Panorama de Seguridad&Defensa
Centro de Investigaciones y Estudios Estratégicos - ANEPE

DEL ERROR 404 AL 505 EN ÁMBITOS DE LA SEGURIDAD Y DEFENSA

Fulvio Queirolo P.[*]
Editor Panorama de Seguridad&Defensa

Portal introductorio

La sociedad actual navega a pasos agigantados por la *World Wide Web* (diminutivo Web, por sus siglas en inglés), accediendo a variados sitios para obtener o gestionar información, empleando protocolos conocidos como *HTML, URL, HTTP*[1]. En ciertas oportunidades nos encontramos con un aviso "Error 404" o bien "Error 505", entre los más comunes en la dimensión de internet.

Para ser breve, dichos códigos revelan que la causa más probable del error es que la información no está disponible**,** ya sea porque el sitio ha cambiado, o bien, el responsable de sostener "el sistema" se encuentra desconectado o no sincronizado, provocando incertidumbre y cuestionamientos en el usuario final.

Empleando una analogía, el presente trabajo pretende reflexionar sobre algunos "errores 404 y/o 505" que se estarían manifestando en el ámbito de la Seguridad y Defensa. Estas perturbaciones, a nuestro entender, son provocadas por riesgos y amenazas al Estado que alteran la manera de gestionar los instrumentos estatales que debiesen operar para contrarrestar los efectos sobre el usuario final (sociedad).

---

[*] Magíster en Ciencia Política, Seguridad y Defensa en la Academia Nacional de Estudios Políticos y Estratégicos. Doctorando en Seguridad Internacional en la Universidad Nacional de Educación a Distancia, UNED. ORCID: https://orcid.org/0000- 0001-6837-0962

[1] HTML, URL, HTTP, IP. [en línea]. [Fecha de consulta: 6 de octubre de 2021] En: https://definicionbryan.blogspot.com/2019/09/html-http-tcp-ip-lan-url-y-ftp.html

Convengamos que a los conflictos inter e intraestatales, como Nagorno-Karabaj (2020), o Afganistán (2021), se han sumado otros fenómenos provocadores de conflictos, que identificaremos como "potenciadores" de hostilidades, los que han transitado por un camino sinuoso y difuso. En este trayecto encontramos la ciberguerra (Estonia, 2007); terrorismo cibernético (incitación al odio); ciberterrorismo (grupo Al Qassam); cibercrimen (fraudes financieros), y otros de velada presencia.

Para contrarrestar los efectos que estos "potenciadores" puedan provocar sobre las infraestructuras (humanas, físicas y lógicas), los Estados conciben la ciberseguridad y ciberdefensa como barreras de contención más conocidas, cuya fortaleza se sostiene en el empleo de inteligencia artificial (IA).

El entorno descrito nos convoca a reflexionar sobre un posible "error 404-505" en la dimensión Seguridad y Defensa provocando una (des)conexión sobre una tríada de "capas" o niveles de gestión, que para nuestro trabajo se sitúan en: *i) Amenazas/riesgos (fenómenos en el ciberespacio) – ii) Estado (arquitectura de ciberespacio) – iii) Instrumentos (mandatados en operaciones de ciberespacio);* que pasaremos a decodificar.

- ***Capa riesgos/amenazas en el ciberespacio***

A fin de reducir el ámbito de la discusión, nos situaremos en el contexto regional, y para ello recurriremos a los preceptos que la Organización de Estados Americanos (OEA) ha reconocido como riesgos y amenazas en el ciberespacio. En este sentido, ha señalado que "*con el desarrollo del internet, así como el uso masivo que ha alcanzado en la última década, surgieron nuevas amenazas y modernas formas de cometer delitos, y para contrarrestar este fenómeno apoya a los Estados Miembros en la lucha contra el crimen cibernético a través del Comité Interamericano contra el Terrorismo (CICTE) y del Programa de Seguridad Cibernética*[2]".

Tal ha sido el incremento de ataques a Estados, organizaciones y personas, que a partir del 2016 se creó el Observatorio Latinoamericano de Ciberseguridad[3]. En el análisis sobre los factores de medición estatales, allí reflejados, se pueden constatar brechas que, pese a los esfuerzos, aún persisten en la región. Temas como la aplicación de normas legales, el desarrollo de estructuras modernas, el interés por capacitar a las personas o bien implementar políticas y estrategias de ciberseguridad, aún se encuentran lejos de las pautas que otras organizaciones internacionales como la Unión Europea (UE) ya ha implementado[4].

[2] OEA. Seguridad cibernética. [en línea] [Fecha de consulta: 04 de octubre de 2021] Disponible en: http://www.oas.org/es/temas/seguridad_cibernetica.asp

[3] OEA. Observatorio ciberseguridad. En: https://observatoriociberseguridad.org/#/about

[4] UE. Ciberseguridad: cómo combate la UE las amenazas cibernéticas. [en línea] [Fecha de consulta: 07 de octubre de 2021] Disponible en: https://www.consilium.europa.eu/es/policies/cybersecurity/

Sin duda que casos como *Stuxnet*[5], o bien *DDOS*[6], demostraron la real posibilidad y capacidad de ataque exitoso de programas maliciosos (*malware*, en inglés), sobre plataformas digitales, sistemas de gestión complejos o módulos de armas. Del mismo modo, y tan efectivo como los casos anteriores resulta la presencia de un intruso malicioso (*malicious insider*) que según el reporte de *Cybersecurity Insiders*[7] establece que el 68% de las organizaciones se sienten vulnerables a penetraciones de sus sistemas por parte de sus propios funcionarios. Recordemos los consabidos procesos sobre Edward J. Snowden, Bradley Manning, Hervé Falciani, entre otros de los más recientes perpetrados a las empresas Shopify, Amazon, Stradis, Twitter y Tesla[8].

Estos ataques últimamente se han focalizado sobre infraestructuras críticas[9] de países, las que por sus repercusiones estratégicas, afectan a instituciones (públicas y privadas), estructuras financieras y empresas, entorno en el que las personas no escapan a sus efectos colaterales, aumentando la vulnerabilidad e inseguridad de los bienes y servicios a proteger.

El ámbito de la Seguridad y Defensa, como sus estructuras de ciberespacio, no se encuentra ajeno a estos ataques, que a diferencia de los primeros, representa un objetivo permanente de penetración antagonista, principalmente por el rol estatal frente al cual están conminado a cumplir, y, por ello, merece un resguardo diferenciado de otras organizaciones.

El cuestionamiento entonces se sitúa en: ¿qué tan protegidas se encuentran las estructuras de ciberseguridad y ciberdefensa? ¿Se podría presentar un “error 404 – 505” que implique desconectar sectores tan importantes para el Estado? ¿Qué consecuencias podría acarrear?

Para dar respuesta a nuestros cuestionamientos, recurriremos a la experiencia española y que fue debidamente expuesta en un Seminario Institucional del Ejército de Chile el 2018, a raíz de la creación del Comando de Ciberdefensa. En dicha ocasión el expositor español señaló: “Cualquier Fuerza Armada moderna posee múltiples sistemas de armas, tecnológicamente muy avanzados, que necesitan obligatoriamente acceder al ciberespacio para ser realmente eficaces. Si ese acceso se pierde, retrocedemos 60 años en el tiempo. En segundo lugar, la protección de infraestructuras críticas de interés para la defensa y que

---

5 CBS Interactive Inc. *Iran Confirms Stuxnet Worm Halted Centrifuges.* [en línea]. Washington DC: CBS News november 29, 2010. [en línea] [Fecha de consulta: 06 de octubre de 2021] Disponible en: https://www.cbsnews.com/news/iran-confirms-stuxnet-worm-halted-centrifuges/

6 BBC. “Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país”, MAYO 2012. [en línea] [Fecha de consulta: 5 de octubre de 2021] Disponible en:https://www.bbc.com/mundo/noticias-39800133

7 CYBERSECURITY, Insiders. Insider Threat Report 2020. [en línea] [Fecha de consulta: 6 de octubre de 2021] Disponible en: https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf

8 EKRAN. Insider Threat Statistic for 2021: Facts and figures. [en línea] [Fecha de consulta: 6 de octubre de 2021] Disponible en: https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures

9 COMISIÓN DE LAS COMUNIDADES EUROPEAS. Programa europeo para la protección de Infraestructuras Críticas (PEPIC). [en línea] CEU, 12 de diciembre de 2006 [Fecha de consulta: 09 de octubre de 2021] Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:ES:PDF

afectan directamente a la operatividad de las FF.AA. deben ser debidamente resguardadas"[10].

- ***Capa Estado***

El incremento de ataques provocados por diferentes actores (estatales, no estatales y otras organizaciones, principalmente con fines criminales), que utilizan el ciberespacio como medio para acceder a sus objetivos, ha incentivado a las administraciones estatales, en el contexto de su realidad local, a la redacción y adecuación de normas, desarrollo de estructuras, así como a adoptar medidas específicas para mitigar los daños que causan y pueden afectar la normal actividad de una sociedad (laboral, económica, integridad personal o colectiva).

Reconociendo este valioso y significativo aporte logrado para resguardar la comunidad, al poco andar nos encontramos con contradictoria evidencia. Los duros datos, desafortunadamente, nos indican que "errores 404 – 505" continúan con alto grado de latencia, principalmente provocado por la lentitud en adaptar normas, asumir el costo de desarrollo de estructuras y en a voluntad por sincronizar capas de gestión.

En este plano de discusión, necesariamente, recurriremos a lo establecido por la Comisión de las Comunidades Europeas, organismo que desde el 2004 se ha cuestionado por la protección de Infraestructuras Críticas. A la fecha, se ha migrado a la protección de sectores estratégicos, entendiendo aquellos que son esenciales para la seguridad nacional de un país (sector energía, aeroespacial, nuclear, administración, financiero, seguridad y defensa)[11], y otros de acuerdo a la realidad local.

A mayor abundamiento, el Reporte de Ciberseguridad BID-OEA (2020), entrega una visión global sobre la situación regional. Interesante y preocupante es lo señalado por el Gerente de Instituciones para el Desarrollo del BID, quien instala como evidencia que "…la región de América Latina y el Caribe aún no está suficientemente preparada para enfrentar los ataques que se producen en el ciberespacio"[12].

- ***Capa Instrumentos (ciberdefensa - ciberseguridad)***

Para nuestro estudio, la experiencia de Colombia resulta muy auspiciosa. En dicho país, a partir del 2016, se puso en marcha la Política de Ciberseguridad y Ciberdefensa, estructurándose una organización funcional y operacional encabezada por el Presidente de

[10] GÓMEZ LÓPEZ de Medina, Juan Carlos. *La Ciberdefensa en España*. En: Seminario Institucional Ejército de Chile - Ciberespacio: Desafíos para la Seguridad y Defensa de Chile en el siglo XXI. (Santiago, Chile, 2018). Trabajos, Santiago, Chile. Ejército de Chile. Disponible en: https://www.translators.cl/es-noticia.php?id=1831

[11] COMISIÓN DE LAS COMUNIDADES EUROPEAS. Op. Cit.

[12] BID-OEA. Reporte Ciberseguridad 2020. BID, 2020. p. 10. [en línea] [Fecha de consulta: 08 de octubre de 2021] Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

la República, el asesor para la Seguridad Nacional, el ministro de Defensa, el ministro de las Tecnologías de la Información y Comunicaciones, el director del Departamento Administrativo de Seguridad (DAS), el director de Planeación Nacional y el coordinador del Grupo de Respuesta a Emergencias Cibernéticas (ColCERT). Adicionalmente, pueden participar otros actores nacionales que representen al sector académico, el sector privado, expertos internacionales u otras instituciones del Estado[13].

Así, el Comando Conjunto Cibernético (CCOC) se posesiona como la autoridad responsable de la ciberdefensa (amenazas externas), el Comando Cibernético Policial (CCP) es la autoridad encargada de la ciberseguridad, por lo cual ofrece a la ciudadanía apoyo, protección y seguimiento ante los delitos cibernéticos, produciéndose una simbiosis civil-militar plausible de imitar. El resultado a la fecha es que se ha levantado una barrera cibernética con capacidad de identificar y contener actividades delictuales que han intentado afectar a la sociedad colombiana. Del mismo modo, ha permitido compartir experiencias de su actuar con otros países de la región que avanzan en la implementación de este modelo.

No cabe duda que una actividad de esta naturaleza requiere una trasformación (material y humana), pero también apostar a la investigación y desarrollo (I + D), una condición en que Latinoamérica no destaca; peor aún, tiende a declinar[14]. Una vinculación directa con el desarrollo de la industria de la Defensa regional, entorno en que solo dos países procuran fortalecer este ámbito: México y Brasil[15].

Entorno de definiciones urgentes e importantes

Desde *el otro lado del charco* (Europa), resulta cautivador analizar ciertas propuestas que, desde el ámbito de la Seguridad y Defensa, exhortan a consolidar estructuras estatales que, de manera incipiente para algunos, y robustecidas en otros, han sido desarrolladas por países que invierten por sobre el 1% de su PIB en I + D, convocando e incentivando la elaboración de proyectos que se orienten al fortalecimiento de capacidades estratégicas para la defensa de intereses nacionales, los que previamente han sido definidos por la autoridad gubernamental. En esta línea podremos evidenciar los siguientes proyectos de desarrollo de capacidades:

[13] CUJABANTE, JARA, PRIETO y QUIROGA. "Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares". En: Revista Científica 30, abril, 2020. En: https://www.researchgate.net/publication/340935140_Ciberseguridad_y_ciberdefensa_en_Colombia_un_posible_modelo_a_seguir_en_las_relaciones_civico-militares

[14] SCIDEV.NET. "Descenso en inversión de I+D se acentúa en Latinoamérica". [en línea] [Fecha de consulta: 08 de octubre de 2021] Disponible en: https://www.scidev.net/america-latina/news/descenso-en-inversion-de-i-d-se-acentua-en-latinoamerica/

[15] ANEPE. CT. N°7, 2020. "Ciencia, Tecnología e Innovación en la Defensa: los casos de Brasil y México (2007-2020). En: https://anepe.cl/wp-content/uploads/2021/03/Cuaderno-de-Trabajo-N%C2%B07-2020.pdf

- Autonomía para despegue y aterrizaje de drones.
- Drones autónomos para navegación y recopilación de información exploratoria en diversas condiciones del terreno.
- Apoyo en la realización de misiones complejas mediante el uso de Realidad Aumentada.
- Comunicación personal y móvil, Ad-hoc *Device to Device* / MESH basado en estándares 5G.
- Identificación de anomalías en tiempo real a partir de varias fuentes de información.
- Ciberseguridad para sistemas heredados al operar un sistema operativo moderno.
- Contrarrestar infracciones a la ciberseguridad a través de actualizaciones de software.
- IA para análisis de información e investigación de riesgos.
- Seguimiento inteligente de baja resolución.
- Navegación autónoma basada en cámaras: campo de la robótica (algorítmica)
- Soluciones de seguridad para sistemas autónomos - campo de la robótica.

La optimización de los recursos (humanos, físicos, lógicos y del ciberespacio), requiere contar con una dirección centralizada, la que a través de diferentes organismos (públicos y privados), intersectoriales –incluidos los sectores de defensa y seguridad– participen eficazmente en la contención de posibles, factibles y reales amenazas en una nueva dimensión espacial que pueden ser llevadas a cabo por personas, grupos, organizaciones o Estados contra los intereses nacionales.

El contar con políticas de I + D e inversión en “ciber seguridad-defensa” se ha situado como una imperiosa necesidad, sin embargo, si estas no van acompañadas de estrategias que operacionalicen el ámbito de **qué, quién, cuándo y cómo** se abordará, implicará que la latencia de “errores 404 o 505” se mantenga o, peor aún, se ramifique afectando significativamente las pantallas situacionales o capas ya señaladas (Estado, organizaciones y sociedad), que provocarán mayores daños a los que estamos ya acostumbrados.

Sin duda que esta dimensión es más amplia de lo que se ha tratado de reflejar en este Panorama, sin embargo el objeto ha sido destacar que las lógicas lineales ya no aplican en esta dimensión, ya que los bordes geográficos entre la Seguridad y Defensa se encuentran superpuestos, los riesgos se han transformado en reales amenazas multi-dominio que impactan ámbitos públicos y privados, y donde el capital humano requiere de un alto estándar de preparación, así como de dirección y coordinación centralizada.