La población como objetivo estratégico de las acciones cibernéticas: Desafíos para la defensa y seguridad multidimensional presentes (o no) en las Políticas y Estrategias Nacionales de Seguridad Cibernética.

Coronel Aviador (FAB) Claudio D. FARIA [1]

Recibido: 15 de mayo de 2024; Aceptado: 26 de junio de 2024.
Revisión al español: Coronel Pedagogo (FARD) Adamilca Emelinda Rodríguez Martínez
Claudio D. Faria, "La población como objetivo estratégico de las acciones cibernéticas: Desafíos para la defensa y seguridad multidimensional presentes (o no) en las Políticas y Estrategias Nacionales de Seguridad Cibernética," *Hemisférico Revista del Colegio Interamericano de Defensa 10* (2024): 26-43. https://doi.org/10.59848/24.1207.HV10n2

Resumen

Este artículo explora el contexto contemporáneo del ciberespacio, destacando la creciente importancia de la ciberseguridad. Se enfatiza la necesidad de defensas efectivas para proteger la información y se subraya la ciberhigiene como una posible línea de defensa a través de la concientización del usuario. El texto discute la persistencia de la cultura de la transgresión, en relación con este concepto y examina el papel de la educación en ciberseguridad en la promoción de la resiliencia nacional. Se aborda la importancia de proteger a la población contra influencias psicológicas de ataques cibernéticos, abogando por que la revisión de las Estrategias Nacionales de Ciberseguridad incluya a la población como una "infraestructura crítica". Las políticas públicas centradas en las personas son esenciales para anticipar los efectos adversos de tales amenazas cibernéticas sobre la población, a fin de evitar que se convierta en arma eficaz y eficiente que exija su seguridad y defensa.

Palabras clave: Ciberhigiene - resiliencia nacional – ciberataques - operaciones psicológicas - infraestructura crítica – anarquía - estrategia nacional de ciberseguridad.

Abstract

This article explores the contemporary context of cyberspace, highlighting the increasing importance of cybersecurity. It emphasizes the need for effective defenses to

[1] El Coronel Claudio Faría se desempeña actualmente en el Colegio Interamericano de Defensa como Jefe de la División de Facilitadores y Mentores del Departamento de Estudios y egresado distinguido de la Clase 62 del CID. Es piloto de la Fuerza Aérea de Movilidad, y su última asignación fue en el Comando de Estado Mayor de la Fuerza Aérea Brasileña, donde tuvo la oportunidad de trabajar en la implementación del nuevo Centro de Operaciones de Ciberdefensa de la Fuerza Aérea. El presente artículo refleja sus propios puntos de vista y reflexiones personales sobre temas del ciberespacio, explorando lo que había aprendido durante su tiempo como estudiante del Colegio Interamericano de Defensa. Correo electrónico: *Claudio.faria@iadc.edu*. https://orcid.org/0009-0009-0582-7019

protect information and underscores cyber hygiene as a possible line of defense through user awareness and education and its implications. The text discusses the persistence of the culture of transgression, especially in Latin America, regarding this concept and examines the role of cybersecurity education in promoting national resilience.

The importance of protecting the population against psychological influences resulting from cyber-attacks is also addressed, advocating that the revision of National Cybersecurity Strategies should include the population as a "critical infrastructure". People-centered public policies are essential to anticipate and mitigate the adverse effects of such cyber threats on the population, aiming to prevent it from becoming an effective and efficient weapon that demands its security and defense.

***Keywords**: Cyber hygiene - national resilience - cyber-attacks - psychological operations - critical infrastructure – lawlessness - national cybersecurity strategy*

Introducción

"*Es necesario esconderse en el seno de la tierra, como las venas de agua, cuyas ramificaciones son insondables. Así ocultarás todas tus diligencias*".[2]

Basándome en estas frases atribuidas a Sun Tzu y que son, para mí, fuente de inspiración, empiezo este artículo creyendo que las palabras que se le atribuyen durante siglos encajan perfectamente, pero con una diferencia: "tierra" sería "ciberespacio", tiempo en el que, evidentemente, esto no existía.

Haciendo las comparaciones y reflexiones, el "Arte de la Guerra" encaja muy bien como referencia y base para que las personas activas en este nuevo dominio creen su propio "Arte Operacional" y que esto sea para el beneficio general de la humanidad y en defensa de los más débiles y oprimidos. Por lo tanto, tal frase del general chino encaja en el tema cibernético, que ahora se está desarrollando.

El lector podrá reflexionar mejor y en consecuencia correlacionar los conocimientos derivados de la seguridad multidimensional, la defensa y la economía de la seguridad, la aplicación de teóricos y pensadores estratégicos, las relaciones

[2] Sueli Cassal, "Sobre el arte de maniobrar las tropas", en Arte da guerra (Porto Alegre: L&PM, 2006), 24.

internacionales, entre otros. Todo ello reafirma el papel transversal que tiene como principal característica la actividad cibernética.

La creciente dependencia de la tecnología e Internet ha hecho que la ciberseguridad sea una preocupación cada vez más importante para los gobiernos, las empresas y las personas. Los medios de defensa son indispensables. Negar ventajas operativas en el ciberespacio por acciones maliciosas es un factor crucial para mantener la confidencialidad, integridad y disponibilidad de este nuevo dominio, recordando que estas tres palabras representan las principales propiedades de la ciberseguridad contenidas en la Recomendación UIT-T X.1205, 2008 de la Unión Internacional de Telecomunicaciones (UIT), organismo de las Naciones Unidas.

Así, en este artículo, describiré cómo entiendo que el ser humano se ha convertido en una pieza fundamental y centro de gravedad para ser considerado como un importante contribuyente a la ciberseguridad y, al mismo tiempo, un objetivo compensador frente a las acciones subversivas surgidas del ciberespacio de hoy y también del mañana.

Primera línea de defensa: higiene cibernética

¿Qué es la higiene cibernética?

En primer lugar, podemos entender el concepto de ciberhigiene, consultando a una de las empresas líderes en el sector: Kaspersky, que la define como los pasos que deben dar los usuarios de ordenadores y dispositivos conectados a internet para aumentar la seguridad de su información, a través de una postura mental y hábitos diarios, con el fin de mitigar las posibles aperturas y posibilidades ante un intruso.[3]

Algunos ejemplos de procedimientos de saneamiento cibernético incluyen el uso de firewalls para evitar el acceso no autorizado; uso de contraseñas seguras; cambios frecuentes de contraseñas; no usar contraseñas 1234...; usar contraseñas diferentes para dispositivos IoT; emplear autenticación multifactor (evitar acciones de robots e IA); realizar copias de seguridad de sus datos personales y de interés en dispositivos de disco duro externos; evite publicar datos personales en las redes sociales (observe el fondo de sus fotos antes de publicarlas); no responder a encuestas que soliciten sus datos

[3] Kaspersky, "Los mejores consejos para la higiene cibernética para mantenerse seguro en línea. Cyber Hygiene Definition," acessado em 11 de fevereiro de 2023, https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

personales; evitar acceder a redes Wi-Fi gratuitas en lugares públicos (contratar un servicio de proveedor privado de internet con contrato y políticas de privacidad); mantener actualizadas las aplicaciones y el software (programar el móvil para que lo haga de madrugada); eliminar las aplicaciones que ya no sean útiles; no utilizar su *nombre personal como nombre de las* redes WiFi domésticas*; utilizar servicios contratados de encriptación de datos en la nube; entre otros.*

¿Por qué no es totalmente eficiente y eficaz? ¿Qué hacer?

Aun considerando que existen varias iniciativas para alertar a los usuarios; sin embargo, lamentablemente, la cultura de la transgresión sigue presente en la vida cotidiana de las personas, especialmente en América Latina, como nos traen Sorj y Martuccelli.[4]

Muchos, a pesar de tener acceso a materiales de orientación en ciberhigiene, no los consultan y no los implementan en casi nada, porque entienden que las reglas y normas son solo para otros y no tienen nada que ver con ellos mismos, corrompiéndose con este pensamiento egoísta que afecta a la colectividad, especialmente cuando se trata de ciberseguridad, a nivel mundial. Muchas personas se conectan cada año.

Sin embargo, esta situación no debe desanimar un proceso de instrucción y fortalecimiento de la doctrina de la ciberhigiene. Para reforzar esta tesis, traigo a Newmeyer.[5] Él, a través de sus recomendaciones, afirma que el sector educativo debe ser tomado en cuenta en la elaboración y ejecución de las Estrategias Nacionales de Ciberseguridad (ENSC).

Su comparación con el sector de la salud pública es perfecta, a mi juicio, para entender más fácilmente el poder de las acciones preventivas (higiene) aplicadas al ámbito cibernético (ciberhigiene) como forma de mitigar las diligencias indeseables ocultas en el ciberespacio. De hecho, en lo que respecta a la ENSC, al consultar a mi país, noté que en dos de sus Objetivos Estratégicos hay un punto a la necesidad de aumentar la

[4] Bernardo Sorj y Danilo Martuccelli, "Problemas y promesas: economía informal, crimen y corrupción, normas y derechos," en *El desafío latinoamericano: cohesión social y democracia* (São Paulo/Río de Janeiro: Instituto Fernando Henrique Cardoso, 2008).

[5] Kevin Newmeyer, "Elements of National Security Strategy for Developing Nations," en *National Cybsersecurity Institute Journal* Vol.1, No.3 (Nueva York: Excelsior College, 2015), 17, consultado el 11 de febrero de 2023, http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf, 13-15.

resiliencia brasileña frente a las amenazas cibernéticas y fortalecer el desempeño de la ciberseguridad en el escenario internacional.

Newmeyer continúa afirmando que, a medida que más y más sistemas están interconectados, se hace imprescindible contar con campañas educativas dirigidas a difundir materiales doctrinales e informativos que contengan buenas prácticas que permitan a los ciudadanos protegerse y contribuir a que todos los componentes de la infraestructura general de las tecnologías de la información y la comunicación (TIC) funcionen de manera satisfactoria y, sobre todo, resiliente.

Si las personas evitan cambiar su conducta de seguridad frente al uso de las TIC, considerando el ciberespacio, es poco probable que las acciones maliciosas de los ciberdelincuentes o ciberatacantes no logren el éxito esperado, porque si las personas confían solo en el desempeño del aparato estatal, aún no está dimensionado para soportar tal demanda de defensa y ciberseguridad.

Digo esto en términos del número de especialistas, así como en términos de sus cualificaciones profesionales apropiadas y sus necesidades de cursos constantemente actualizados.

Pero ¿por qué este énfasis en la individualidad como refuerzo de una colectividad?

Educación en ciberseguridad y resiliencia nacional

Pues bien, para tratar de presentar una posible respuesta a esta pregunta, traigo a la mente los elementos componentes de la actividad cibernética, tal y como se enseña en el CID, y también con lo que entiende Microsoft, que son: Perpetrador, Objetivo, Acción e Impacto, destacando que el usuario común puede, sí, ser un perpetrador de una ciberamenaza, sirviendo como un *útil Insider*[6] comprometiendo los sistemas con su mala praxis y conducta, como aprendí de Mariano Bartolomé en sus clases en este mismo Colegio.[7] [8]

[6] Por definición general, sería la persona que tiene alguna relación con la institución (personal o profesional) objeto de acciones cibernéticas maliciosas que, intencionadamente o no, sirven como agentes facilitadores de las consecuencias perjudiciales de estos actos.

[7] Mariano Bartolomé, "*Características de las cibercomodidades,"* (Washington-DC: Colegio Interamericano de Defensa, Curso de Ciberseguridad y Seguridad Pública de la Maestría en Defensa y Seguridad, 2023), diapositiva 29.

[8] Microsoft, "Evaluating Behavior in Cyberspace," em *International Security Norms: Reducing conflict in an Internet-dependent world*, acessado em 11 de fevereiro de 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA, 6.

Se puede ver que muchas personas siguen siendo víctimas de técnicas de *phishing* y terminan contribuyendo a un proceso de *ransomware* en su vida personal y profesional. Esta situación se ha agravado durante la pandemia, como también nos traen Bartolomé y Lima en un artículo haciendo hincapié en el trinomio Crimen, Terrorismo y Ciberespionaje. Los autores nos muestran que, solo en el primer semestre de esta enfermedad en 2020, los ciberataques crecieron un 34% en comparación con el mismo periodo anterior.[9]

De esta manera, considero importante fortalecer la educación de la persona común a través de la enseñanza y difusión de las mejores prácticas en materia de ciberhigiene como una forma de contribuir a lograr un mayor nivel de seguridad ciudadana en general.

Vale la pena subrayar aquí en este punto que los derechos de una persona están limitados por los derechos de los demás, por la seguridad de todos y por las justas exigencias del bienestar común y general, como nos ha traído el artículo XXVIII de la Declaración Americana de los Derechos y Deberes del Hombre desde 1948.

Creo que, al hacerlo, estaríamos contribuyendo a un mayor grado de resiliencia nacional frente a las acciones malvadas que se esconden en el entorno del ciberespacio. Esto puede ayudar mucho a los países del hemisferio, ya sea con más o menos recursos, a ofrecer un mayor grado de dificultad a los ciberdelincuentes, que tendrían más dificultades para actuar.

Sin embargo, como ciudadano interamericano, me sigue preocupando ver indicadores como los presentes en el Informe de Ciberseguridad de la OEA.[10] Los países de América Latina aún tienen un desempeño inferior al satisfactorio, especialmente en base a los resultados de las dimensiones nº 2 y nº 3, en sus ítems D2.1, D2.3 y D3.1.

Estos tres anteriores se refieren al tema de la Madurez Cibernética analizado en los estándares de esta organización internacional y se relacionan con la mentalidad de ciberseguridad, la comprensión del usuario de la protección de la información personal en internet y la concienciación, respectivamente, que traigo aquí para reforzar que el

[9] Mariano Bartolomé e André Lima, "La pandemia como uma amenaza a la vida y a la seguridad del Estado. El ciberespacio, durante y después de la pandemia COVID-19," em *Revista Academica de Guerra del Ejército Ecuatoriano*, Vol.14, No. 1 (Quito: CEHE, 2021), 72

[10] Organización de los Estados Americanos, "Perfiles de países," en *Informe de Ciberseguridad 2020: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe* (Washington-DC: BID, 2020), consultado el 21 de febrero de 2023, https://www.cybersecurityobservatory.org/#/final-report, 45-179.

usuario común sigue siendo un objetivo útil capaz de ser explotado por ciberdelincuentes y similares, afectando así a la ciberseguridad nacional en el ámbito de una seguridad multidimensional en esta parte del mundo.[11]

Al consultar con la UIT, apunta en cierta medida en la dirección de lograr cierto grado de ciberseguridad nacional, sugiriendo que los gobiernos y el sector privado deberían prevenir, detectar y responder a la ciberdelincuencia y al uso indebido de las TIC a través de una legislación que permita la investigación y el enjuiciamiento con el fin de ofrecer asistencia mutua; fortalecer el apoyo institucional a nivel internacional y fomentar la educación con el consiguiente aumento de la conciencia situacional del problema.

Me llama la atención aquí sobre la ratificación de la UIT en el punto en cuestión sobre la importancia de la cibereducación ciudadana como forma de sumar esfuerzos para reducir el poder de penetración maliciosa desde el ciberespacio. Este conocimiento se proporciona a través de su Resolución nro. 174.

En general, creo que esas contribuciones internacionales son válidas e incluso pueden alentar a los Estados a adoptar medidas preventivas, incluida la cuestión del uso del ciberespacio. Las Organizaciones no Gubernamentales (ONG) también están entrando en escena para unir fuerzas en esta misma dirección. Veamos un ejemplo de mi país. Louise Huriel, del Instituto Igarapé, propone algunas recomendaciones para la redacción/actualización de la Estrategia Nacional de Ciberseguridad de Brasil.[12]

En ellos, hay algunos en cuanto a elevar el nivel de madurez de la sociedad en ciberseguridad. Este ítem tiene 14 preguntas para mejorar este documento nacional. Destaco aquí algunos de ellos como ejemplos: crear eventos formativos para la ciudadanía, llevar a cabo acciones de sensibilización de la sociedad en general; y crear políticas públicas que promuevan la concientización permanente, entre otras que han sido propuestas por esta ONG dedicada.

[11] Siempre en relación con la ciberseguridad nacional, es importante aportar sus cinco perspectivas expuestas en el Manual de "Seguridad Cibernética Nacional" elaborado por el CCDCOE de la OTAN, a saber: Ciberseguridad Militar; la lucha contra la ciberdelincuencia; Inteligencia y Contrainteligencia de la Fuente Cibernética; Protección de Infraestructuras Críticas Nacionales y Gestión de Crisis; y la Ciberdiplomacia, para entender que todo está interconectado y debe ser visto como un único ecosistema global.

[12] Louise Huriel, "Ciberseguridad en Brasil: un análisis de la estrategia nacional," en *Artículo Estratégico 54*, (Río de Janeiro: Instituto Igarapé, 2021), visitado el 21 de febrero de 2023, https://ciberseguranca.igarape.org.br/estrategia/, 39

Además, creo que, si tengo la oportunidad, ofrecería la sugerencia de insertar otra recomendación para las ENSC de los países que aún no las han implementado, esto es: adoptar el término Ciberhigiene, ya que esta palabra, a mi juicio, tiene la fuerza suficiente para una fácil comprensión y absorción por parte del ciudadano común, así como aprovechar la comparación con la actividad sanitaria es un factor muy apropiado y oportuno para facilitar la comprensión y lograr para tener más éxito en el esfuerzo educativo.

Además, otros documentos internacionales ya lo han adoptado, como el Manual Nacional de Ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN) y el Manual de Derecho Internacional Humanitario aplicable a la Guerra Cibernética, también de la OTAN/CCDCOE y adoptado por países de este hemisferio como fuente y referencia.[13]

En mi paso por el Estado Mayor de la Fuerza Aérea de Brasil, participé especialmente en los equipos de trabajo para la creación e implementación del Sistema de Ciberdefensa de la Fuerza Aérea. En ese momento, el equipo tuvo cuidado de incluir un sector específico para la ciber educación en las propuestas para la estructura organizativa de la unidad responsable de actuar como órgano central de este sistema. Así, una de sus tareas era, precisamente, promover la concienciación del público interno con el fin de obtener un mayor grado de resiliencia, es decir, del público objetivo interno en su vertiente de conducta individual y grupal.

Quisiera recordarles que hemos utilizado muchos productos fabricados por la Junta Interamericana de Defensa y el CSIRT brasileño (CTIR.GOV), con el fin de obtener un mayor grado de solidez frente a una iniciativa de este tipo.[14] [15]

Ahora veo que hemos contribuido, indirectamente, también al público externo, es decir, a la gente común, porque los militares y servidores civiles de la Fuerza Aérea tienen familias y estas son potenciales difusores de técnicas de ciberhigiene en sus hogares, propagándolas de manera beneficiosa y, de esta manera, contribuyendo a la concientización general, lo que resulta en un excelente aporte al esfuerzo nacional.

[13] El Centro de Excelencia Cooperativo de Defensa Cibernética (CCDCOE) es una estructura de la OTAN dedicada a ayudar a los países en cuestiones de ejercicio e investigación con un enfoque en el fortalecimiento de las capacidades de defensa y ciberseguridad, considerando las áreas de entrenamiento, operaciones, tecnología, estrategia y legal.

[14] Junta Interamericana de Defensa, "Cyberdefense: News Bulletins," consultado el 24 de febrero de 2023, https://www.jid.org/ciberdefensa-2/.

[15] Centro Gubernamental de Prevención, Tratamiento y Respuesta a Incidentes Cibernéticos, "Recomendaciones," consultado el 23 de febrero de 2023, https://www.gov.br/ctir/pt-br.

Por lo tanto, la percepción sería que mantener altos estándares de higiene cibernética constantemente como una doctrina individual y colectiva por parte de los ciudadanos comunes, fortalecería el poder de resiliencia cibernética de un país. En consecuencia, también se puede inferir que cada país, al hacerlo, un grupo de países podría alcanzar un mayor grado de resiliencia en términos regionales. Esta sería una iniciativa para crear una cadena regional de defensa y ciberseguridad si todos lo hacen de manera coordinada. ¡Qué bonito sería eso! Sin embargo...

El eslabón más débil de la cadena

Después de haber estudiado el caso de Estonia en 2007, en el que el país sufrió una serie de acciones maliciosas orquestadas en el ciberespacio, noté un factor interesante que podría recibir atención. Allí, en palabras del general ruso Sergey Chekinov, citado por Beskow y Carley, señaló en 2013 que la nueva generación de guerra se caracterizará por operaciones de información y psicológicas que debilitarán a las Fuerzas Armadas y a la población del rival.

Así, el general continúa afirmando que estas acciones serán fundamentales para preparar el terreno para la victoria en lo que él llama la Revolución de las Tecnologías en el campo de batalla. Un año después, el brigadier Philip Breedlove afirma, en la OTAN, que Rusia está librando la más increíble *guerra relámpago* informativa, haciendo menciones a tácticas que implican el concepto de utilizar varias maniobras coordinadas con varios medios avanzando constantemente sobre un conjunto de objetivos y de manera rápida para no dar al enemigo oportunidades de reaccionar o reorganizarse para un nuevo ciclo de reacciones defensivas.

Llegados a este punto, la comparación sería muy oportuna, analizando el ciberespacio.

Vemos que, en el mismo año de 2014, los rusos intervienen en la guerra civil siria, en apoyo de Bashar al-Assad, y comienzan a apoyar a los separatistas prorrusos en la provincia de Donbass, en el este de Ucrania.

En tal escenario, los rusos también utilizan el ciberespacio para su campaña de desinformación, ya que Matos Barboza nos plantea el uso de la técnica del troll[16] para impulsar la opinión pública y ejercer presión sobre la población objetivo.[17] A los trolls se les encomendó la tarea de publicar comentarios en artículos de noticias 50 veces al día. Los que escribían *blogs* tenían que mantener seis cuentas de Facebook y publicar al menos tres *posts diarios*. En Twitter (ahora X), necesitaban tener al menos 10 cuentas, en las que publicaban 50 veces para mantener los efectos de este proceso.

En mi opinión, siguiendo a Visacro, digo que ya estamos en una guerra informativa contemporánea a través del ciberespacio.[18] El Jefe del Estado Mayor General de la Federación Rusa, General Valery Gerasimov, es citado por el autor en su disertación sobre los aspectos de una Guerra Híbrida, donde los medios no militares de carácter político, económico, social, humanitario e informativo aumentan la eficacia, con el fin de lograr objetivos políticos y estratégicos, y este punto también es visible en la doctrina rusa. Además de lo mismo que se nota en la doctrina china.

Traigo aquí al debate a Tarien y Priisalu que son unánimes en destacar en sus relevantes ponencias que hay, sí, presente en el mundo actual y comportándose como un hecho que lleva[19] el futuro en el que el objetivo de provocar el caos en un determinado grupo de ciudadanos, a través del sentimiento de pérdida de confianza y el sentimiento de impotencia y aislamiento por parte de sus gobiernos hacia ellos como resultado de los ciberataques.[20] [21]

¡Este es el punto clave de este artículo!

Cabe destacar que más que proteger las Infraestructuras Críticas, per se, lo importante sería conseguir que la población no entre en esta fase de influencia psicológica

[16] Según el contenido del libro, los trolls son personas contratadas y entrenadas para denigrar a los opositores de Putin, con más de 600 personas empleadas en toda Rusia y un presupuesto anual de 10 millones de dólares.

[17] Carlos Eduardo de Matos Barboza, "La estrategia rusa en el conflicto de Ucrania: contribuciones a la doctrina militar brasileña," (Río de Janeiro: Escuela de Estado Mayor del Ejército, 2018), visitado el 24 de febrero de 2023, https://bdex.eb.mil.br/jspui/bitstream/123456789/3868/1/MO%205965%20-%20MATOS%20BARBOZA.pdf, 54-55.

[18] Alessando Visacro, "Doing the Right Things: Security and Defense of the Modern State," en *Cadernos de Estudos Estratégica* nº 1 (Río de Janeiro: ESG, 2019), visitado el 21 de febrero de 2023, http://www.ebrevistas.eb.mil.br/CEE/article/view/6725/5821, 70.

[19] Definición disponible en el manual de Planificación Estratégica de la Escuela Superior de Guerra de Brasil.

[20] Jaak Tarien, "Ciberseguridad en Estonia 2020: Lo que ha cambiado", mesa redonda, 15 de junio de 2020, vídeo, 23:32.

[21] Jaan Priisalu et al, "Six Colours: War in cyberspace", OTAN-OTAN, 27 de abril de 2007, video, 8:25.

(pánico) y actúe como motor descontrolado para desequilibrar el equilibrio y las capacidades de las fuerzas de defensa nacional y de seguridad pública.

Recordando a Contreras, creo que el poder asimétrico sobre la seguridad multidimensional que las ciberamenazas imponen al mundo se puede correlacionar con el modelo número 2 de Beaufré, teniendo en cuenta objetivos, medios y libertad de acción.[22] Este sería el modelo de Presión Indirecta, mediante el cual se busca alcanzar objetivos políticos a través de la presión psicológica, sin utilizar la fuerza física directa.

En este caso, los medios utilizados son la propaganda, la diplomacia, el espionaje y el sabotaje, con el objetivo de debilitar la resistencia del oponente y facilitar la consecución de los objetivos políticos previstos. La libertad de acción es alta, ya que el uso de medios indirectos y no violentos le da al agente un gran margen de maniobra y flexibilidad, lo que permite la adaptación de las tácticas según lo requiera la situación.

En este contexto, me llamó la atención el caso de Estonia, especialmente cuando reflexioné sobre Andžāns y Bērziņa-Čerenkova, cuando fue posible darse cuenta de que, como resultado de las lecciones aprendidas en 2007, hubo un reordenamiento de la clasificación de sus Infraestructuras Críticas a Funciones Críticas y... *¡Sorpresa!* La sociedad estonia se considera la principal, y debe ser informada al Consejo Europeo sobre sus aspectos críticos y vulnerables.[23] Cabe destacar que en la ENSC de Estonia existe la disposición del Objetivo Estratégico número 1 que demuestra la atención prestada por los estonios en términos de que su sociedad esté digitalizada, cohesionada y, especialmente, ciberresiliente.[24]

Me parece, al leer su ENSC, que los estonios tienen un orgullo nacional de ser una sociedad verde/*sin papel*, así como confían en su sistema nacional de identificación personal protegido por encriptación. Esto aparece en muchas partes del texto del documento. De hecho, hasta este momento, ha sido el único país que hace referencia al concepto de reputación para que otros puedan considerarlo confiable y deseen hacer negocios con él a todos los niveles. Esto sería similar a cuando compramos a un vendedor,

[22] Arturo Contreras, "Estrutura y Lógica de la Estrategia Contemporánea" en *Estrategia: Las Viejas y las Nuevas Amenazas*, (Santiago: Mago Editores, 2007): 4.

[23] Consejo de la Unión Europea, *Directiva 2008/114/CE del Consejo*, en Diario Oficial de la Unión Europea, (Bruselas: UE, 2008), acessado em 26 de fevereiro de 2023, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF#:~:text=This%20Directive%20establishes%20a%20procedure,to%20the%20protection%20of%20people, 78-79. Nota del autor: Esta é referente ao Artigo IV da Diretriz 2008/114/EC.

[24] República de Estonia, "Cybersecurity Strategy - Strateegilised Eesmärgid," (Tallin: Ministerio de Asuntos Económicos y Comunicaciones, 2019), acessado em 26 de febrero de 2023, *https://www.mkm.ee* › medios › descargar.

pero primero comprobamos su aceptación en cuanto a cuántas *estrellas* tiene, o incluso consultamos webs especializadas en internet para saber de antemano si el distribuidor es fiable y si debemos o no seguir adelante con la compra o contratación del servicio.

Recordando una vez más a Newmeyer, nos ofrece los siguientes paradigmas en su obra: seguridad nacional, economía y salud.[25] Al estudiar los posibles casos recientes en los que las actividades cibernéticas pueden haber sido parte de los ataques a una entidad extranjera, llego a pensar que también sería oportuno añadir, a los conceptos que el autor presenta, uno más por mi cuenta. Sería el paradigma psicosocial como una cuarta parte de esta lista. Llego a esta conclusión después de analizar el poder de las personas y su fuerza en la seguridad multidimensional.

De hecho, otro factor importante que Newmeyer también había destacado en su investigación sobre la ENSC sería que una de las grandes dificultades es la falta de consenso sobre qué agencia se encargaría de liderar el proceso de resolución de crisis en casos cibernéticos. Reflexionando ahora: quienquiera que sea una agencia de este tipo, ¿tendría el personal capacitado para prever la posibilidad de ocurrencias de disturbios sociales cuya ignición habría sido originada, motivada, iniciada debido a una influencia cibernética engañosa?

Sé que esta fue una pregunta retórica solo para mostrar, elocuentemente, la importancia que veo en el aspecto del ciudadano, de la persona humana, de las personas mismas, como un actor racional, pero ampliamente influenciado hasta el punto de que es objeto de operaciones psicológicas por parte de ciberatacantes, algo que ninguna ENSC a la que he tenido acceso trata directamente y con la debida claridad ante la importancia de proteger a las personas del miedo, desesperación, agonía y tantos otros malos sentimientos, que pueden llevar a una manifestación masiva en oleadas de violencia. Que los ciudadanos comunes practiquen actos oscuros porque perciben cualquier posibilidad de perder la satisfacción de sus necesidades básicas, como se aprende consultando la pirámide de Maslow.

Veo que la regla 29 del Manual de Tallin[26] contribuye en este sentido y puede considerarse desde mi punto de vista que la persona humana en la sociedad se convierte

[25] Newmeyer, 9-19.

[26] La regla 29 del Manual de Tallin se refiere a la protección de que los civiles puedan ser considerados combatientes si se demuestra que participan en actos de beligerancia u hostilidades entre las partes. Tiene como referencia el Primer Protocolo Adicional (1977) de los Convenios de Ginebra (1949) en su esencia

en un objetivo primario no combatiente hoy y cada vez más en el mañana, como nos trae Schmitt.[27]

Desde Oriente, los autores Xiangsui y Liang traen la confirmación de que esta misma sociedad está en la lista de posibles objetivos a explotar, según la doctrina china.[28] Esto se llevaría a cabo a través de una mezcla de tácticas convencionales agregadas con tácticas informativas que, a través de un combate cruzado y coordinado, tiene como objetivo generar sinergia en la acción y, así, obtener un mayor grado de impacto en el adversario de adentro hacia afuera. Además de traer una parte clara de la doctrina china que explora una acción híbrida en el combate contemporáneo, los autores del libro Guerra sin restricciones también se refieren a la importancia de contar con un Comando Conjunto como estándar de liderazgo y que esté compuesto por varios especialistas multidisciplinarios.

En mi experiencia profesional, tuve la oportunidad de pertenecer a algunos Comandos Conjuntos de la estructura de defensa militar brasileña. No recuerdo que existiera una célula, un sector, una sección, un departamento, una división diseñada para predecir y proporcionar acciones psicológicas sobre una población objetivo o parte de ella. Sí, ya sé que existe una estructura de relación Cívico-Militar, pero con otras atribuciones diferentes al enfoque de este artículo, es decir: la población como Infraestructura Crítica a proteger... y voy a ir más allá: un Sistema Crítico para tener en cuenta.

En la época en que tuve la oportunidad de participar en el proceso de revisión de la ENSC en mi país, antes de ser estudiante del CID (Clase 62),[29] recuerdo que el equipo hizo sugerencias en la época, sin embargo, no teníamos la percepción, idea o reflexión de que la población brasileña, independientemente del avance de las tecnologías disruptivas, podría convertirse en uno de los centros de gravedad y talón de Aquiles para infligir mayores demandas de apoyo y atención por parte de la población brasileña, parte de los medios de seguridad y defensa nacional hasta una gran escala. Por lo tanto, lamentablemente no sugerimos nada al respecto, pero siempre habrá nuevas oportunidades al reanudar el debate público sobre la revisión de la ENSC en Brasil.

[27] Michael Schimitt, "Conferencia PILAC sobre Operaciones Cibernéticas y DIH: Líneas de Falla y Vectores," *Programa HLS sobre Derecho Internacional y Conflictos Armados*, 3 de abril de 2015, 56:23.

[28] Xiangsui, Wang y Liang, Qiao. "Diez mil métodos combinados en uno: combinaciones que trascienden las fronteras" en *Unrestricted War* (Pekín: Casa del EPL, 1999).

[29] *¡La Mejor!* (Esta es una referencia a una tradición muy particular del Colegio Inter-Americano de Defensa cuando se nombra la clase actual, con la que se dice en voz alta: *¡La Mejor!*)

¿Y qué?

Ahora... ¡sencillo!

No es posible *prever* si no somos capaces de *prever*.

Para predecir, es necesario explorar el debate de manera amplia con la debida diversidad de pensamiento y experiencia. Ideas innovadoras. Ampliar las percepciones.

Objetivo: Predecir, predecir y predecir qué puntos pueden ser explotados por el ciberatacante.

¿Cuál de estos tiene el potencial de generar efectos psicológicos negativos y, en consecuencia, revueltas masivas en la población, o en parte de ella, es editar una lista priorizada de tales puntos en los planes nacionales de resiliencia, capaz de orientar la idealización, elaboración, implementación y revisión de las políticas públicas con el fin de fortalecer la respuesta gubernamental que sea realmente perceptible para la población y que esta sea oportunamente rápida? De esta manera, creo que también tendríamos un cierto efecto disuasorio sobre los aspirantes a aventureros del ciberespacio.

Dato: Estamos jugando con el equipo en desventaja y defensivamente.

El adversario tiene un comportamiento operativo difícil de predecir, detectar y que se adapta rápidamente utilizando el avance *supersónico* de las tecnologías disruptivas.

De hecho, no conozco soluciones fáciles que se apliquen a muchos casos al mismo tiempo; soluciones definitivas y decisivas. Sin embargo, creo que tenemos que ser más ágiles en términos de planificación estratégica a largo plazo. Por cierto, me pregunto ahora: ¿Qué sería a largo plazo, teniendo en cuenta la cibernética? Pues bien, las ENSC suelen recibir sus revisiones y posibles actualizaciones en ciclos de unos pocos años, dependiendo del país que las haya editado.

¿Sería esto coherente con la realidad de los cambios en el escenario percibido por el ciudadano común a través de los medios de comunicación globalizados en estos días?

Así, nos acercamos al final de este artículo considerando lo mencionado en párrafos anteriores sobre el tema de la importancia de definir un organismo centralizador para la planificación de acciones que logren el grado de resiliencia en niveles satisfactorios. Teniendo en cuenta la velocidad y los impactos que las actividades maliciosas tienen en las infraestructuras críticas; considerando que, en ocasiones, los medios de defensa y seguridad nacional no están a la altura de lo que realmente necesita

un país, e incluso por su extensión geográfica, que tiene dificultades para satisfacer más de una demanda al mismo tiempo en su territorio; que el adversario es consciente de tales debilidades y está seguro de que puede explotarlas; y, finalmente, considerando que, una vez que se percibe la ineficiencia del Estado para proveer a la seguridad de su pueblo y la satisfacción de sus necesidades básicas, el adversario los utiliza como fuerza anárquica e impulsora para agotar todos los medios y, así, interferir en el mantenimiento de la deseable y necesaria paz social, surge una reflexión: no es tan simple como se dijo en la apertura de esta parte.

Sin embargo, me gustaría reiterar que debemos revisar nuestras ENSC. Entender que la población debe ser concebida como la "*infraestructura*" crítica más importante de una nación. Por lo tanto, una vez que este concepto sea constante y ampliamente debatido, ya que estaría contemplado en un documento al más alto nivel estatal, derivará de él políticas públicas más coherentes con la realidad del escenario operativo.

Aquí está nuestro "¿y qué?"

El centro de atención se centra más en *las personas* y menos en *las cosas*.

De este modo, nos damos la oportunidad de predecir mejor el comportamiento anárquico causado por estas variables abordadas. Prever en tiempos de paz. Documentar para no olvidar y debatir con más frecuencia y agilidad gubernamental. Mejorar nuestro proceso de planificación estratégica basado en capacidades para aquellos que lo han implementado.

En consecuencia, es mejor predecir para proporcionar mejor.

Reflexiones finales

Al final, el lector se da cuenta de que mi enfoque estaba en las personas. Creo que, en el funcionamiento de cualquier tecnología, el ser humano siempre será el eslabón más débil de la cadena. Por lo tanto, está claro que la higiene cibernética es un tema crucial y contribuye al poder de resiliencia cibernética de un país y a mitigar las posibilidades de interferencia ilícita que surgen y se ocultan en las "ramificaciones insondables de las venas de agua" del ciberespacio, recordando el pasaje de Sun Tzu dicho en la introducción de este artículo.

No se puede dejar de lado los sentimientos de las personas. Lo que les hace sentir miedo, angustia y desesperación. Perder su dinero, perder la seguridad de su casa... de su familia, debido a los ataques cibernéticos que fueron exitosos por el adversario. Este es

más un reino para operaciones psicológicas y para obtener ventajas sobre los objetivos con el fin de obtener su estado final deseado sobre otros que no estaban preparados y no eran conscientes.

Un asesor estratégico de alto nivel, que también ha sido capacitado por el CID, no debe olvidar esto y la redacción de los diversos y variados resultados de aprendizaje descritos en cada *Syllabus*, de los cuales traigo aquí algunos relacionados con el tema de la ciberseguridad, haciendo hincapié en el trabajo de la asesoría de más alto nivel, que son: abordar los riesgos que las amenazas cibernéticas representan para la seguridad pública, defensa y seguridad nacional; diagnosticar los principales desafíos críticos de ciberseguridad en el hemisferio e interpretarlos desde una perspectiva de seguridad multidimensional; ofrecer diferentes medidas y recomendaciones para abordar los desafíos de la ciberseguridad; integrar diferentes conocimientos y saberes sobre el tema; formular recomendaciones y colaborar en el proceso de toma de decisiones a nivel estratégico, para abordar los desafíos de ciberseguridad, incluyendo respuestas multilaterales, entre otros.

Al fin y al cabo, todos somos conscientes de que somos servidores públicos en la esencia de la palabra y, como tales, tenemos en la persona humana la razón de nuestro trabajo. Así que, finalmente, el mensaje sería que podemos ser más atentos, creativos, inteligentes y perspicaces. Igualmente, estar en hermandad con las naciones vecinas, ya que el entorno cibernético no tiene en cuenta ningún límite físico para lanzar su interferencia.

El bienestar de nuestros pueblos debe ser la tónica frente a este nuevo espacio dimensional, que aún no es la última frontera,[30] que requiere un enfoque multidisciplinario y multidimensional, explorando la diversidad del pensamiento crítico y libre de ataduras. También nos desafía a saber hasta dónde puede llegar la humanidad para bien o para mal; individual o colectiva; en el hoy y en el mañana, yendo audazmente a donde antes no imaginábamos.

Bibliografía.

[30] Menciona el inicio de la serie de televisión iniciada en los años 60 y creada por Gene Roddenberry. Siguió durante décadas más tarde como la franquicia de Star Trek y presenta los viajes de la nave espacial Enterprise al espacio, la última frontera, en su misión de cinco años para explorar nuevos mundos, nuevas civilizaciones, yendo audazmente a donde ningún humano ha ido antes. Aquí, es apropiado hacer un paralelismo con el ciberespacio.

Barboza, Carlos Eduardo de Matos. "La estrategia rusa en el conflicto de Ucrania: aportes a la doctrina militar brasileña." (Río de Janeiro: Escuela de Estado Mayor del Ejército, 2018). Consultado el 24 de febrero de 2023, ttps://bdex.eb.mil.br/jspui/bitstream/123456789/3868/1/MO%205965%20-%20MATOS%20BARBOZA.pdf, 54-55.

Bartolomé, Mariano. "*Características de los ciberservicios."* (Washington-DC: Colegio Interamericano de Defensa, Curso de Ciberseguridad y Seguridad Pública de la Maestría en Defensa y Seguridad, 2023). Diapositiva 29.

Bartolomé, Mariano e Lima, André. "La pandemia como uma amenaza a la vida y a la seguridad del Estado. El ciberespacio, durante y después de la pandemia COVID-19." Em *Revista Academica de Guerra del Ejército Ecuatoriano.* Vol.14. No. 1 (Quito: CEHE, 2021), 72.

Brasil. Centro Gubernamental de Prevención, Tratamiento y Respuesta a Incidentes Cibernéticos. "Recommendations." consultado el 23 de febrero de 2023. https://www.gov.br/ctir/pt-br.

Cassal, Sueli. "Sobre el arte de maniobrar las tropas." en *Arte da guerra* (Porto Alegre: L&PM, 2006). 24.

Contreras, Arturo. "Estrutura y Lógica de la Estrategia Contemporánea" en *Estrategia: Las Viejas y las Nuevas Amenazas.* (Santiago: Mago Editores, 2007): 4.

Estados Unidos de América. Junta Interamericana de Defensa. "Ciberdefensa: Boletines de Noticias." consultado el 24 de febrero de 2023. https://www.jid.org/ciberdefensa-2/.

Unión Europea. El Consejo de la Unión Europea. *Directiva 2008/114/CE del Consejo.* En Diario Oficial de la Unión Europea, (Bruselas: UE, 2008). Acessado em 26 de fevereiro de 2023. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF#:~:text=This%20Directive%20establishes%20a%20procedure,to%20the%20protection%20of%20people, 78-79.

Huriel, Louise. "Ciberseguridad en Brasil: un análisis de la estrategia nacional. en *Artículo Estratégico 54*, (Río de Janeiro: Instituto Igarapé, 2021). Visitado el 21 de febrero de 2023, https://ciberseguranca.igarape.org.br/estrategia/. 39

Kaspersky. "Los mejores consejos de higiene cibernética para mantenerse seguro en línea. Cyber Hygiene Definition." acessado em 11 de fevereiro de 2023. https://www.kaspersky.com/resourse-center/preemptive-safety/cyber-hygiene-habits.

Kevin Newmeyer. "Elements of National Security Strategy for Developing Nations." en *National Cybsersecurity Institute Journal* Vol.1. No.3 (Nueva York: Excelsior College, 2015). 17, consultado el 11 de febrero de 2023, http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf, 13-15.

Microsoft. "Evaluating Behavior in Cyberspace." em *International Security Norms: Reducing conflict in an Internet-dependent world*, acessado em 11 de febrero de 2023. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA, 6.

Organización de los Estados Americanos. "Perfiles de país", en *Informe de Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe* (Washington-DC: BID, 2020). Consultado el 21 de febrero de 2023, https://www.cybersecurityobservatory.org/#/final-report, 45-179.

Priisalu, Jaan et al. "Six Colours: War in cyberspace." OTAN-OTAN, 27 de abril de 2007, video. 8:25.

República de Estonia. "Cybersecurity Strategy - Strateegilised Eesmärgid." (Tallin: Ministerio de Asuntos Económicos y Comunicaciones, 2019). acessado em 26 de fevereiro de 2023. *https://www.mkm.ee* › medios › descargar.

Schimitt, Michael. "Conferencia de PILAC sobre Operaciones Cibernéticas y DIH: Líneas de Falla y Vectores." *Programa de HLS sobre Derecho Internacional y Conflictos Armados*. 3 de abril de 2015, 56:23.

Sorj, Bernardo y Martuccelli, Danilo. "Problemas y promesas: economía informal, crimen y corrupción, normas y derechos." en *El desafío latinoamericano: cohesión social y democracia* (São Paulo/Río de Janeiro: Instituto Fernando Henrique Cardoso. 2008).

Tarien, Jaak. "Ciberseguridad en Estonia 2020: Lo que ha cambiado." mesa redonda. 15 de junio de 2020, vídeo, 23:32.

Visacro, Alessandro. "Hacer lo correcto: seguridad y defensa del Estado moderno." en *Cadernos de Estudos Estratégica* nº 1 (Río de Janeiro: ESG, 2019) Visitado el 21 de febrero de 2023. http://www.ebrevistas.eb.mil.br/CEE/article/view/6725/5821, 70.

Xiangsui, Wang y Liang, Qiao. "Diez mil métodos combinados en uno: combinaciones que trascienden las fronteras." en Unrestricted War (Pekín: Casa del EPL, 1999).