La Ciberseguridad: Análisis político y estratégico*

(Segunda 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

Luego de desglosar en la primera entrega las características estratégicas del dominio cibernético más los elementos estructurales y geopolíticos, en esta segunda entrega se da continuidad a la exposición de otros elementos fundamentales de análisis para el diseño y desarrollo de la política y la estrategia de la ciberseguridad.

El ecosistema digital en el contexto internacional

Debido a su naturaleza, es más que evidente que el ciberespacio no puede considerarse, de manera sensata, como un tema nacional. Es un hecho innegable que el ecosistema digital en muchos aspectos es una manifestación de la globalización y, en consecuencia, debe ser analizado en el marco internacional, ya que los temas fundamentales tales como seguridad y gobernanza, entre otros, tienen sus posibles soluciones con la participación colectiva de los Estados.

Los conflictos cibernéticos son hoy, por naturaleza, globales, dado que las actividades en el espacio digital, lícitas e ilícitas, cruzan las fronteras y rebasan las reglas tradicionales de regulación (Vaishnav, 2013; Schmidt, 2013). Hoy se cuestiona cómo configurar las Relaciones Internacionales en el ciberespacio; qué tipo de soberanía ejerce un Estado en esta zona, qué tipo de influencia y poder político tienen los países, cómo hablar de la seguridad nacional y las fronteras (Choucri, 2012). De la misma manera, debido a que el espacio digital no tiene quién lo regule y en él se mueven múltiples actores (stakeholders), también existe la discusión sobre si todos –gobiernos, empresas, organismos no-gubernamentales, individuos– tienen el derecho a defenderse y tomar medidas ofensivas unilaterales.

"Debido a que el espacio digital no tiene quién lo regule y en él se mueven múltiples actores (stakeholders), también existe la discusión sobre si todos –gobiernos, empresas, organismos no-gubernamentales, individuos– tienen el derecho a defenderse y tomar medidas ofensivas unilaterales".

Por esta misma razón, la gobernanza del ciberespacio se ha convertido en un reto de los países y de los organismos internacionales en determinar quién tiene la autoridad de establecer las leyes en este dominio, qué tipo de leyes y quién tiene el mando para ejecutarlas (Robles Carrillo, 2017). Hasta el momento y en gran medida, las normas han sido de carácter voluntario y las amenazas digitales globales se han enfocado en el espionaje, el sabotaje y la subversión. Además, la agresión cibernética proviene de múltiples fuentes y de variados intereses y esta puede iniciar desde los Estados, de *hacker*s copiones (copy-cat), de grupos criminales y/o de actores políticos independientes. Es así entonces, como una crisis puede generar daños físicos catastróficos en la infraestructura crítica de un país y, aun rastreando las intrusiones de los incidentes, el anonimato y la falta de atribución hacen endebles a todas las naciones. Con la meta de trazar un plan de acción en el espacio cibernético, es menester que cada país identifique sus vulnerabilidades para el manejo de riesgos de los incidentes, y aumente sus capacidades y nivel de resiliencia.

Uno de los grandes retos que enfrentan los países es cómo ejercer la soberanía de un Estado en el espacio cibernético, donde las fronteras físicas y políticas al estilo westfaliano ya no existen. Hoy en día los conflictos en el espacio cibernético son asimétricos, multidimensionales, disruptivos y continuos. Se requiere de una visión de competencia para vislumbrar que, dada esta naturaleza, los conflictos cibernéticos como herramientas utilizadas por los Estados, son más un tema de inteligencia, donde se aprende del adversario y no de una 'guerra' suma-cero (Segal, 2016).

Siguiendo los principios de la teoría de juegos, se opera con la mentalidad de que la meta no es necesariamente aniquilar al adversario porque se entiende que este se reconfigura y regresa mejor informado para penetrar de manera incesante e infinita. Más bien se detiene, boquea, desequilibra, ordena, compartimenta o contiene la intrusión. No obstante, existe el riesgo de que el conflicto escale del ámbito digital al físico, y este cause

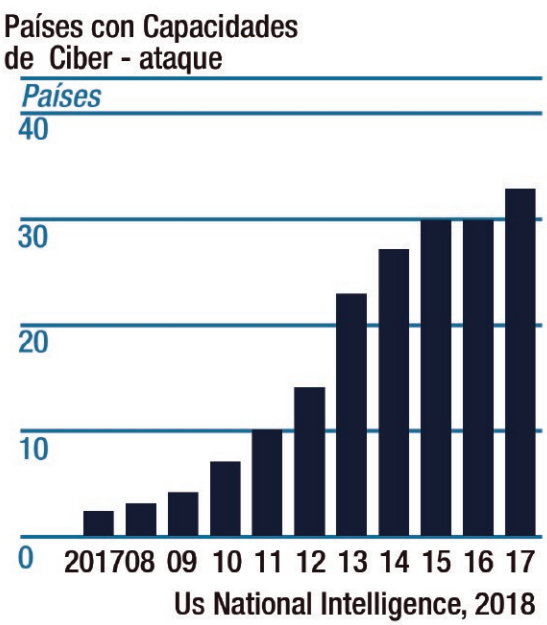
daños a la infraestructura crítica de un país. Los ataques cibernéticos pueden infligir considerables daños a la economía de un país que, a su vez, pueden repercutir de manera negativa en toda la región.

El desenlace de los actores internacionales

De acuerdo con el informe sobre amenazas globales presentado por la Comunidad de Inteligencia de Estados Unidos en febrero 2018, *"la competencia entre países aumentará en este año conforme a las grandes potencias y agresores regionales que explotan tendencias globales complejas."* Las potencias con capacidad cibernética en el mundo han aumentado de menos de 5 en 2007 a más de 30 en 2017 (*véase Tabla 1*), resaltando entre las más agresivas Rusia, China, Corea del Norte e Irán. "Adversarios y actores maliciosos utilizarán todos los instrumentos de Poder Nacional –incluyendo información y medios cibernéticos– para moldear sociedades y mercados, reglas e instituciones internacionales y focos problemáticos regionales para su beneficio".

Rusia sigue siendo un actor enérgico en las relaciones internacionales y en el ciberespacio no se queda atrás; utiliza sus operaciones como herramientas de Estado para lograr sus objetivos estratégicos. Lo hace de manera activa y disruptiva, agregando a su amplio uso de tácticas digitales, las operaciones de intrusión y divulgación de información (*hack* & *leak*), los ataques de denegación de servicio distribuido (DDoS) y, entre otras, los ataques de falsa bandera o sin atribución. La visión del conflicto en el espacio digital del Kremlin es una actividad constante y sin fin y, cada vez más, se apoya en *hacktivistas* y redes criminales en el ciberespacio para ofuscar el tema de atribución (Connell y Vogler, 2017). Al minar datos en la red, busca obtener acceso a todo tipo de información y, en particular, sobre la infraestructura crítica de un país y su estrategia política. Se especula sobre la intervención rusa en las elecciones presidenciales del 2016 en Estados Unidos y de la desinformación en las redes sociales y medios de comunicación (*fake news*). También hay inquietud sobre sus operaciones

Tabla 1



en las elecciones regionales en América Latina, donde en 2018 dos de cada tres países tendrán elecciones.

China se apoya en el espionaje cibernético para avanzar su Seguridad Nacional, política y económica, a la vez que fortalece sus capacidades de ataque y desconfía de las 'fuerzas hostiles extranjeras', en particular, del poder cibernético de Estados Unidos, por el uso ofensivo de sus armas digitales y la recaudación de información de sus empresas como *Microsoft* y *Google* (Lindsay, 2015). Una serie de eventos en 2015 fueron significativos: en mayo, China firmó con Rusia un acuerdo de cooperación en seguridad internacional, para no realizarse ciberataques mutuamente. En julio, China publicó su proyecto de ley de seguridad cibernética y cuando el

"Con la meta de trazar un plan de acción en el espacio cibernético, es menester que cada país identifique sus vulnerabilidades para el manejo de riesgos de los incidentes, y aumente sus capacidades y nivel de resiliencia".

"Siguiendo los principios de la teoría de juegos, se opera con la mentalidad de que la meta no es necesariamente aniquilar al adversario porque se entiende que este se reconfigura y regresa mejor informado para penetrar de manera incesante e infinita".

presidente Xi visitó Washington en septiembre del 2015, se acordó entre estos dos países el no respaldar el robo en línea, de propiedad intelectual. Todo esto disminuyó el flujo de actividades cibernéticas desde la República Popular China, sin embargo, el gigante asiático mantiene una actividad digital constante en todo el mundo y muy especialmente en América Latina (KPMG, 2017).

Asimismo, para mitigar el efecto de las sanciones económicas por sus agresiones militares, Corea del Norte continuará lanzando ataques *DDoS*, trabajando en la eliminación de datos y en el despliegue de secuestro de información (*ransomware*). Sus intenciones de interrumpir o destruir sistemas las ha emprendido como una medida de represalias en contra de sus adversarios que amenazan sus intereses. Al igual que Corea del Norte, Irán está aumentando rápidamente sus capacidades digitales y ve al ciberespacio como un arma para la proyección de sus objetivos estratégicos.

Estados Unidos tiene tanto la capacidad defensiva como la ofensiva en el ciberespacio y este se ha establecido entre uno de sus cinco dominios aparte del mar, la tierra, el aire y el espacio (U.S. Department of Defense, 2017). Se concentra más en conceptualizar el espacio cibernético y busca establecer el equilibrio entre las libertades civiles y la necesidad de cuidar la Seguridad Nacional. Actualmente enfrenta varios desafíos internos, entre ellos: identificar sus vulnerabilidades, permitir el adecuado acceso a la información sin violar las leyes de habeas data, regular la higiene de redes de robots informáticos (botnets), promover la legislación –actualmente inexistente– sobre las medidas ofensivas de las

Foto: https://www.kdisonline.com/the-importance-of-cyber-liability-insurance-for-homeowners-associations/

empresas en caso de recibir ataques, proteger en contra del *hacking* en elecciones y el uso de "noticias falsas" como un arma.

Al igual que Estados Unidos, la Unión Europea (UE) busca la cooperación para equilibrar el dilema de menos libertad con miras a incrementar la seguridad de los países miembros (European Commission, 2017; Gordon, 2017). Las medidas de ciberseguridad están fragmentadas por las diferencias en capacidades operacionales y prioridades estratégicas de los Estados miembros (Meulen, 2015). Israel es propenso a la apertura en el ciberespacio, sin embargo, toma en cuenta la dinámica y las limitaciones que se viven en la región. Es un Estado con límites al acceso del espacio cibernético, donde la vigilancia es menester a su supervivencia, dado que el entorno regional no le permite mayor apertura.

Los Organismos Internacionales y la cooperación

En la Organización de las Naciones Unidas (ONU) hubo un aparente avance en cooperación cuando en 2013 el grupo de Grupo de Expertos Gubernamentales (GGE) en seguridad informática acordó que el Derecho Internacional, especialmente la Carta de las Naciones Unidas, aplicaba a la actividad de los países en el ciberespacio. En 2015, este grupo acordó que se establecieran cuatro normas: la primera, que los Estados no interfirieran en la infraestructura crítica de los demás; la segunda, que no atacaran los equipos nacionales de respuesta a emergencias computacionales (CERT|, por sus siglas en inglés) de otros países; la tercera, apoyar a otros a investigar los ciberataques; y la cuarta, que asumieran la responsabilidad de acciones que se originaran en su territorio. Sin embargo,

> "Una serie de eventos en 2015 fueron significativos: en mayo, China firmó con Rusia un acuerdo de cooperación en seguridad internacional, para no realizarse ciberataques mutuamente".

Foto: https://www.gcheng.com/

"América Latina enfrenta grandes retos, entre ellos un lento crecimiento económico, corrupción y actividad del crimen organizado".

en 2017 el grupo enfrentó un *impasse* a la hora de establecer si el Derecho Internacional le otorgaba a un Estado la facultad de autodefensa y la responsabilidad de tomar medidas de contra ataque. Estados Unidos estaba a favor, mientras que otros países, incluyendo China, Rusia y Cuba, se opusieron a la propuesta argumentando que esta medida militarizaba el ciberespacio y promovía el uso de la fuerza. El GGE del 2017 no logró establecer un consenso en las normas internacionales para el uso del ciberespacio y los Estados han regresado a buscar aliados con quien sumar esfuerzos para proteger sus intereses estratégicos.

La Organización del Tratado del Atlántico Norte (OTAN), como institución internacional y regional, ha optimizado sus capacidades a través del uso de redes de transferencia de información interactivas (*network-centric operations*) para el control de sus operaciones. La seguridad colectiva de la Organización se basa en el reconocimiento que todas las crisis o conflictos en el futuro tendrán una dimensión digital y que se requiere de mayor colaboración entre aliados. La OTAN busca establecer al ciberespacio como un dominio operativo y para esto se apoya en los países que ya lo han establecido así, como es el caso de Estados Unidos, Francia y los Países Bajos; y analiza los casos de Francia y Estonia, que han organizado una fuerza de reserva civil especializada (Shea, 2018).

América Latina enfrenta grandes retos, entre ellos un lento crecimiento económico, corrupción y actividad del crimen organizado. La Organización de Estados Americanos (OEA) a través del Comité Interamericano contra el Terrorismo (CICTE), estableció su Programa de Seguridad Cibernética. Entre sus principales objetivos se encuentran la creación de Equipos de Respuesta a Incidentes (CSIRT), crear una red de alerta hemisférica, apoyar en el diseño de estrategias nacionales de ciberseguridad y el fomento de una cultura cibernética en el Hemisferio. Del 28 de febrero al 1 de marzo del 2018, el CICTE organizó la primera reunión del grupo de trabajo sobre medidas de fomento de cooperación y confianza en el ciberespacio en la sede de la OEA en Washington D.C. donde se discutió, entre otros temas: el uso ampliado del Internet y las TIC; el crecimiento económico y las nuevas formas de compartir información; la promoción de libertades fundamentales; las vulnerabilidades que dan pie al crimen cibernético; la importancia de la cooperación internacional en el hemisferio occidental; los programas de desarrollo de capacidades para prevenir y responder a incidentes cibernéticos, y las medidas a tomar para fomentar la confianza entre los países miembros de la Organización.

En cuanto al diseño de estrategias nacionales, el CICTE ha apoyado con asesoría y recomendaciones a varios países de la región, y aquellos que han presentado estrategias nacionales de seguridad cibernética son: Trinidad y Tobago (2013), Panamá (2013), Jamaica (2015), Colombia (2011 y 2016), Paraguay, Chile y Costa Rica y México (2017). No obstante, hay mucho trabajo por desarrollar en el ámbito político y estratégico en los países y en la región en general.

Conclusiones

El ciberespacio no debe ser apreciado como un agregado de cosas y sus propiedades, ya que trasciende sus componentes para hacerse algo en sí mismo. Por ello demanda una conceptualización única que logre capturar el todo formalmente, a través de una política nacional centrada en la promoción y rápida incorporación de la cultura cibernética definida como la capacidad del Estado para desarrollar y explotar la tecnología. En este orden de ideas, 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.

El análisis del ciberespacio como dominio nos deja en claro, en primer lugar, que la conceptualización y empleo de este espacio tiene una trascendencia importante en su diseño y

función. Bajo esta conceptualización, es posible lograr la ciberseguridad que el Estado demanda, en forma eficiente y eficaz. En segundo lugar, que el ciberespacio como creación del hombre, plantea interrogantes muy complejos por su característica, si lo comparamos con otros dominios. Y, en tercer lugar, que la Seguridad y Defensa en este nuevo espacio requiere un esfuerzo a nivel nacional e internacional, que constituye un verdadero reto histórico de carácter global.

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.

- 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.