecurity Index 2020. ITU Publications. [En línea] 2021. [Citado el: 5 de enero de 2022.] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/.

SORIANO Gatica, Juan Pablo. 2012. El peso de la cultura estratégica en las relaciones internacionales de Brasil y México. La reforma de la arquitectura interamericana de seguridad (2001-2006). Madrid : Doppel, S.L., 2012.

TARGETT, Ed. 2021. 10 key insights into UK's bullish new national cybersecurity strategy. The Stack. [En línea] 2021. [Citado el: 19 de enero de 2022.] https://thestack.technology/uks-2022-national-cyber-security-strategy/

The 21st Century Security Environment and the Future of War. Gray, Colin S. 2008. [ed.] U.S. Army War College. Fort Carlisle : s.n., 2008, U.S Army War College Parameters, Vol. 38.

The Art of Strategy and Force Planning. Bartlett, Henry C., Holman, G. Paul y and Somes, Timothy E. 1995. 2, Article 9, 1995, Naval War College Review, Vol. 48.