La Ciberseguridad: análisis político y estratégico*

(Primera entrega)

Dr. Boris Saavedra**
Doctor en Paz y Seguridad Internacional

Dra. Luisa Parraguez
Doctora en Relaciones Internacionales

**Articulista invitado Profesor del Centro de Estudios Hemisféricos de Defensa William J. Perry

- Extendemos nuestros agradecimientos al equipo de apoyo en investigación: Abil Razo y Suzanne Claeys

El presente artículo de reflexión surge del proyecto de investigación sobre Ciberseguridad del Centro de Estudios Hemisféricos de Defensa William J. Perry, Universidad Nacional de Defensa, Washington, D.C.

Foto: https://www.travelers.com/cyber-insurance/4-ways-cyber-insurance-helps-protect-your-business

Resumen

El ciberespacio es un ambiente complejo y dinámico caracterizado por ser una creación humana sujeta a cambios acelerados, motivados por tres fuerzas que interactúan: la tecnología digital, la globalización y el cambio climático. Este artículo se enfoca en el análisis del ciberespacio desde la óptica de la Seguridad y Defensa a nivel político y estratégico. Se discute el tema de la gobernanza a través de la ciberseguridad adecuada, lo cual constituye el reto más importante y relevante a escala global en este ámbito. El logro de este objetivo requiere del análisis para generar las capacidades estructurales (tecnológicas) así como también de observaciones geopolíticas correspondientes. La complejidad del ciberespacio requiere de una política nacional que defina la capacidad del Estado para desarrollar la tecnología, el recurso humano competente, el financiamiento adecuado y el material necesario. La estrategia deberá explicar el empleo de todos los componentes del ciberespacio y su papel para la materialización de los fines delineados en la política. Finalmente, el ecosistema digital y los actores internacionales ponen en evidencia la compleja dinámica que se presenta actualmente en la interacción entre los Estados.

Palabras clave: Ciberseguridad; Estrategia; Geopolítica; Internet; Relaciones Internacionales.

Abstract

Cyberspace is a complex and dynamic environment created by humans and subject to rapid and accelerated changes, motivated by three forces that interact: digital technology, globalization and climate change. This article focuses on an analysis of cyberspace from a Security and Defense perspective at the political and strategic level. The topic of governance is addressed through adequate cybersecurity which constitutes the most important and relevant global challenge in this area. In order to reach this goal, analysis is required to generate the structural capacities (technological) as well as the geopolitical enquiry. The complexity of cyberspace calls for a national policy that defines the capacity of the State to develop technology, competent human resources, the adequate financing and the necessary material. The strategy should explain the use of all the components in cyberspace and its role in achieving the goals underlined in the policy. Finally, the digital ecosystem and the international actors demonstrate the complex dynamics involved in the interaction among States.

Key Words: cybersecurity; strategy; geopolitics; Internet; International Relations.

> *"El potencial de sorpresa en el ciberespacio aumentará en el próximo año y más allá, ya que miles de millones de dispositivos digitales están conectados, con relativamente poca seguridad incorporada, y tanto los Estados nacionales como los actores malignos se vuelven más atrevidos y mejor equipados en el uso de herramientas cibernéticas cada vez más extendidas. El riesgo de que algunos adversarios realicen ataques cibernéticos, como la eliminación de datos o interrupciones localizadas y temporales de la infraestructura crítica, es cada vez mayor."*
>
> *Comunidad de Inteligencia de Estados Unidos, febrero 13, 2018*

Introducción

La ciberseguridad es el asunto de mayor relevancia hoy día y se mantendrá así en los años por venir. Las organizaciones de Tecnologías de la Información y la Comunicación (TIC) se mantienen en una alerta constante para proteger la información en la base de datos y la propiedad intelectual almacenada en las redes conectadas en Internet. Las vulnerabilidades del *software* son omnipresentes, con proveedores de seguridad ofreciendo soluciones actualizadas pero temporales; los proveedores de antivirus no pueden mantenerse a nivel de la evolución de las amenazas y solo ofrecen soluciones reactivas a los virus. El software de barrera de protección (*firewalls*) es utilizado por instituciones públicas y privadas, sin embargo, no escapa de los efectos de la penetración de agentes maliciosos capaces de atacar a las redes de TIC y pivotear asuntos de valor, generando pérdidas billonarias.

En consecuencia, este artículo tiene como objetivo plantear algunos elementos fundamentales de análisis para el diseño y desarrollo de la política y la estrategia de la ciberseguridad.

El ambiente de la ciberseguridad, al igual que el ciberespacio, es complejo y dinámico, caracterizado por la aceleración del cambio y motivado por las tres fuerzas que interactúan: la tecnología digital, la globalización y el cambio climático, siendo el factor definidor de esta aceleración la velocidad de rotación del cambio (Friedman, 2016). Estas fuerzas ejercen influencia en el dominio operativo cibernético enmarcado por el uso de electrones en un espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de Internet y su infraestructura asociada (Kuehl, en Kramer, 2009).

El diseño del marco político y estratégico para la gobernabilidad del ciberespacio es posiblemente el reto más importante de la humanidad, y requiere no solo de capacidades estructurales (tecnológicas), sino también del análisis geopolítico correspondiente, con la organización efectiva que permita el desarrollo de operaciones con capacidades integradas de ataque y defensa de la red informática como base fundamental para el desarrollo de la doctrina cibernética que incorpore la totalidad de elementos del sector público y privado (Kramer, 2009). Este conjunto de elementos estructurales y geopolíticos deben concluir con la generación de esfuerzos cooperativos a nivel internacional en materia de ciberseguridad, por la necesidad imprescindible de cooperación en un ambiente donde las fronteras no existen y, en consecuencia, la soberanía tiene una connotación de interdependencia para el logro de la gobernabilidad global que satisfaga la necesidad de seguridad del espacio cibernético.

"Este conjunto de elementos estructurales y geopolíticos deben concluir con la generación de esfuerzos cooperativos a nivel internacional en materia de ciberseguridad, por la necesidad imprescindible de cooperación en un ambiente donde las fronteras no existen y, en consecuencia, la soberanía tiene una connotación de interdependencia para el logro de la gobernabilidad global que satisfaga la necesidad de seguridad del espacio cibernético".

Las características estratégicas del dominio cibernético

Este dominio está integrado por sistemas físicos y lógicos y posee una infraestructura que está gobernada por leyes físicas e igualmente por la lógica de códigos computacionales. Cabe observar que las principales leyes físicas que gobiernan el ciberespacio son las relacionadas con el electromagnetismo y la luz. La velocidad con la cual se propagan las ondas y los electrones que se mueven, generan ventajas y retos tales como: comunicaciones instantáneas a través del ciberespacio y una gran cantidad de *data* que puede transitar enormes distancias sin impedimento físico o fronteras políticas (Goodman, 2015). En definitiva, la velocidad y libertad de movimiento crean retos y ventajas para los individuos, las organizaciones y los Estados, pero al mismo tiempo conciben vulnerabilidades que pueden ser explotadas o aprovechadas por el adversario (Campbell, 2015).

En el ciberespacio, al igual que en el aire y el espacio, todas las actividades involucran el uso de la tecnología. El ciberespacio es el único entorno en el cual las interacciones están regidas por *hardware* y *software* creados por el ser humano y, como resultado, la geografía del ciberespacio es mucho más mutable que la de otros ambientes. La topografía de los ambientes físicos es muy difícil de transformar como es el caso de montañas, ríos y mares. En cambio, porciones del ciberespacio pueden ser encendidas o apagadas con el movimiento de un interruptor para crear o mover el ambiente mediante la inserción de un nuevo código de instrucciones en un router o interruptor. Sin embargo, esta flexibilidad no es

infinita, ya que existen limitaciones de los pasos y alcance de estos cambios que están sujetos a leyes físicas, lógicas, propias de los códigos y las capacidades de la organización y el personal (Libicki, en Kramer, 2009).

Los sistemas y la infraestructura que integran el ciberespacio tienen una gran variedad de interconexiones. Desde una computadora personal conectada a una impresora que utiliza un pequeño y aislado enclave en el ciberespacio, hasta el Internet. Este último se ha convertido en el principal ejemplo de una red global masiva en el ciberespacio, incrementando, en forma constante, los aparatos que generan un número considerable de interconectividad moderada por *software* y protocolos, particularmente con la masificación de estándares digitales y sistemas inalámbricos (*Wireless*) que facilitan el tránsito de la información entre sistemas (Schneider, 2015). Sin embargo, gobiernos como la República Popular China, países del Medio Oriente y otros, hacen uso de filtros y demás técnicas para limitar el uso de Internet global a sus ciudadanos.

El capital humano adecuadamente preparado es fundamental en el ciberespacio, ya que ejerce influencia en el uso del medio ambiente. No es tan solo tener el conocimiento y las habilidades, sino mantenerse actualizado. Es un reto constante, ya que la evolución de la tecnología, por lo acelerado de los cambios, exige la permanente actualización de estos actores (Singer y Friedman, 2014). Adicionalmente, el número de personas es fundamental, por el grado de especificidad que demanda la variedad de situaciones que pueden generar acciones preventivas, correctivas y reactivas para ejercer el control con eficiencia y eficacia, ya que de ello dependerá el grado de soberanía que se puede alcanzar en el ciberespacio. Finalmente, es necesario destacar que las teorías y enfoques para ejercer el control del Estado y el aprovechamiento del control como Poder Nacional, no se han desarrollado aún.

El ambiente estratégico del ciberespacio tiene dos elementos fundamentales: los elementos estructurales y los geopolíticos (Kramer, 2009). Es así como los elementos estructurales se enfocan en esa parte del espacio cibernético que genera capacidades en general y que incluyen el incremento de la seguridad, la expansión y el desarrollo de la investigación y el capital humano, el aumento de la gobernanza y la organización efectiva. Los elementos geopolíticos se enfocan en la forma tradicional de los esfuerzos en Seguridad y Defensa; en este grupo se incluyen a las operaciones centradas en la red, el uso de red de computadoras con capacidades de ataque, defensa, y disuasión que incorporen al ciberespacio, operaciones de estabilidad e influencia.

> "El ciberespacio es el único entorno en el cual las interacciones están regidas por hardware y software creados por el ser humano y, como resultado, la geografía del ciberespacio es mucho más mutable que la de otros ambientes".

Los elementos estructurales

Los elementos estructurales son los generadores de capacidades en el ciberespacio, el cual, a diferencia de los otros dominios físicos, se caracteriza por el uso de *bits* y *bytes* (unidades computacionales) y no de bombas, cañones, aviones, buques o tanques de guerra, que representan la fuerza física para la superioridad en combate. Esta característica requiere el uso de algoritmos que es una explicación científica para resolver un problema, dado que es un conjunto ordenado y finito de operaciones que permite hallar la solución de un problema, mediante instrucciones que representan un modelo específico (Clark, 2017).

El algoritmo no debe confundirse con programa, ya que este último es la codificación del primero en lenguaje de programación o en instrucciones a la computadora. La resolución de problemas mediante computadora conlleva dos pasos: hallar un algoritmo y su posterior codificación. En otras palabras, un estratega de ciberseguridad debe conocer bien lo que puede hacer un algoritmo y cómo lo hace.

En la actualidad, el empleo de algoritmos permite realizar el análisis de un problema en pocos minutos con muy alta precisión. Por otro lado, la clasificación de datos complejos no debe realizarse solamente con las herramientas tradicionales de análisis de datos, por lo cual se han creado nuevos algoritmos especialmente diseñados para el análisis de datos masivos (*Big Data analytics*) (Simon, 2014).

Los activos digitales de una organización son propensos a ser atacados en cualquier momento. La naturaleza multidimensional de la amenaza en el dominio cibernético demanda de las organizaciones capacidades para la evaluación objetiva de los riesgos mediante la aplicación de *software* cada vez más novedoso. Basados en los hallazgos, las empresas asignan cada vez más recursos para mitigar riesgos de ataques cibernéticos. La predicción cuantitativa de las posibilidades de ataque puede ayudar a las organizaciones a contrarrestar las ocurrencias de estos.

El Sistema Común de Calificación de Vulnerabilidad (CVSS, por sus siglas en inglés) es un estándar marco utilizado por organizaciones para comunicar las características y los impactos a las vulnerabilidades en un ataque a TIC (Luo, 2014). El CVSS ayuda a establecer un lenguaje común en la comunidad de TIC. Por esta razón, el uso de un modelo algorítmico podría predecir el impacto de un ataque basado en los factores importantes que influyen en la seguridad cibernética.

Foto: http://kmrdpartners.com/2018/05/02/cyber-liability-insurance-small-business/

Los elementos geopolíticos

El ciberespacio es un dominio y a la vez un apoyo para el ejercicio del poder en las naciones, organizaciones públicas y privadas, en las comunidades, los individuos y los actores no estatales, incluyendo las bandas criminales y terroristas. A su vez, el poder y la Seguridad Nacional podrían definirse incluyendo todos los aspectos de la dinámica social en general, para poder realizar un mejor y más efectivo análisis y recomendaciones de los elementos geopolíticos en el ambiente cibernético. El concepto de dominio implica ciertos contenidos como el de la superioridad, la cual está relacionada con la capacidad de control para ejercer influencia con las competencias o habilidades en la actuación en este ámbito.

Hay dos aspectos que merecen ser analizados en profundidad. Primero, si el ciberespacio es un dominio comparable a los otros dominios analizados en el contexto geopolítico. En este sentido el Departamento de Defensa de Estados Unidos describe el dominio cibernético en los mismos términos globales comunes a los otros dominios. Sin embargo, algunos diseñadores de política y estrategia en este medio concluyen que en esta comparación nada se repite, nada tiene un seguimiento que confirme las similitudes. En consecuencia, al considerarse el espacio digital como dominio, simplemente se necesita determinar su connotación.

En segundo lugar, se debe considerar si 'dominio' implica superioridad, si esta implica que sea absoluta. Si es así, la superioridad en el mar, aire y espacio se puede alcanzar visiblemente, por la experiencia y tecnología adquirida a través de los años. Sin embargo, el ciberespacio presenta tres características del

domino terrestre que son: número de actores, facilidad de penetración y oportunidad para el ocultamiento, lo cual hace que la superioridad en este dominio sea más compleja y difícil de obtener (Kramer, 2009). En consecuencia, se requerirá demostrar en forma clara que somos capaces de ejercer superioridad en el ciberespacio de manera constante, veinticuatro horas al día y siete días a la semana.

Hasta ahora no se ha logrado la capacidad para libramos de la amenaza de las intrusiones maliciosas, que permita la superioridad en el dominio del ciberespacio. Hay varios elementos que debemos considerar para el análisis geopolítico del ciberespacio: operaciones centradas en la red, ataques con redes computacionales, disuasión, influencia, operaciones de estabilidad, doctrina, entrenamiento, logística, personal y finanzas (Kramer, 2009). Todos estos elementos por sus características requieren ser entendidos por el impacto que tiene su accionar en el contexto cibernético a diferencia de los dominios físicos.

- Las operaciones centradas en la red son muy utilizadas y eficientes, sin embargo, no deben considerarse suficientes para el desarrollo de capacidades ya que estaríamos creando vulnerabilidades que pueden ser explotadas por los potenciales adversarios.

- Los ataques con redes computacionales presentan alta clasificación de seguridad que limita las actividades, lo cual hace difícil su integración con otros sistemas. De allí la necesidad de bajar la clasificación sin afectar la capacidad creando vulnerabilidades.

- La disuasión en el ciberespacio podría ser considerada como parte de una disuasión general y del Estado y no como una disuasión específica para el ciberespacio, ya que está muy relacionada con la capacidad de identificación del potencial

"La naturaleza multidimensional de la amenaza en el dominio cibernético demanda de las organizaciones capacidades para la evaluación objetiva de los riesgos mediante la aplicación de software cada vez más novedoso".

Foto: https://local-insurance.ca/insurance-company-ontario/comprehensive-cyber-insurance-elora

"Hasta ahora no se ha logrado la capacidad para librarnos de la amenaza de las intrusiones maliciosas, que permita la superioridad en el dominio del ciberespacio".

agresor y la respuesta adecuada que podría ir más allá del ciberespacio.

- La influencia no necesariamente es proporcional a la capacidad de producir información, de manera que hay varios elementos culturales, políticos y económicos que influyen en las audiencias que se pretenden captar.

- Las operaciones de estabilidad están íntimamente relacionadas con la influencia, ya que el éxito que se persigue con estas dependerá de la capacidad que se tenga de ejercer la influencia necesaria para que las operaciones que se pretenden desarrollar, cuenten con el éxito buscado.

- La doctrina, organización, entrenamiento, logística, personal y finanzas en el pensamiento estratégico del ciberespacio, deberían pensarse como una dimensión comprensiva. Para lograr esto, la asociación público-privada juega un papel muy importante, por la predominancia del sector privado en el ciberespacio. El objetivo sería poder integrar un cuerpo cibernético multidisciplinario de los sectores público y privado para desarrollar las capacidades operativas de influir, atacar, defender y explotar en el terreno operativo del ciberespacio en forma integral, pero también a las instituciones especializadas del Estado relacionadas directamente con el ciberespacio.

En la segunda entrega de la próxima edición, se abordarán en detalle aspectos referentes al ecosistema digital en el contexto internacional, el desenlace de los actores internacionales así como el papel de los organismos internacionales y la cooperación.

Referencias

- Campbell, R.J. (10 de junio del 2015). Cybersecurity Issues for the Bulk Power System. Washington DC Congressional Research Service. Obtenido de www.fas.org/sgp/crs/misc/R43989.pdf

- Choucri, N. (2012). Cyberpolitics in International Relations. Nueva York: HarperCollins.

- Clark, A. y Eddy, R.P. (2017). Warnings Finding Cassandras to Stop Catastrophes. Nueva York: HarperCollins publishers.

- Connell, M. y Vogler, S. (2017). Russia's Approach to Cyber Warfare. CNA Analysis and Solutions. Obtenido de https://www.realcleardefense.com/articles/2017/05/09/russias_approach_to_cyber_warfare_111338.html

- European Commission. (2017). Cybersecurity initiatives: working towards a more secure online environment. Obtenido de http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

- European Commission. (2017). Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level. Obtenido de http://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en

- Friedman, A. y Singer, P. W. (2014). Cybersecurity and Cyberwar what everyone needs to know. Oxford: Oxford University Press.

- Friedman, T. L. (2016). Thank You for Being Late: An optimist's Guide to Thriving in the Age of Acceleration. Nueva York: Farrar, Straus & Giroux.

- Goodman, M. (2015). Future Crimes Everything is Connected Everyone is Vulnerable and What We Can Do about It. Nueva York, EE.UU: Doubleday.

- Gordon, B. (2017). The EU Gets Serious About Cyber: The EU Cybersecurity Act and Other Elements of the Cyber Package. Obtenido de https://www.lexology.com/library/detail.aspx?g=c401bf00-99dd-4a11-8d63-9387f10374bd

- KPMG. (2017). Overview of China's Cybersecurity Law. KPMG. Obtenido de https://

assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

➢ Kramer, Franklin D., et al. (eds.). (2009) Cyberpower and National Security. Washington: National Defense University Press & Potomac Books, Inc.

➢ Lindsay, J., et al. (2015). China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. Oxford: Oxford University Press.

➢ Luo, J., et al. (2014). A software vulnerability rating approach based on the vulnerability database. Journal of Applied Mathematics. Obtenido de https://www.hindawi.com/journals/jam/2014/932397/abs/

➢ Meulen, van der, Nicole, et al. (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, RAND Corporation, European Parliament.

➢ NATO. (2017). Cyber defence. Acceso a https://www.nato.int/cps/en/natohq/topics_78170.htm.

➢ Robles Carrillo, M. (2017). Gobernanza política versus gobernanza tecnológica del ciberespacio, Instituto Español de Estudios Estratégicos. Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO56-2017_Gobernanza_Margarita_Robles.pdf

➢ Schmidt, E. y Cohen, J. (2013). The New Digital Age: Transforming Nations, Businesses and Our Lives. Nueva York: Vintage Company.

➢ Schneier, B. (2015). Data and Goliath The Hidden Battles to Collect Your Data and Control Your World. Nueva York: W. W. Norton & Company, Inc.

➢ Segal, A. (2016). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Era. Nueva York: Public Affairs.

➢ Shea, J. (2018). How is NATO Meeting the Challenge of Cyberspace? PRISM, 7(2), 19-29.

➢ Simon, P. (2013). Too Big to Ignore: The Business Case of Big Data. Nueva Jersey: John Wiley & Sons, Inc.

➢ Singer P.W. y Friedman, A. (2014). Cybersecurity and Cyberwar what everyone needs to know. Oxford: Oxford University Press.

➢ United Nations Office for Disarmament Affairs. (2018). Developments in the field of information and telecommunications in the context of international security. Obtenido de https://www.un.org/disarmament/topics/informationsecurity/

➢ UNLP (2016). Minería de datos aplicada a datos masivos. Obtenido de http://sedici.unlp.edu.ar/handle/10915/52901

➢ U.S. Department of Defense. (2015). The Department of Defense Cyber Strategy. Obtenido de https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

➢ U.S. National Intelligence. (2018). Statement for the record: Worldwide Threat Assessment of the US Intelligence Community. Obtenido de https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-021318.PDF

➢ Vaishnav, C., et al. (2013). "Cyber International Relations as an Integrated System." Environment Systems and Decisions, 33(4), 561–576.

CURRÍCULUM

Dr. Boris Saavedra: Doctor en Paz y Seguridad Internacional, Instituto Universitario Gutiérrez Mellado de la Universidad Nacional de Educación a Distancia en España; y Profesor de Seguridad Nacional, Centro de Estudios Hemisféricos de Defensa William J. Perry, Universidad Nacional de Defensa, Washington, D.C. .

Dra. Luisa Parraguez: Doctora en Relaciones Internacionales, Universidad Nacional Autónoma de México; Investigadora Fulbright, Centro de Estudios Hemisféricos de Defensa William J. Perry, Universidad de la Defensa Nacional, Washington, D.C.; y Profesora Investigadora del Tecnológico de Monterrey, Campus Ciudad de México.