ÍNDICE DE PREPARACIÓN CIBERNÉTICA 2.0

UN PLAN PARA LA PREPARACIÓN CIBERNÉTICA: UNA LÍNEA DE BASE Y UN ÍNDICE

Investigadora Principal: Melissa Hathaway

Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri

Noviembre de 2015

POTOMAC INSTITUTE FOR POLICY STUDIES

Publicado por Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA, 22203
www.potomacinstitute.org
Teléfono: 703.525.0770; Fax: 703.525.0299

Correo electrónico: *CyberReadinessIndex2.0@potomacinstitute.org*

Síganos en Twitter:
@CyberReadyIndex

Agradecimientos

El Potomac Institute for Policy Studies desea agradecer a la División de Seguridad Cibernética y Aplicaciones TIC de la Unión Internacional de Telecomunicaciones y al Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) por su apoyo continuo. Los autores también desean agradecer a Sherry Loveless y a Alex Taliesen por su trabajo editorial y de diseño.

ÍNDICE DE PREPARACIÓN CIBERNÉTICA 2.0

UN PLAN PARA LA PREPARACIÓN CIBERNÉTICA: UNA LÍNEA DE BASE Y UN ÍNDICE

TABLA DE CONTENIDO

La traducción al español del CRI 2.0 fue posible gracias
al apoyo del Programa de Seguridad Cibernética de la
Organización de los Estados Americanos (OEA).

ÍNDICE DE PREPARACIÓN CIBERNÉTICA 2.0

UN PLAN PARA LA PREPARACIÓN CIBERNÉTICA: UNA LÍNEA DE BASE Y UN ÍNDICE

Investigadora Principal: Melissa Hathaway
Chris Demchak, Jason Kerben,
Jennifer McArdle, Francesca Spidalieri

El Índice de Preparación Cibernética 2.0 es aumentado del Índice de Preparación Cibernética 1.0, publicado en noviembre de 2013.

INTRODUCCIÓN

Hoy en día, ningún país está preparado cibernéticamente.

Es un hecho que el crecimiento económico mundial depende cada vez más de la rápida adopción de la tecnología de información y comunicación (TIC) y de la conexión de la sociedad a Internet. De hecho, la agenda digital de cada país promete estimular el crecimiento económico, aumentar la eficiencia, mejorar la capacidad y la prestación de servicios, impulsar la innovación y el aumento de la productividad, y promover la buena gobernanza. Sin embargo, la disponibilidad, integridad y resiliencia de esta infraestructura central están en peligro. El volumen, alcance, velocidad y sofisticación de las amenazas a nuestros sistemas e infraestructuras en red son reales y están creciendo. Las violaciones de datos, actividad delictiva, interrupciones de servicio y la destrucción de la propiedad se están convirtiendo en algo común y amenazan la economía de Internet.

Los líderes mundiales entienden que el aumento de la conectividad a Internet conduce al crecimiento económico solo si la infraestructura subyacente y los dispositivos conectados a ella están a salvo y seguros. Por lo tanto, los países deben alinear sus visiones económicas con sus prioridades de seguridad nacional.

Hasta ahora, sin embargo, no ha habido una metodología experiencial integral y comparativa para evaluar la madurez y el compromiso de los países con el aseguramiento de sus servicios e infraestructura nacional cibernéticas de los que dependen su crecimiento y futuro digital. El Índice de Preparación Cibernética o *Cyber Readiness Index (CRI por sus siglas en inglés)* 1.0[1] representó una nueva forma de examinar el problema y fue diseñado para promover el debate internacional e inspirar la acción global para abordar la erosión económica causada por la *inseguridad cibernética*.

Sobre la base del CRI 1.0, el CRI 2.0 examina ciento veinte y cinco países que han adoptado, o están comenzando a adoptar, las TIC e Internet. Luego se aplica una metodología objetiva para evaluar la madurez y el compromiso de cada país con la seguridad cibernética a través de siete elementos esenciales. Mediante la aplicación de esta metodología, un país puede entender mejor sus entrelazamientos de Internet e Infraestructura y las dependencias y vulnerabilidades resultantes.[2] En concreto, el CRI 2.0 evalúa los niveles de preparación de los países para determinados riesgos cibernéticos e identifica las áreas donde los líderes nacionales pueden alterar o refinar la postura actual de su país mediante el aprovechamiento o el cambio de las leyes, políticas, normas, palancas de mercado (por ejemplo, incentivos y regulaciones), y la implementación de otras iniciativas para preservar la seguridad de su conectividad y proteger el valor de su economía.

ANTECEDENTES

La mayoría de los países han adoptado estrategias económicas habilitadas por las TIC y están trabajando para proporcionar comunicaciones rápidas, confiables y asequibles a todos los hogares y empresas para lograr que su sociedad de la información avance hacia la era digital.[3] Iniciativas de modernización como gobierno electrónico, banca electrónica, salud electrónica, aprendizaje electrónico, redes eléctricas de última generación, y la automatización de los elementos de la infraestructura de transporte y otros servicios esenciales están en la cima de la agenda económica de la mayoría de los países. Por ejemplo, la estrategia de Internet Plus de China busca fomentar activamente el desarrollo sano del comercio electrónico, redes industriales y la banca por Internet, así como facilitar el crecimiento de nuevas industrias y la expansión de la huella de Internet internacional de sus empresas.[4] Al igual que muchos otros países, China considera el Internet como una clave para sus futuras oportunidades de crecimiento y desarrollo. Del mismo modo, el Primer Ministro Modi de la India expuso su visión de transformar su país en una "economía del conocimiento facultado digitalmente", mediante el aprovechamiento de la competencia en la tecnología de información (IT) de la India, aclamada a nivel mundial, para crear puestos de trabajo en TI, telecomunicaciones y en los mercados de dispositivos electrónicos. Además, la India pretende convertirse en un innovador en soluciones TIC para la salud, la gestión del conocimiento y mercados financieros.[5] Por último, la Comisión Europea está trabajando para crear un mercado único significativo para servicios digitales que puedan permitir la libre circulación de bienes, servicios, capital y empresas. Se estima que la implementación exitosa de esta "estrategia para el mercado único digital" resultará en un crecimiento del PIB de unos € 415 000 millones adicionales al año en toda Europa.[6]

Los gobiernos, en particular en los países en desarrollo, están presionando para que haya estrategias de adopción de las TIC aún más agresivas para proporcionar servicios adicionales a millones de ciudadanos con el fin de impulsar y profundizar más rápidamente los avances económicos.[7] De hecho, el Banco Mundial estima que por cada 10 por ciento de la población conectada a Internet, el PIB

Los países deben alinear sus visiones económicas nacionales con sus prioridades de seguridad nacional.

crece en un 1 a 2 por ciento.[8] Por otra parte, investigación reciente sugiere que existe un creciente reconocimiento entre los gobiernos y las empresas que aprovechar el Internet y las TIC mejorará su competitividad y el bienestar social a largo plazo, lo que podría contribuir hasta en un 8 por ciento al PIB de una nación.[9] Algunos informes hasta sugieren que la modernización de los sistemas industriales (por ejemplo, redes de energía eléctrica, oleoductos y gasoductos, manufactura, etc.) representa una participación de 46 por ciento de la economía global, y podría aumentar hasta un 50 por ciento en los próximos diez años.[10]

Las naciones no pueden permitirse el lujo de ignorar esta oportunidad económica. Pero pocos están teniendo en cuenta el impacto y los costos económicos de los servicios críticos menos resilientes, la exposición/violación de la privacidad de los ciudadanos, el robo de datos privados corporativos y secretos de estado, y el impacto del fraude electrónico y el delito electrónico, todo lo cual conduce a inestabilidad de la seguridad económica y nacional. En pocas palabras, la *inseguridad* cibernética es un impuesto al crecimiento.[11]

Por ejemplo, se estima que el Grupo de los Veinte (G-20) han perdido dos punto cinco millones de puestos de trabajo debido a la falsificación y la piratería, y que los gobiernos y los consumidores pierden US $ 125 000 millones anuales, incluidas las pérdidas en ingresos fiscales.[12] Estados Unidos estima en US $ 300 000 millones el impacto anual del robo a la propiedad intelectual (PI) internacional en la economía estadounidense. Esto corresponde a un 1 por ciento de su PIB.[13] Otros estudios realizados por los Países Bajos, Reino Unido y Alemania estiman pérdidas similares en el PIB. Ninguna nación puede darse el lujo de perder ni un 1 por ciento de su PIB debido a actividades ilícitas cibernéticas. Sin embargo, a medida que los países siguen adoptando la conectividad de Internet y de las TIC, la exposición, los riesgos concomitantes y los costos económicos aumentarán exponencialmente si no se ponen la seguridad y la resistencia en el centro de sus estrategias de modernización.

La inseguridad cibernética es un impuesto al crecimiento.

Sociedades conectadas y resilientes deben impulsar la modernización teniendo en el centro la seguridad.

La medición de dichas pérdidas a la economía obligará a los líderes nacionales a alinear mejor la agenda de seguridad nacional de su país con su agenda económica e invertir en el valor derivado de ambos.[14] Al hacer transparentes las pérdidas económicas causadas por la inseguridad cibernética se puede despertar el interés nacional y mundial para hacer frente a esta erosión económica. El CRI 2.0 establece un marco para orientar a los países en la búsqueda, de forma segura, del crecimiento económico de una sociedad conectada, resiliente y mejorada por las TIC.

ÍNDICE DE PREPARACIÓN CIBERNÉTICA 2.0– LA METODOLOGÍA

El CRI 2.0 tiene dos componentes principales: en primer lugar, está diseñado para informar a los líderes nacionales de las medidas que deben tener en cuenta para proteger a sus países cada vez más conectados y el potencial

de crecimiento del PIB, mediante la evaluación objetiva de la madurez y el compromiso de cada país con la seguridad cibernética y la resiliencia. En segundo lugar, el CRI 2.0 define lo que significa para un país estar "preparado cibernéticamente" y establece los componentes básicos de la preparación cibernética en un plan accionable que sea seguido por los países. La metodología CRI 2.0 representa una herramienta útil, única y fácil de usar para evaluar la brecha entre la postura de seguridad cibernética actual de una nación y las capacidades cibernéticas nacionales necesarias para lograr su visión económica. El modelo desarrollado y empleado para este análisis incluye más de setenta indicadores de datos únicos a través de los siete índices siguientes:

1. Estrategia Nacional;
2. Respuesta de Incidentes;
3. Delito electrónico y aplicación de la ley;
4. Intercambio de información;
5. Inversión en investigación y desarrollo (I+D);
6. Diplomacia y comercio; y
7. Defensa y respuesta a las crisis.

Las evaluaciones basadas en hechos para cada país se apoyan en fuentes primarias, y cada punto de datos único se basa en investigación y documentación empírica. Los países se evalúan en cada indicador a través de tres niveles de preparación cibernética: evidencia insuficiente, parcialmente operativa o totalmente operativa.

Se está aplicando la metodología CRI 2.0 para evaluar la preparación cibernética de ciento veinte y cinco países, mediante la evaluación de la madurez y el compromiso de cada país con la seguridad cibernética y los servicios e infraestructuras resilientes (Figura 1 y Tabla 1).

La selección de país incluye los setenta y cinco primeros países del *Índice de Desarrollo TIC (IDI)* de la Unión Internacional de Telecomunicaciones (UIT) para hacer énfasis en la importancia de la conectividad. Se añadieron miembros de las economías del G-20, ya que representan el 90 por ciento del PIB mundial, el 80 por ciento del comercio internacional, el 64 por ciento de la población mundial y el 84 por ciento de todas las emisiones de combustibles fósiles.

Evidencia insuficiente: se carece de pruebas o hace falta localizarlas. Es posible, sin embargo, que existan datos, pero todavía o no están disponibles para el público o son confidenciales.

Parcialmente operativa: hay evidencia de políticas, actividades y/o financiación, pero la actividad puede ser inmadura, incompleta o encontrarse todavía en las primeras etapas de desarrollo. Si bien se pueden observar estas iniciativas, su funcionalidad puede ser difícil de medir.

Totalmente operativa: hay pruebas suficientes para observar y medir una actividad madura, funcional.[15]

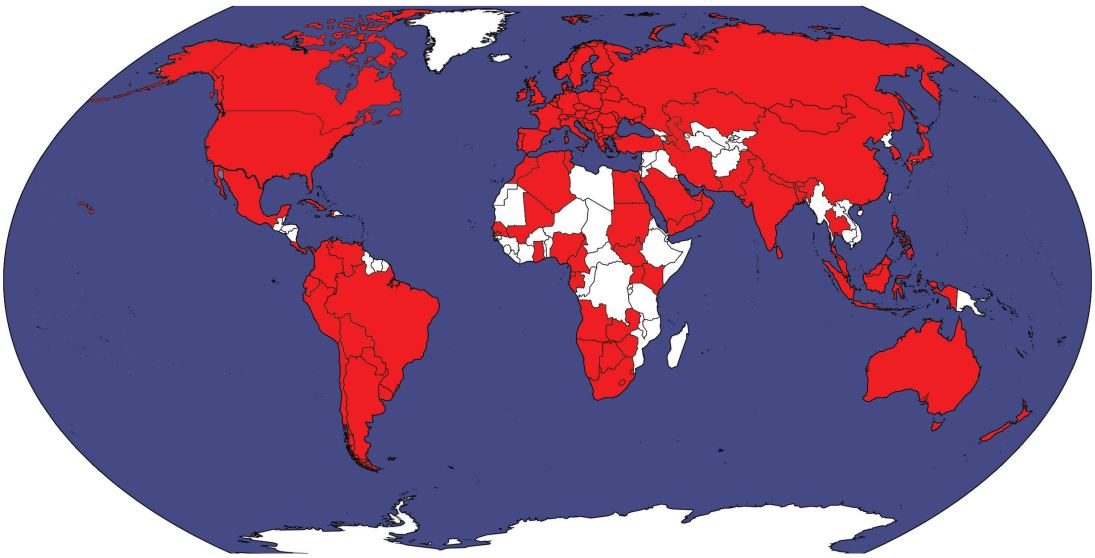

Figura 1: CRI 2.0 Selección de país

Alemania	Catar	Grecia	Méjico	Senegal
Andorra	Chile	Hong Kong	Moldavia	Serbia
Angola	China	Hungría	Mónaco	Seychelles
Antigua y Barbados	Chipre	India	Mongolia	Singapur
Arabia Saudita	Colombia	Indonesia	Montenegro	Sri Lanka
Argelia	Corea del Sur	Irlanda	Namibia	Sudáfrica
Argentina	Costa Rica	Irán	Nepal	Sudán
Armenia	Croacia	Islandia	Nigeria	Suecia
Australia	Cuba	Israel	Noruega	Suiza
Austria	Dinamarca	Italia	Nueva Zelanda	Suazilandia
Azerbaiyán	Ecuador	Japón	Omán	Tailandia
Bahréin	Egipto	Kazajstán	Países Bajos	Taiwán
Bangladesh	Emiratos Árabes Unidos	Kenia	Pakistán	Trinidad y Tobago
Barbados	Eslovaquia	Lesoto	Panamá	Túnez
Bélgica	Eslovenia	Letonia	Paraguay	Turquía
Bután	España	Líbano	Perú	Ucrania
Bielorrusia	Estados Unidos de América	Lituania	Polonia	Uganda
Bolivia	Estonia	Luxemburgo	Portugal	Uruguay
Bosnia-Herzegovina	ex República Yugoslava de Macedonia	Macao, China	Reino Unido	Uzbekistán
Botsuana	Filipinas	Malasia	República Checa	Venezuela
Brasil	Finlandia	Maldivas	República Kirguisa	Vietnam
Brunei Darussalam	Francia	Malí	Rumania	Yemen
Bulgaria	Gabón	Malta	Rusia	Yibutí
Camerún	Gambia	Marruecos	Saint Kitts y Nevis	Zimbabue
Canadá	Ghana	Mauricio	San Vicente y Granada	Zambia

Tabla 1: CRI 2.0 Selección de país

Para ser regionalmente representativos y globalmente incluyentes, se seleccionaron países adicionales de: la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Comunidad Económica Africana (CEA), la Asociación Latinoamericana de Integración (ALADI), la Cooperación Económica Asia-Pacífico (APEC), la Cooperación Económica Regional de Asia Central (CAREC), el Consejo de Cooperación del Golfo (CCG), la Asociación para la Cooperación Regional de Asia Meridional (SAARC) y la Federación de Comercio de América del Norte (NAFTA). Países de estos grupos económicos regionales están representados en el IDI, y a veces también se incluyen en el *Network Readiness Index* del Foro Económico Mundial (WEF). Esto asegura que todos los países seleccionados están adoptando las TIC y están invirtiendo en servicios de Internet accesibles y asequibles para promover el crecimiento económico.

Teniendo en cuenta que el CCG no representa el Oriente Medio, también se incluyeron tres estados que tienen la clasificación más alta del PIB fuera del GCC: Irán, Yemen y Líbano.[16]

Esta sección transversal de ciento veinte y cinco países representa una parte importante del mundo y muestra la naturaleza diversa y representativa de los criterios de selección de país del CRI 2.0.

El enfoque del CRI 2.0 en la interconexión entre la economía y la seguridad (o la falta de esta) proporciona una base sólida para que cada país evalúe su madurez de seguridad cibernética y sirve como marco para informar a la política y estrategia, las iniciativas institucionales y operativas, los requisitos de recursos, la formulación reglamentaria y legislativa, y la ejecución de apalancamiento del mercado diverso. La implementación del CRI 2.0 aumentará la concienciación sobre la conexión entre un ciberespacio sostenible y el crecimiento del PIB de cada país, teniendo en cuenta que es probable que el futuro del PIB de un país esté cada vez más dominado tecnológicamente y relacionado con Internet. Por otra parte, se crea la base para la comprensión de la erosión económica causada por la inseguridad cibernética y el grado en que las preocupaciones de seguridad nacional se consideran un componente de la agenda digital y económica de un país. Esta metodología puede llevar a la toma de decisiones basadas analíticamente sobre cómo responder y/o estar adelante del problema.

Por último, el CRI 2.0 les proporciona a entidades internacionales como la UIT, el Foro Económico Mundial, la Organización de Estados Americanos (OEA), el Banco Interamericano de Desarrollo (BID), el Banco Mundial, y otros, un marco y un enfoque complementario a sus respectivas iniciativas y debates internacionales.

A continuación se presenta una descripción detallada de los siete elementos esenciales de la metodología CRI 2.0. Cada sección contiene un elemento esencial con al menos diez indicadores de apoyo para la evaluación que, cuando se combinan, representan un modelo de preparación cibernética de un país. Además, se proporcionan ejemplos de países que ilustran soluciones innovadoras y multiculturales para poder estar cibernéticamente preparados. Si bien estos ejemplos no son de ninguna manera exhaustiva, sí hacen énfasis en enfoques particulares a nivel de país.

1. ESTRATEGIA NACIONAL

La primera área *–y la más importante–* que revela la preparación cibernética de un país es

la articulación y la publicación de una Estrategia Nacional de Seguridad Cibernética que alinea la visión económica del país con sus imperativos de seguridad nacional. El Internet, las redes de banda ancha, las aplicaciones móviles, los servicios de TI, y el software y hardware constituyen los cimientos de la economía digital y el futuro digital de un país.[17] El Internet y las TIC se han convertido en la columna vertebral de las plataformas de la familia (por ejemplo, Facebook™, Twitter™, Instagram™, Renren™, VKontakte™, etc.), los motores de negocios, servicios e infraestructuras críticas y la economía global.[18] La interdependencia y la híper-conectividad están presentes en cada sector. Por ejemplo, la manufactura avanzada utiliza sistemas de control industrial y robótica para aumentar la productividad y disminuir la necesidad de intervención manual. La agricultura moderna incorpora dispositivos del protocolo de Internet (IP) en los cultivos para determinar las necesidades de fertilizantes y ajustar los suministros de agua. También se les coloca dispositivos IP al ganado para determinar dónde pastan los animales y dónde consumen agua, y de ese modo evalúan la salud de los animales de forma casi constante. El comercio electrónico, que es el libre flujo de bienes y servicios a través de fronteras, está desplazando el papel de las tiendas tradicionales, ofreciendo una gran variedad de artículos directamente a la puerta de los compradores en línea poco después de hacer un pedido en línea. Los sistemas de transporte ahora utilizan sensores, dispositivos móviles y quioscos no tripulados para gestionar el tráfico y poner multas. Las ciudades conectadas utilizan dispositivos de localización geográfica para realizar un seguimiento de la velocidad y la ubicación de los automóviles para determinar si un conductor ha obedecido las leyes de la carretera. Iniciativas de modernización en la industria de la salud están digitalizando la historia clínica de los ciudadanos y utilizan la computación basada en la nube para permitir un acceso rápido a los registros de salud en cualquier parte del mundo. La telemedicina utiliza Internet de alta velocidad para ofrecer asesoramiento y servicios médicos a las zonas marginadas. Por último, los sistemas financieros intercambian billones de dólares al día, los mercados de productos básicos comercian utilizando moneda digital y la banca por Internet está sustituyendo la necesidad de contar con bancos locales, físicos.

Las amenazas a las infraestructuras en red están en aumento. Los países están comenzando a entender estas amenazas y están formulando la necesidad de tener una protección de infraestructuras, protección de datos, defensa de la patria y otros descriptores. Una estrategia integral de seguridad cibernética nacional necesita describir las amenazas para el país en términos económicos, y diseñar los pasos, programas e iniciativas necesarias que deben llevarse a cabo para abordar esas amenazas y proteger la conectividad a Internet y las TIC utilizadas por los ciudadanos y las organizaciones públicas y privadas.[19] La estrategia debe basarse en el potencial económico de Internet y adopción de las TIC e incluir las iniciativas que ayuden a reducir la erosión del PIB causada por las amenazas cibernéticas, así como aumentar la seguridad y la resiliencia del país en su conjunto.

Las estrategias nacionales de seguridad cibernética deben reflejar la importancia económica de la seguridad cibernética.

Una Estrategia de Seguridad Cibernética Nacional válida no debe estar articulada simplemente. Debe ser accionable. Hoy en día, los temas principales reflejados en la mayoría de las estrategias incluyen: la definición de la autoridad organizativa y posicional al interior del gobierno; el fomento de la sensibilización y la educación entre los ciudadanos; la construcción de una capacidad de respuesta de incidentes y gestión de crisis; la ampliación de la capacidad de las fuerzas de la ley para abordar la tasa de delitos cibernéticos; la facilitación de las asociaciones público-privadas y el desarrollo de intercambios de información de confianza; y la destinación de recursos hacia I+D y la agenda de innovación. Muchas estrategias comienzan con estadísticas, mediante la cuantificación del volumen de incidentes y la tasa de infección de infraestructura, y la definición de la variedad de amenazas. Los datos se utilizan para justificar la atribución de responsabilidades y una mayor financiación para las misiones y organizaciones. Estas estrategias rara vez les dan prioridad a los servicios e infraestructuras que están en mayor riesgo, y tampoco alinean las medidas de seguridad y las necesidades de recursos necesarios para reducir la exposición y las pérdidas económicas. Una Estrategia Nacional de Seguridad Cibernética apropiada debe plantear el problema o problemas estratégico (s) en términos económicos; identificar y capacitar a la autoridad competente[20] que es responsable de la ejecución de la estrategia; incluir objetivos específicos, medibles, alcanzables, basados en los resultados y basados en el tiempo en un plan de ejecución; y reconocer la necesidad de comprometer recursos limitados (por ejemplo, voluntad política, dinero, tiempo y personas) en un entorno competitivo para lograr la seguridad necesaria y los resultados económicos.

Al menos sesenta y siete países (y otros que están en desarrollo) ya han publicado su estrategia de seguridad cibernética, trazando los pasos clave que deberán aumentar su seguridad nacional y resiliencia.[21] Muchos otros tienen estrategias nacionales (no relacionadas específicamente con la seguridad cibernética) que guían y coordinan sus esfuerzos para avanzar en su postura de seguridad cibernética. Sin embargo, son pocos los países que están conectando explícitamente sus agendas de seguridad tanto económica como nacional, y abordando específicamente la importancia económica de la seguridad cibernética. Son menos aún los países que están construyendo estrategias de acciones concretas. Por lo tanto, todos los países tienen la oportunidad de revisar o desarrollar sus estrategias de manera que se refleje la importancia económica de la seguridad cibernética.

Los elementos de una estrategia de seguridad cibernética nacional integral deben incluir:

Declaración:

A. La publicación de una estrategia de seguridad cibernética nacional que incluya las oportunidades económicas y los riesgos asociados a la implantación de las TIC;

Organización:

A. La designación de una autoridad competente y la delimitación clara de su posición de autoridad;

B. La identificación de las entidades gubernamentales clave afectadas por, y/o responsables de, la ejecución del plan nacional de seguridad cibernética;

C. La identificación de las entidades del sector comercial afectadas por, y/o responsables de, la ejecución del plan nacional de

seguridad cibernética (reconociendo dependencias del sector comercial);

Recursos:

A. La identificación de los recursos financieros y humanos solicitados y asignados para la ejecución del plan;

B. La identificación del porcentaje del PIB que se espera que se ganará o perderá (en términos generales) por la ejecución del plan;

Implementación:

A. La identificación de los mecanismos necesarios para asegurar la infraestructura cibernética crítica y adopción de las TIC;

B. La identificación de los servicios críticos (no las infraestructuras críticas) que el plan pretende hacer más seguro y resiliente; y

C. La identificación de las normas nacionales para la continuidad de los acuerdos de servicio (veinticuatro horas/siete días a la semana) y los requisitos de presentación de informes para cada corte de servicio, industria e infraestructura crítica.

Los hallazgos de este elemento esencial, al igual que con las otras seis áreas, representan una instantánea en el tiempo de un paisaje dinámico y cambiante. A medida que los países continúan desarrollando sus estrategias de seguridad cibernética nacionales, las actualizaciones de este elemento esencial reflejarán esos cambios y monitorearán, rastrearán y evaluarán los avances inherentes y notables. Así, el CRI 2.0 continuará proporcionando un modelo con nuevos ejemplos para informar a los demás en la formulación o revisión de sus estrategias.

2. RESPUESTA A INCIDENTES

El segundo elemento esencial que demuestra la preparación cibernética de un país tiene que ver con el establecimiento y mantenimiento de una capacidad de respuesta efectiva ante un incidente nacional. A menudo, esta capacidad se identifica con tener uno o más Equipos de Respuesta a Incidentes de Seguridad Informática Nacional (los CSIRT Nacionales) o Equipos de Respuesta a Emergencias Informáticas (los CERT) –en adelante denominados colectivamente los CSIRT– responsables de la gestión de respuesta a incidentes en caso de la ocurrencia de catástrofes naturales o desastres de origen humano relacionados con la cibernética que afectan los servicios e infraestructuras de información críticas.[22] En la actualidad, se han establecido ciento dos CSIRT nacionales en todo el mundo y otros cuatro CSIRT están en desarrollo.[23] Los equipos CSIRT suelen estar formados por una mezcla de expertos en seguridad de TI y profesionales de la academia, el sector privado y el gobierno. Además de proporcionar la competencia técnica específica para responder a incidentes cibernéticos de interés nacional, estos equipos de respuesta a incidentes fortalecen la capacidad de un gobierno nacional para entender y combatir las amenazas cibernéticas. Por lo tanto, operar un CSIRT Nacional constituye un componente esencial de la estrategia global de un país para asegurar y mantener los servicios e infraestructuras que son vitales para la seguridad nacional y el crecimiento económico.[24]

Los CSIRT nacionales, a diferencia de los que son estrictamente gubernamentales, sirven a un amplio grupo que incluye desde departamentos del gobierno a entidades privadas y públicas, a ciudadanos. Un CSIRT

nacional bien establecido ofrece servicios reactivos por encima de los demás, es decir, la capacidad de responder a incidentes al contener y mitigarlos a medida que van ocurriendo.[25] Aunque la forma específica de organización de un CSIRT Nacional puede variar y no todos los países pueden tener las mismas necesidades y recursos, estas unidades especializadas y dedicadas deberán proporcionar una serie de funciones tanto proactivas como reactivas, así como servicios preventivos, educativos y de gestión de calidad de la seguridad. Estos servicios incluyen, pero no se limitan a: el establecimiento de la comprensión compartida de las amenazas que enfrenta el país; publicación de alertas y advertencias sobre vulnerabilidades y amenazas cibernéticas; la promoción de la concienciación y las mejores prácticas sobre seguridad cibernética; la identificación, detección, contención y gestión de las amenazas de seguridad y la preparación para posibles incidentes; la coordinación de las actividades de respuesta a incidentes; el análisis de los incidentes de seguridad informática y la proporción de retroalimentación y lecciones aprendidas (para el aprendizaje compartido); la promoción de actividades que aumentan la resiliencia; y el apoyo a la estrategia nacional de seguridad cibernética.

La resiliencia de los servicios críticos es vital para la seguridad nacional y el crecimiento económico.

Por ejemplo, el CSIRT nacional de Singapur (SingCERT) fue desarrollado por la *Infocomm Development Authority* (IDA) de Singapur en cooperación con la Universidad Nacional de Singapur (NUS) en 1997. Este luego se volvió parte de la Agencia de Seguridad Cibernética de Singapur (CSA). SingCERT fue diseñado como un centro integral para la respuesta a incidentes en Singapur para facilitar la detección, resolución y prevención de incidentes relacionados con la seguridad en Internet. SingCERT proporciona asistencia técnica y coordina la respuesta a incidentes de seguridad cibernética, identifica y sigue las tendencias de intrusos cibernéticos, difunde oportunamente información sobre amenazas y coordina con otras agencias de seguridad para resolver incidentes de seguridad informática.[26] SingCERT también ha participado activamente en la organización y ha sido anfitrión de ejercicios de la Asociación de Naciones del Sudeste Asiático (ASEAN) y el Equipo de Respuesta a Emergencias de Asia Pacífico (APCERT). Además, Singapur acoge a siete miembros del Foro de Equipos de Respuesta a Incidentes de Seguridad Informática (FIRST).

Las capacidades de respuesta a incidentes de Brasil se componen de un equipo nacional de respuesta de emergencias informáticas, CERT.BR, y treinta CSIRT regionales divididos en cuatro estados, todos bajo la autoridad del Comité Gestor de Internet en Brasil. Este Comité es una organización de múltiples partes interesadas no gubernamentales y es la entidad principal responsable de la defensa de la red y de respuesta a incidentes en Brasil.[27] El CERT.BR de Brasil es responsable de la respuesta a incidentes, la sensibilización, la recopilación de datos sobre las amenazas

cibernéticas y las intrusiones y la coordinación con múltiples partes interesadas que incluyen los CSIRT, la academia y el sector privado. Además, los CSIRT de Brasil incluyen equipos del sector financiero, militar, del gobierno y universidades.[28]

Aparte de los CSIRT nacionales, entidades regionales similares se han establecido para mejorar y coordinar las actividades de respuesta a incidentes dentro de las regiones geográficas específicas. AfricaCERT, por ejemplo, es una organización sin fines de lucro que incluye once países africanos y proporciona un foro para la cooperación y el intercambio de información técnica entre los operadores de las redes conectadas a Internet en la región. Los objetivos principales de AfricaCERT incluyen pero no se limitan a: la coordinación de la cooperación entre los CSIRT africanos para manejar incidentes de seguridad informática; la contribución al establecimiento de CSIRT en países que actualmente carecen de las capacidades de respuesta a incidentes; el fomento y apoyo a la prevención de incidentes y programas educativos de extensión en materia de seguridad TIC; el fomento del intercambio de información; y la promoción de las mejores prácticas para la seguridad cibernética. Del mismo modo, APCERT comprende una red de veintiocho CERT miembros y otros expertos en seguridad de confianza en la región y su objetivo es mejorar el conocimiento y competencias en relación con los incidentes de seguridad informática y mejorar la capacidad de respuesta a incidentes en toda la región Asia-Pacífico.[29] La misión de APCERT es la búsqueda de un ciberespacio "limpio, seguro y confiable" a través de la colaboración global. Con el fin de comunicar de manera efectiva sobre las amenazas cibernéticas, el marco organizativo de APCERT se basa en un sistema de punto de contacto (POC), en el que cada uno de los países delega a un miembro APCERT para servir como un POC en situaciones de emergencia, a fin de ayudar a facilitar la respuesta oportuna.[30] Asimismo, el Equipo de Respuesta de Emergencia Informática de la Organización de Cooperación Islámica (OCI-CERT) –que incluye los estados miembros en el sudeste de Asia, el sur de Asia, Oriente Medio, África y Asia Central– también trabaja para mejorar la colaboración entre los CERT de los Estados miembros y de la OCI-CERT.

Además de desarrollar capacidades de respuesta a incidentes, los países también están participando en ejercicios de respuesta a incidentes cibernéticos. Ejercicios de respuesta a incidentes cibernéticos ayudan a los países en la práctica y desarrollo de habilidades para la gestión eficaz de las crisis y verificar la capacidad operativa de un CSIRT para responder bajo presión. Por ejemplo, en noviembre de 2011, el poder ejecutivo alemán realizó un ejercicio de un día sobre Planeación/ Preparación de crisis. El objetivo del ejercicio era practicar procedimientos de respuesta del gobierno ante un ataque múltiple que incluyó: ataques de denegación de servicio distribuido (DDoS) contra las infraestructuras críticas; la inyección de malware en el sistema bancario, lo que provocaría una crisis con cajeros automáticos y tarjetas de crédito; y la inserción de falso tráfico dentro del sistema de control del tráfico aéreo.[31] La Agencia Sueca de Contingencias Civiles (MSB), el *Post and Telecom Authority* (PTS) y el *National Defence Radio Establishment* (FRA) también organizan regularmente cursos cooperativos de Director de Aseguramiento de la Información (CIAO) para MSB, PTS y los empleados de FRA que trabajan en niveles de alta dirección. El curso culmina en un ejercicio cumbre –una simulación de gestión de crisis cibernética– que incluye a actores públicos y privados clave en el proceso

de toma de decisiones y también a oficiales del Parlamento y Directores Ejecutivos (CEO) de empresas encargadas de los servicios críticos suecos. El ejercicio destaca las deficiencias políticas y legales cruciales, al tiempo que educa a todos los participantes sobre la seguridad cibernética.[32] Además, la República Checa llevó a cabo un ejercicio de respuesta a incidentes en octubre 2015 que se centró en las amenazas a la infraestructura crítica, con un énfasis específico en las centrales nucleares.[33] Sin embargo, algunos países están llevando a cabo ejercicios de reacción en caso de incidentes cibernéticos. Por ejemplo, la Presidenta Park Geun-hye de Corea del Sur ordenó simulacros de guerra cibernética y capacitación para todo el personal, como resultado de malware encontrado en múltiples plantas de Korea Hydro and Nuclear Power (KHNP).[34]

Además, los ejercicios internacionales ponen a prueba las capacidades de respuesta a incidentes operacionales, mientras adelantan la simulación de la cooperación entre los países. Estados Unidos, por ejemplo, realiza un ejercicio bianual de Tormenta Cibernética que busca fortalecer la preparación cibernética en los sectores público y privado. Cada ejercicio de Tormenta Cibernética se construye sobre las lecciones aprendidas de incidentes anteriores de la vida real, para garantizar que los participantes tengan la oportunidad de practicar la respuesta a incidentes ante incidentes cibernéticos cada vez más sofisticados. La Tormenta Cibernética de 2016 incluirá dieciséis estados, once países y catorce agencias federales.[35] La Unión Europea también tiene ejercicios bianuales de respuesta a incidentes cibernéticos entre los Estados miembros y el sector privado, titulado *Cyber Europe* (Europa cibernética).[36] Durante un ejercicio cibernético de veinticuatro horas en 2014, *Cyber Europe* permitió que casi todos los estados miembros de la UE pusieran a prueba su capacidad de reacción frente a un máximo de dos mil ataques cibernéticos de la vida real, que incluyó DDoS, ataques de desfiguración de la web, ex filtración de datos y ataques cibernéticos contra la infraestructura crítica.[37] Por otra parte, la Agencia Europea de Defensa (EDA) y la Organización del Tratado de América del Norte (OTAN) también llevan a cabo ejercicios de gestión de crisis cibernética complejos en toda la región, con el objetivo de fortalecer la capacidad de respuesta a incidentes cibernéticos entre los Estados miembros y la comprensión de las dependencias transfronterizas.[38] EE.UU. y el Reino Unido también ha anunciado recientemente que harán pruebas sobre cómo responderían los centros financieros a ambos lados del Atlántico a un ataque cibernético masivo. El ejercicio se desarrollará en noviembre de 2015 y pondrá a prueba la respuesta del país y la coordinación y la comunicación transatlántica.[39]

También se pueden utilizar CSIRT nacionales como un mecanismo para la generación de confianza entre los países y el fomento a la cooperación. Por ejemplo, China, Japón, y Corea –tres países que históricamente han vivido tensiones– han desarrollado una reunión CSIRT anual trilateral para discutir los mecanismos de respuesta a incidentes cibernéticos. Las reuniones han ayudado a infundir confianza, lo que ha resultado en el desarrollo de una "línea directa" cibernética para comunicar sobre incidentes cibernéticos significativos.[40]

Las capacidades y ejercicios de respuesta a incidentes cibernéticos son solo algunas de las capacidades de la línea de base que pueden ayudar a un país, de manera proactiva, a prepararse y mitigar las repercusiones de un incidente mayor cibernético. Los CSIRT pueden ayudar a aumentar la velocidad, la recuperación

y la resiliencia de un país contra las amenazas cibernéticas, y así reducir el impacto económico y operacional general de un ataque cuando ocurre. Algunas de las condiciones previas clave para el despliegue exitoso de estos equipos de respuesta a incidentes son contar con un personal bien capacitado y herramientas eficaces de despliegue rápido. Esto facilita la habilidad de un equipo de respuesta a incidentes de fomentar la cooperación y la coordinación en la prevención de incidentes, habilitar una reacción rápida a incidentes y promover el intercambio de información entre las partes interesadas, tanto a nivel nacional como internacional.

Los elementos de una capacidad apropiada de respuesta a un incidente nacional deben incluir:

Declaración:

A. La publicación de un plan de respuesta a incidentes de emergencias y crisis;

B. La identificación y mapeo de dependencias intersectoriales que aborden la continuidad de las operaciones y los mecanismos de recuperación de desastres;

C. La evidencia de que el plan se ejerce y se actualiza con regularidad;

D. La publicación y difusión de una (s) evaluación (es) nacional (s) de amenaza cibernética en el gobierno, en las infraestructuras críticas y las redes de servicios esenciales;

Organización:

A. La creación de un CSIRT nacional para la gestión de respuesta a incidentes y servir a una amplia circunscripción nacional (más allá del gobierno y los proveedores de infraestructura crítica);

B. La identificación de una red de puntos de contacto nacionales autorizadas para los organismos gubernamentales y regulatorios;

C. La identificación de una red de puntos de contacto nacionales autorizadas para industrias críticas que son esenciales para el funcionamiento y la recuperación de los servicios e infraestructuras críticas;

D. El desarrollo de una advertencia de información y sistema de alerta que pueda ser utilizado por los centros nacionales de crisis/respuesta para recibir, abordar y transmitir información urgente de manera efectiva en el momento oportuno;

Recursos:

A. La identificación de los recursos financieros y humanos solicitados y asignados para el CSIRT Nacional para llevar a cabo su mandato;

B. La identificación de fondos adicionales para activar y poner a prueba regularmente el sistema de aviso de información y alerta, y para medir la resiliencia del país a incidentes y crisis cibernéticas a través de ejercicios de seguridad cibernética nacionales;

Implementación:

A. Una capacidad demostrada en la contención de incidentes, gestión, resiliencia, y procesos de recuperación de los servicios e infraestructuras críticas;

B. Una capacidad demostrada por parte de los centros nacionales de crisis/respuesta para abordar y transmitir alertas de manera oportuna;

C. Evidencia de la existencia de métodos de investigación en curso que analizan las tendencias o grupos de incidentes de seguridad informática de preocupación nacional –el intercambio de agentes o tácticas, técnicas y procedimientos similares– con el fin de identificar patrones; y

D. El desarrollo e implementación de un sistema/programa para probar y medir regularmente la resiliencia de la nación ante los incidentes cibernéticos y las crisis a través de ejercicios de seguridad cibernética nacionales.

Los resultados iniciales de este elemento esencial se basan en los inventarios de los CSIRT nacionales proporcionados por la División CERT de la Universidad Carnegie Mellon (CMU),[41] la Agencia Europea de Seguridad de las Redes y de la Información (ENISA),[42] FIRST[43] y la UIT. Se consultan fuentes primarias y secundarias adicionales, tales como los sitios web de los CSIRT Nacionales y artículos de noticias relacionadas, para determinar si existen las capacidades y si están financiadas. A medida que los países van reconociendo la importancia de establecer CSIRT nacionales, las actualizaciones de este elemento esencial supervisarán, seguirán y evaluarán esos avances.

3. DELITO ELECTRÓNICO Y APLICACIÓN DE LA LEY

El tercer elemento esencial que indica la preparación cibernética de un país se demuestra a través de su compromiso de proteger a su sociedad contra el delito cibernético. Sin embargo, el delito cibernético no es simplemente una cuestión interna; trasciende las fronteras nacionales y, por tanto, requiere soluciones transnacionales. Los países deben mostrar un compromiso *internacional* para proteger a la sociedad contra la delincuencia electrónica. Muy a menudo, esta capacidad se traduce en participación en los foros internacionales dedicados a abordar las cuestiones de delincuencia cibernética internacionales, así como el establecimiento de mecanismos legales y reglamentarios nacionales para combatir el delito cibernético. Las autoridades legales y reglamentarias pertinentes designadas con la realización de tales actividades deben definir lo que constituye un delito cibernético y darle autonomía de las entidades gubernamentales con los mecanismos, conocimientos y recursos para investigar y perseguir eficazmente las actividades de la delincuencia cibernética.

Dos acuerdos de tratados internacionales ayudan a demostrar el compromiso de un país para proteger a la sociedad contra el delito cibernético: la "Convención sobre delito cibernético" del Consejo de Europa y el "Acuerdo de cooperación en materia de garantizar la seguridad de la información internacional" de la Organización de Cooperación de Shanghái. El "Convenio sobre la delincuencia cibernética" del Consejo de Europa, en vigor desde el 1 de julio de 2004 y comúnmente llamado la *Convención de Budapest*, ofrece un mecanismo a través del cual se armonizan las leyes de delitos cibernéticos nacionales divergentes y se fomenta la colaboración policial.[44] La eficacia de la Convención de Budapest es un poco limitada, ya que les permite a los países firmantes implementar selectivamente elementos de

la Convención de Budapest sobre la base de hallazgos que de otra manera "menoscabarían su soberanía, seguridad, orden público u otros intereses esenciales".[45] El "Acuerdo de cooperación en materia de garantizar la seguridad de la información internacional" de la Organización de Cooperación de Shanghái, firmado en 2009 y a veces conocido como el Acuerdo de Ekaterimburgo, tiene principios consistentes con el enfoque de aplicación de la ley de la Convención de Budapest. También busca mejorar la base legal de información y establecer mecanismos prácticos de cooperación entre las partes para garantizar la seguridad de la información internacional.[46] En virtud de estos tratados, los países se comprometen a adoptar una legislación apropiada, fomentar la cooperación internacional y combatir los delitos mediante la facilitación de su detección, investigación y enjuiciamiento tanto a nivel nacional como internacional. El CRI 2.0 acredita a países que han ratificado o se han adherido a cualquiera de estos tratados porque, al hacerlo, un país tiene una obligación y deber específico en su legislación interna para mantener un compromiso en un contexto internacional.

Además de los mecanismos internacionales mencionados anteriormente, existen y se están buscando otros enfoques internacionales, multinacionales y regionales hacia el abordaje de la delincuencia cibernética internacional. Por ejemplo, la Asamblea General de las Naciones Unidas (AGNU) ha aprobado una serie de resoluciones relativas a los delitos cibernéticos, como la "Lucha contra la utilización de la tecnología de la información con fines delictivos" de 2001 y la "Creación de una cultura mundial de seguridad cibernética y protección de infraestructuras críticas" de 2003.[47] En particular, el Grupo de Expertos Gubernamentales (GEG) de las Naciones Unidas, que consta de veinte países, tuvieron un gran avance cuando acordaron cooperar en el enjuiciamiento del uso criminal y terrorista de las TIC. Sus compromisos se codificaron en el informe de junio de 2015 del GEG sobre los avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional.[48] La APEC también llevó a cabo un proyecto de creación de capacidad sobre la delincuencia cibernética para las economías miembros para establecer estructuras legales y crear capacidad para investigar el delito electrónico. Como parte de este proyecto, las economías avanzadas de APEC apoyan otras economías miembros mediante la capacitación de las autoridades legislativas y personal de investigación.[49]

El CRI 2.0 se basa en estos enfoques internacionales, multinacionales y regionales para evaluar la preparación cibernética de un país. Además, el CRI 2.0 también incluye información sobre el país sobre delitos informáticos de la ASEAN y la UIT, entre otros.

Aunque exista la intención de cooperar contra la delincuencia cibernética y es importante la ratificación de los acuerdos de delincuencia cibernética, esto no demuestra necesariamente la disposición a combatir el delito cibernético. Los Estados también deben trabajar para construir proactivamente la capacidad de aplicación de la ley cibernética nacional. Por ejemplo, el Centro Avanzado de Investigación, Desarrollo y Capacitación en Medicina Forense y Derecho Cibernético en la Escuela Nacional de Derecho de la Universidad de la India en Bangalore trabaja para traducir la ley a términos técnicos y viceversa, al proporcionar capacitación y educación a funcionarios judiciales, fiscales, organismos de investigación, personal de seguridad cibernética, tecnólogos y otros. Financiado por el Departamento de

Electrónica y Tecnología de la Información (DeitY) del Ministerio de Comunicaciones y de Tecnología de la Información de la India, el Centro ofrece un componente único y práctico de capacitación en un laboratorio forense cibernético que facilita la rápida comprensión de cuestiones complejas.[50]

Otro ejemplo es el reciente lanzamiento de la Organización Policial Internacional (INTERPOL) de un Complejo Mundial de INTERPOL para la Innovación (CMII) en Singapur. Este servicio les permite a los funcionarios encargados de hacer cumplir la ley asociarse con la industria para desarrollar nuevas técnicas de capacitación y usar herramientas avanzadas para hacer frente a la delincuencia cibernética y aumentar la seguridad cibernética.[51] Por ejemplo, INTERPOL creó un juego de simulación para enseñarles a los funcionarios encargados de hacer cumplir la ley sobre la intersección y el riesgo de la Red Oscura (*Darknet*) y las criptomonedas (*cryptocurrencies*). La Darknet ha permitido el surgimiento de una economía subterránea (ilegal) que vende información personal identificable (PII), inteligencia militar, diseños de armas, malware modular, ataques de día cero, claves y credenciales de cifrado privadas, y muchos otros tipos de datos obtenidos ilegalmente. El primer ejercicio de simulación/capacitación de INTERPOL se llevó a cabo en julio de 2015.[52]

La reducción del número de dispositivos infectados conectados en red es una inversión importante en la lucha contra la delincuencia electrónica.

La delincuencia y el fraude cibernéticos son un impuesto al crecimiento económico.

Además de la creación de capacidad para la aplicación de la ley y contra el delito electrónico, los Estados también deben trabajar para limpiar las infecciones en sus infraestructuras de red, conocidas como botnets.[53] Actualmente, se estima que entre el cinco y doce por ciento de los computadores de todo el mundo están en peligro como parte de una red botnet. El FBI estima que se infectan dieciocho sistemas por segundo a través de los ejércitos de botnets, que causa un estimado de $ 110 000 millones en daños a nivel mundial.[54] Algunos países han trabajado para abordar esta amenaza, con cierto éxito. Por ejemplo, el Proyecto de espacio oscuro del gobierno canadiense conocido como *Advanced Analytics and Dark Space Analysis for Predictive Indicators of Cyber Activity*, liderado por Bell Canada y en el que participó un equipo de expertos de organismos gubernamentales canadienses, instituciones académicas y la industria, elaboró un caso de negocio para una solución de 'tuberías limpias' a las amenazas cibernéticas, al proporcionar un cuerpo convincente de pruebas para apoyar proactivamente la contención de las amenazas a Canadá procedentes de Internet. Los hallazgos del proyecto se constituyeron en el caso de negocio para una estrategia nacional de tuberías limpias y influyeron en la elaboración de una Norma de seguridad cibernética para los proveedores de servicios de telecomunicaciones.[55] Otro ejemplo, en Japón, fue el Centro cibernético limpio (*The Cyber Clean Center*), un esfuerzo financiado a cinco años, operado por el CERT japonés (JPCERT) entre 2006 y 2011.[56] Este Centro fue el resultado de una colaboración interdisciplinaria

entre JP-CERT, varios vendedores de seguridad y proveedores de servicios de Internet (PSI) que creó una "red de la guarda" automatizada contra infección y ataques de malware botnet. También proporcionó soluciones a medida para abordar malware específico en equipos específicos.[57] Las gestiones del Centro cibernético limpio han continuado en Telecom-ISAC Japón.[58] Por último, iCode de Australia, una asociación público-privada a través de la Iniciativa de seguridad de Internet australiano (AISI), tiene como objetivo promover una cultura de seguridad entre los PSI al reducir el número de dispositivos de computación comprometidos en Australia. El iCode anima a todos los PSI australianos a unirse a AISI y les proporciona a los miembros PSI de AISI datos diarios de infección de malware y vulnerabilidad del servicio.[59]

La delincuencia y fraude cibernético son un impuesto al crecimiento económico. La delincuencia cibernética ha llegado a un estimado de $ 445 000 millones en todo el mundo, con un impacto negativo en las economías nacionales de al menos 1 por ciento del PIB y más de doscientos mil puestos de trabajo perdidos.[60] Una inversión en la lucha contra la delincuencia electrónica cibernética y el aumento de la capacidad de las fuerzas de la ley es una inversión necesaria para la economía. Mediante el desarrollo de las capacidades de aplicación de la ley para luchar contra la delincuencia electrónica a través de la ratificación de los documentos de los tratados, la cooperación internacional, el desarrollo de capacidades, la implementación de programas de lucha contra botnets y otras iniciativas, los países pueden mitigar sus riesgos cibernéticos e impulsar el crecimiento económico futuro.

Los elementos esenciales de un compromiso internacional válido a nivel de país para proteger a la sociedad contra la delincuencia cibernética deben incluir:

Declaración:

A. Una compromiso demostrado nacional e internacional para proteger a la sociedad contra el delito cibernético a través de la ratificación de acuerdos internacionales de delincuencia cibernética u otros acuerdos equivalentes en la lucha contra la delincuencia cibernética;

B. Un compromiso demostrado para establecer mecanismos jurídicos y de políticas nacionales para reducir específicamente la actividad delictiva que emana del país y promover mecanismos de coordinación para abordar la delincuencia cibernética internacional y nacional;

Organización:

A. La creación de una capacidad institucional madura para luchar contra la delincuencia cibernética, incluida la formación de jueces de tribunales, fiscales, abogados, agentes del orden, especialistas forenses y otros investigadores;

B. El establecimiento de un organismo de coordinación con la misión y la autoridad principal de asegurar que todos los requisitos internacionales de delito cibernético se están cumpliendo a nivel nacional y a través de líneas jurisdiccionales (es decir, cooperación transfronteriza);

Recursos:

A. La identificación de los recursos financieros y humanos solicitados y asignados para la lucha contra la delincuencia cibernética;

B. El establecimiento de un mecanismo de contabilidad para determinar qué porcentaje del PIB anual se ve afectado por la delincuencia cibernética (pérdida real en moneda real), con el fin de evaluar las compensaciones sistémicas de costo-beneficio nacionales y asignar recursos correspondientes;

Implementación:

A. La evidencia demostrable del compromiso de un país para revisar y actualizar las leyes vigentes y los mecanismos regulatorios de gobernanza, identificar dónde puede haber brechas y superposición de autoridades, y aclarar y darles prioridad a las áreas que requieren de modernización (por ejemplo, leyes vigentes, como la antigua ley del telecomunicaciones);

B. El establecimiento de infracciones penales en el derecho interno para las acciones dirigidas contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes, y datos informáticos, así como el mal uso de este tipo de sistemas, redes, y datos, que incluye la infracción internacional de derechos de autor; y

C. Evidencia demostrable de la efectividad de un país en la reducción de las infecciones que emanan de sus propias infraestructuras y redes (por ejemplo, la creación de iniciativas de remediación de malware y anti-botnet).

Los hallazgos iniciales de este elemento esencial se basan en una revisión de si un país ha ratificado o se ha adherido a la Convención de Budapest o al Acuerdo de Ekaterimburgo de la Organización de Cooperación de Shanghái y si el país es un participante activo en los enfoques regionales, multinacionales o internacionales en el abordaje de la delincuencia cibernética. Además, la actividad botnet actual (tanto de nodos de mando y control como infecciones totales) que emana del país se utiliza para evaluar la eficacia de las iniciativas contra la botnet. El CRI 2.0 se basa en fuentes primarias y secundarias para determinar si un país ha establecido mecanismos legales y reglamentarios, otras actividades de reducción de riesgos, y asignado fondos para asegurar una ejecución exitosa. Las actualizaciones de este elemento esencial supervisarán, realizarán un seguimiento y evaluarán los avances sustantivos y notables.

4. INTERCAMBIO DE INFORMACIÓN

El cuarto criterio que indica la preparación cibernética de un país es su capacidad para establecer y mantener mecanismos de intercambio de información que permitan el intercambio de inteligencia y/o información para la acción entre los gobiernos y los sectores industriales. Las principales actividades tales como la identificación, evaluación y respuesta a los ataques dirigidos –que pueden tener implicaciones significativas para las telecomunicaciones, el comercio y los negocios mundiales– requiere más que mecanismos de vigilancia y de protección tradicionales. A nivel mundial, la mayoría de los gobiernos y organizaciones han establecido programas de intercambio de información para comprender mejor los riesgos planteados por los actores estatales y no estatales y gestionado su exposición a vulnerabilidades e infecciones posteriores y violaciones.

Los mecanismos formales de intercambio de información, similares a algunos de los servicios prestados por los CSIRT y CERT nacionales,

pueden ayudar a fomentar la coordinación en la respuesta a incidentes, facilitar el intercambio en tiempo real de información de amenazas e inteligencia, y ayudar a mejorar la comprensión de cómo los sectores se convierten en objetivo, qué información se pierde y qué métodos se puede utilizar para defender los activos de información. Han surgido al menos cuatro modelos diferentes de intercambio de información para abordar las amenazas cibernéticas y para ayudar a las entidades a asegurar sus activos de información a saber: un modelo (1) impulsado por el gobierno; (2) impulsado por la industria; (3) impulsado por una asociación sin fines de lucro; e (4) impulsado por una asociación híbrida académica, gubernamental, y de la industria. Cada método tiene sus desafíos únicos, como el equilibrio entre la necesidad de intercambio oportuno y accionable de información sobre seguridad cibernética, al tiempo que se protege la confidencialidad de los datos, la protección de las libertades civiles, y la gestión de recursos e intereses financieros y humanos que compiten entre sí. Se requieren dos factores, sin embargo, para que cualquiera de los cuatro modelos tenga éxito: el convencimiento y la confianza, que deben ser respaldados por objetivos, roles, responsabilidades y resultados claramente definidos. En pocas palabras, cuando una parte participa de mala gana o a la defensiva, el éxito será difícil de lograr.[61]

Por otra parte, los interesados deben poder compartir información valiosa sobre incidentes graves, que requiere una definición clara de qué tipo de información debe ser compartida, quién tendrá acceso a la misma, y qué medidas de seguridad se deben tomar para proteger la información una vez que el propietario original la da a conocer. La complejidad de este intercambio de información sensible crece proporcionalmente con el tamaño del grupo, y tal vez de manera exponencial cuando los miembros del grupo son estados soberanos con distintas preocupaciones de seguridad nacional.

Muchos países en particular ya han desarrollado programas sólidos nacionales de intercambio de información que podrían ser aprovechados por otros países como aprendizajes de buenas prácticas. Estos programas tienden a centrarse en la alineación de partes interesadas similares en grupos y, posteriormente, la alineación de los grupos en un programa nacional. Los Países Bajos, por ejemplo, creó el Centro Nacional de Seguridad Cibernética (NCSC), una iniciativa impulsada por el gobierno que se desarrolló a partir del GOVCERT holandés a una exitosa asociación público-privada, encargada de la seguridad digital y el intercambio de información en el país.[62] Una de sus principales tareas es la de supervisar continuamente todas las fuentes (potencialmente) sospechosas en Internet y alertar a las autoridades públicas y las organizaciones sobre cualquier amenaza

El intercambio de información debe basarse en la confianza y la aceptación por parte de todos los interesados.

cibernética identificada. NCSC también está conectado directamente a todos los Centros de Intercambio de Información y Análisis (ISAC) en el país y se comparte la información en virtud del Protocolo Semáforo (TLP), que clasifica la información en cuatro niveles: rojo, amarillo, verde y blanco. El programa holandés de intercambio de información fue modelado basado en el Centro de Coordinación de Seguridad de la Infraestructura Nacional (NISCC) del Reino Unido, que les entregó consejos de seguridad de información enfocada a las empresas nacionales de infraestructuras críticas.[63] Del mismo modo, la Agencia de Promoción de la Tecnología de Información japonesa (IPA) actúa como la autoridad institucional encargada del intercambio de información entre el gobierno y las industrias críticas, y tiene un historial probado de establecer relaciones de confianza con las principales empresas del país y proporcionar inteligencia oportuna y eficaz. Además, IPA trabaja en estrecha colaboración con el Ministerio de Economía, Comercio e Industria (METI), el Centro Nacional de Seguridad de la Información (INEC), y el Equipo de Asesoramiento de Rescate Cibernético (J-CRAT) para responder a los principales incidentes cibernéticos que afectan la infraestructura crítica.[64]

Alternativamente, en EE.UU., el Centro de Intercambio y Análisis de Información de Servicios Financieros (FS-ISAC) –una iniciativa impulsada por la industria y desarrollada por el sector de servicios financieros– ayuda a facilitar la detección, prevención y respuesta a incidentes cibernéticos y actividad de fraude. Ha construido fuertes lazos con los proveedores de servicios financieros; empresas de seguridad comerciales; agencias del gobierno nacionales/federales, estatales y locales; fuerzas de la ley; y otra entidades de confianza para proporcionarles alertas de amenazas cibernéticas confiables y oportunas y otra información crítica a las firmas miembro en todo el mundo. Como parte de estos esfuerzos, FS-ISAC utiliza un protocolo de tráfico diferente para determinar qué públicos pueden y deben recibir información específica.[65] FS-ISAC está ampliando su intercambio de información sobre amenazas a nivel internacional al Reino Unido y Europa. También existen otros ISAC en muchos sectores, pero no son tan eficaces.

La Alianza Nacional de capacitación y análisis forense cibernético (NCFTA) en Estados Unidos es una corporación sin fines de lucro con la misión de facilitar la colaboración entre la industria privada, la academia y la policía para identificar, mitigar y neutralizar las amenazas complejas relacionadas con la cibernética. Además de los representantes de las fuerzas de la ley y de la industria estatal y local, esta iniciativa impulsada por la asociación sin fines de lucro cuenta con representación internacional de Canadá, Australia, Inglaterra, India, Alemania, Países Bajos, Ucrania y Lituania. NCFTA les ofrece el intercambio ágil y oportuno de inteligencia sobre amenaza cibernética a las corporaciones; y también se asocia con expertos en la materia en los sectores académicos, públicos, privados y de aplicación de la ley para mitigar los riesgos y las actividades fraudulentas y reunir las pruebas necesarias para enjuiciar a los delincuentes.[66]

Información procesable en tiempo real es clave para la mitigación de las amenazas informáticas.

Por último, el Centro para Seguridad de la Información y Cibernética (CCIS) de Noruega en Gjøvik University College es una iniciativa conjunta (entre la academia, el gobierno y la industria) y representa otro enfoque para el intercambio de información y la colaboración en materia de seguridad cibernética. CCIS promueve un enfoque sistemático, de todo el país, a la seguridad de la información y cibernética y ofrece un esquema de intercambio de información para salvaguardar la capacidad de la sociedad para detectar, alerta y manejar incidentes cibernéticos graves. Además, apoya la investigación nacional de alta calidad y el desarrollo de soluciones en el campo de la cibernética y la seguridad de la información.

Además de los diversos programas de intercambio de información que están desarrollando los países, las agencias de defensa e inteligencia de la mayoría de los gobiernos recogen valiosa información relacionada con la cibernética, y algunos han comenzado a desclasificar este tipo de inteligencia y compartirla con otras entidades gubernamentales e industrias críticas. De hecho, a menudo es clave el conocimiento de la situación en tiempo real para prevenir o mitigar las amenazas informáticas específicas. Algunos países, como Brasil, han ideado mecanismos para desclasificar (*write-for-release*) información procesable que alerta a otras entidades (públicas y privadas) sobre las vulnerabilidades, amenazas específicas y tácticas, y posibles soluciones defensivas como parte de sus iniciativas de intercambio de información.[67] La mejora de la postura defensiva del país es esencial y algunos países están dispuestos a desclasificar partes de inteligencia para garantizar una mejor seguridad.

La capacidad de un país para intercambiar información accionable, oportuna y precisa, dentro y entre entidades de los sectores públicos y privados, ayuda a reducir las vulnerabilidades y la exposición que posteriormente pueden reducir los riesgos concomitantes. A medida que el intercambio de información aumenta en frecuencia y calidad, las entidades deben poder abordar las amenazas informáticas a sus infraestructuras de red de una manera más rápida y proactiva. Establecer y mantener programas de intercambio de información procesable es una inversión fundamental para el crecimiento.

Los elementos de un programa de intercambio de información procesable, intersectorial y nacional eficaz deben incluir:

Declaración:

A. La articulación y difusión de una política sobre el intercambio de información de todos los sectores que permita el intercambio de inteligencia/información procesable entre los gobiernos y los sectores de la industria;

Organización:

A. La identificación de una estructura institucional que transmita información fidedigna de fuentes gubernamentales a las agencias gubernamentales e industrias críticas (de gobierno a gobierno);

B. La identificación de una estructura institucional que asegure que existan mecanismos (esquemas de informes, tecnología, etc.) para el intercambio intersectorial de información de incidentes (bidireccional), tanto operativo (casi en tiempo real) como forense (post-facto) (gobierno-industria/industria-industria);

C. El establecimiento de un mecanismo impulsado sin fines de lucro o académico para el intercambio de información de la vulnerabilidad, incidente, o solución (modelo alternativo, por ejemplo, NCFTA o la base de datos nacional de vulnerabilidad);[68]

Recursos:

A. La identificación de los recursos financieros y humanos solicitados y asignados para el intercambio de información de autoridad impulsado por el gobierno u otra (s) estructura (s) institucional (es) dedicadas a los mecanismos de intercambio de información;

Implementación:

A. Evidencia demostrable de que los mecanismos de coordinación intersectorial y transversal de interesados, definidos para abordar interdependencias críticas –incluyendo conocimiento de la situación del incidente y gestión de incidentes intersectoriales y transversales de interesados– se mantienen y se ponen a prueba de manera adecuada para un desempeño eficaz; y

B. Evidencia demostrable de la capacidad y los procesos oportunos para la desclasificación por parte del gobierno de información de inteligencia relacionada con la cibernética utilizable y el intercambio con el resto del gobierno e industrias críticas.[69]

Los hallazgos iniciales de este elemento esencial se basan en una revisión de si un país ha establecido el intercambio de información y otros mecanismos de coordinación. Basándose en fuentes primarias y secundarias, el CRI 2.0 determina si existen tales mecanismos y si están financiados adecuadamente. Las actualizaciones de este elemento esencial supervisarán, realizarán un seguimiento y evaluarán los desarrollos sustantivos y notables.

5. INVERSIÓN EN INVESTIGACIÓN Y DESARROLLO

El quinto elemento que demuestra la preparación cibernética de un país es mediante el establecimiento de una prioridad nacional y la inversión en investigación básica y aplicada en seguridad cibernética e iniciativas de las TIC, en general. Los avances en las TIC han revolucionado casi todos los sectores de la economía y han transformado las empresas, los gobiernos, la educación, y la forma en que los ciudadanos viven, trabajan y juegan. Estas innovaciones impulsan el crecimiento económico y pueden mejorar la resiliencia y establecer las condiciones para una fuerte postura de seguridad.

Los gobiernos y las empresas tienen cada uno un papel que desempeñar y pueden combinar el poder de sus presupuestos de I+D para mejorar la próxima generación de soluciones y tecnologías habilitadas por Internet y las TIC. Las empresas y los gobiernos están adoptando Internet móvil, la computación por nube, datos grandes, la computación cuántica y la Internet de las Cosas (IOT), y deben invertir en la confianza, la seguridad y la resiliencia de estos servicios y tecnologías digitales. Al invertir en I+D cibernética y otras innovaciones, los países, las universidades y las empresas pueden mejorar su capacidad para cerrar la brecha entre su inseguridad cibernética y las capacidades del atacante.

Por ejemplo, el programa Horizonte 2020 de la Unión Europea ha asignado un estimado de € 80 000 millones para las iniciativas de investigación y desarrollo tecnológico. Con el principio fundacional de acceso abierto de la UE, el programa tiene la intención de impulsar los resultados de investigación, acelerar la innovación, crear una mayor eficiencia y mejorar la transparencia. Horizonte 2020 tiene tres componentes principales. La primera área se centra en ciencia básica y aplicada, denominada "Ciencia Excelente" y tiene previsto financiar la formación doctoral de otros veinticinco mil candidatos de doctorado durante los próximos siete años. La segunda área se centra en "Liderazgo en tecnologías industriales y habilitantes" con énfasis en las TIC, nanotecnologías, materiales avanzados y el procesamiento, entre otros. La tercera área financia soluciones a problemas sociales y económicos, como la salud, la energía, el transporte y la seguridad. Uno de los criterios de evaluación de esta inversión es la cooperación transnacional entre empresas y soluciones que satisfagan las necesidades paneuropeas.[70]

La innovación I+D en seguridad cibernética debe mejorar la confianza, la seguridad y la resiliencia de nuestra sociedad futura y en red.

Del mismo modo, Estados Unidos prioriza, coordina, y dedica más de $ 4 000 millones anuales a la investigación transversal a través del programa Nacional de Investigación y Desarrollo de Tecnología de la Información (NITRD). Áreas de investigación prioritarias para 2016-2020 incluyen: grandes datos, sistemas físicos cibernéticos, seguridad cibernética e I+D de privacidad, computación de gama alta e intercambio de espectro de forma inalámbrica.[71] El programa NITRD es la fuente principal de Estados Unidos de trabajo financiado por el gobierno federal en tecnologías avanzadas de la información en computación, redes y software. El programa busca acelerar el desarrollo y despliegue de tecnologías avanzadas de la información para mejorar la defensa nacional y la seguridad nacional, así como mejorar la productividad de Estados Unidos y la competitividad económica. Además, la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA), la Actividad de Proyectos de Investigación Avanzada de la Inteligencia (IARPA), y la Agencia de Proyectos de Investigación Avanzada de la Seguridad Nacional (HSARPA) también han dedicado financiación a la I+D cibernética. Sin embargo, si se sumara todo el presupuesto en I+D cibernética, la cantidad total seguiría siendo el equivalente a menos del 1 por ciento del PIB de Estados Unidos. En base a la magnitud de los riesgos actuales y futuros cibernéticos de Estados Unidos, el 1 por ciento del PIB no es suficiente para cerrar la brecha de la inseguridad cibernética.

Otras iniciativas patrocinadas por el gobierno fomentan la innovación en seguridad cibernética ofreciendo incentivos de mercado, tales como créditos fiscales por I+D. Por ejemplo, reconociendo que estimular la inversión institucional y corporativa a menudo requiere el apoyo y el compromiso del Gobierno, Israel recientemente aprobó desgravaciones fiscales significativas para las empresas de defensa cibernética que se unan y establezcan actividades en su parque nacional cibernético en Be'er Sheva.[72] Al fomentar un ecosistema único de industria, academia y fuerzas militares a través de la co-localización

de talento técnico, Israel está creando un centro de seguridad cibernética económica y estratégica. El parque cibernético de Be'er Sheva también aumenta las asociaciones público-privadas en el ámbito cibernético; sirve como un centro de excelencia para la innovación; y proporciona reservas de empleo y de formación eficaces.

Ayudas y becas son otro mecanismo del mercado utilizado para avanzar en la educación en seguridad cibernética, desarrollar conocimientos y desarrollar habilidades. Por ejemplo, el programa "Ciencia sin Fronteras" del gobierno brasileño ofrece becas en todos los campos de ciencia, tecnología, ingeniería y matemáticas, incluyendo la informática y la tecnología de la información. Del mismo modo, el Consejo Nacional de Desarrollo Científico y Tecnológico (CNPq), organismo dependiente del Ministerio de Ciencia, Tecnología e Innovación, proporciona una "Beca de Iniciación a Ciencia" para incentivar la educación de las TIC en los estudiantes jóvenes.[73]

Los centros de innovación cibernética aceleran la transferencia de ideas y tecnologías a soluciones.

Los centros de innovación de seguridad cibernética, como el Delta de Seguridad de La Haya (HSD), fomentan I+D de seguridad cibernética innovadora y fomentan la colaboración entre las empresas del sector privado, los gobiernos y las instituciones de investigación. HSD, una fundación con el apoyo de la Municipalidad de La Haya y el Ministerio de Economía holandés, es la red de seguridad más grande de Europa con puentes de conocimiento a las principales redes de seguridad en EE.UU., Canadá, Singapur y Sudáfrica. Su programa de seguridad cibernética incluye iniciativas como la Academia de Seguridad Cibernética y el Laboratorio de Experiencia de Incidentes Cibernéticos. Los proyectos actuales incluyen la construcción de una plataforma de detección de malware avanzada y la entrega de soluciones para la detección, notificación y gestión de vulnerabilidades cibernéticas través de escáneres cualitativos.[74]

Otros "centros de innovación cibernéticos" de sectores privados han surgido en Silicon Valley, Tel Aviv, Boston, Nueva York y Londres. Por ejemplo, el centro de innovación cibernético de Londres, denominado CyLon o cibernética de Londres, es el primer acelerador de nueva creación de seguridad cibernética de Europa. CyLon trabaja para fomentar el ecosistema de innovación cibernética en Londres y ayuda a las empresas a desarrollar productos relacionados con la seguridad de la información.[75]

Estas diversas iniciativas de I+D y centros de innovación cibernéticos aceleran la transferencia de ideas y tecnologías a soluciones para avanzar el mercado digital, mejorar la seguridad y resiliencia de las redes e infraestructuras subyacentes y mejorar el bienestar social.

Los elementos del compromiso de un país para avanzar su I+D cibernética, educación y esfuerzos de desarrollo de capacidades deben incluir:

Declaración:

A. Un compromiso anunciado públicamente por parte del gobierno con invertir a nivel nacional en seguridad cibernética básica e investigación aplicada;

B. Mecanismos de incentivos anunciados públicamente (por ejemplo, crédito fiscal para I+D) para fomentar la innovación en seguridad cibernética y la difusión de nuevos conocimientos, tecnologías de línea de base, técnicas, procesos y herramientas;

C. Mecanismos de incentivos del gobierno anunciados públicamente (por ejemplo, subvenciones, becas) para fomentar la educación en seguridad cibernética, la creación de conocimientos y desarrollo de habilidades;

Organización:

A. La identificación de al menos una entidad con la responsabilidad de supervisar las iniciativas de I+D en materia de seguridad cibernética nacional y servir como un punto de contacto para la colaboración nacional e internacional;

B. El establecimiento de programas de grado institucionalmente apoyados en seguridad cibernética, seguridad de la información o áreas de tecnología avanzada similares que se centran en la seguridad y la resiliencia del entorno digital;

C. El establecimiento de una entidad con la misión de medir e informar sobre la tasa de los programas de transición comerciales o gubernamentales exitosos (de la investigación a producto/servicio) con un enfoque en las soluciones que mejoran la seguridad y la resiliencia del entorno digital;

Recursos:

A. La identificación de los recursos financieros y humanos solicitados y asignados para seguridad cibernética básica e investigación aplicada e iniciativas;

B. La identificación de recursos financieros y humanos solicitados y asignados para transferencia comercial o gubernamental de tecnología e innovación mejorada;

Implementación:

A. La implementación de programas dedicados al desarrollo, la difusión y la rutinización de normas técnicas seguras e interoperables, aceptables para –y reforzadas por– organismos de estándares reconocidos internacionalmente;

B. La evidencia de las gestiones del gobierno nacional para apoyar, adelantar, y sostener la I+D en seguridad cibernética, especialmente en lo que se demuestra en términos de la tasa de conversión de investigación/producción (por ejemplo, el porcentaje aplicado operativamente dentro del gobierno) y de la tasa de adopción comercial de programas de transición exitosa ; y

C. La evidencia de las gestiones comerciales adicionales (por ejemplo, centros de innovación cibernética) para apoyar, adelantar y sostener I+D de seguridad cibernética, sobre todo en términos de la tasa de conversión de investigación/

producto (por ejemplo, porcentaje implementado operativamente dentro del sector privado) y de la tasa de adopción del gobierno de programas de transición con éxito del sector comercial.

Los hallazgos iniciales de este elemento esencial se basan en una revisión de si un país está invirtiendo en I+D cibernética, educación, creación de conocimiento, y desarrollo de habilidades, además de financiar iniciativas de seguridad cibernética de manera más amplia. Basándose en fuentes primarias y secundarias, el CRI 2.0 determina el tipo, en su caso, de mecanismos de incentivos gubernamentales ya existentes y los recursos dedicados a iniciativas similares a las descritas anteriormente. Las actualizaciones de este elemento esencial supervisarán, realizarán un seguimiento y evaluarán los desarrollos sustantivos y notables.

6. DIPLOMACIA Y COMERCIO

El sexto elemento esencial de la preparación cibernética se demuestra a través del compromiso con asuntos cibernéticos de un país como parte de su política exterior. En un nivel fundamental, la diplomacia cibernética busca encontrar soluciones mutuamente aceptables a los desafíos comunes. Están surgiendo asuntos cibernéticos en muchas áreas de relaciones internacionales diferentes, que incluye los derechos humanos, el desarrollo económico, acuerdos comerciales, control de armas y tecnologías de doble uso, la seguridad, la estabilidad, la paz y la resolución de conflictos. Si bien las cuestiones de seguridad cibernética están entremezcladas en casi todos los temas y la mayoría de los negociadores son expertos en un área temática específica (es decir, el control de armas o comercio), esos expertos a menudo no están familiarizados con las oportunidades o riesgos adicionales que surgen en un contexto cibernético. Por lo tanto, el establecimiento de una oficina o personal dedicado, cuyo enfoque principal es un compromiso diplomático en temas cibernéticos, debe ser un componente integral de la política exterior de un país.

En un nivel fundamental, la diplomacia cibernética busca encontrar soluciones mutuamente aceptables a desafíos comunes.

Dada la lentitud de la recuperación económica, muchos países están formulando nuevas políticas económicas internacionales consagradas en acuerdos comerciales como un medio para acelerar el crecimiento y crear oportunidades de mercado. Sin embargo, estas iniciativas económicas se están convirtiendo en espacios en los que se están negociando asuntos de seguridad nacional, sub-rosa. Por ejemplo, se celebró el Acuerdo de Asociación Transpacífico (TPP) el 5 de octubre de 2015. El objetivo del acuerdo es mejorar el comercio y la inversión entre los países socios del TPP, promover la innovación, el crecimiento y desarrollo económico, y apoyar la creación y retención de empleos. Fueron necesarios cinco años para llegar a un acuerdo, en parte debido a problemas cibernéticos. Los países socios no podían ponerse de acuerdo sobre cuestiones clave, incluida la protección de datos y los requisitos de privacidad (por ejemplo, protección de la propiedad intelectual), deseos de localización de datos y restricciones de contenido.

EE.UU. y la UE está negociando una Asociación de Inversión y Comercio Transatlántico

(TTIP), que es un acuerdo similar al TPP. Este acuerdo busca incrementar el acceso al mercado, eliminar los obstáculos regulatorios innecesarios, establecer normas que regulen las relaciones comerciales entremezcladas entre las dos regiones, crear empleos y promover el crecimiento del PIB.[76] Dos de los temas centrales que están retrasando esta negociación son la protección de datos y privacidad. Durante la última década, Europa y Estados Unidos se han puesto de acuerdo en la utilización de normas de protección comunes para la transferencia y el almacenamiento de todos los datos personales, que se mueven y/o residen entre la UE y Estados Unidos.[77] Sin embargo, los documentos filtrados por Edward Snowden expuso las actividades de recolección de datos a otros gobiernos y a ciudadanos por parte de los servicios de inteligencia del gobierno de Estados Unidos, lo que llevó a una pérdida de confianza entre gobiernos. Como resultado, muchos países europeos están exigiendo el establecimiento de normas mutuas de privacidad a nivel estatal, reglas de cifrado y marcos jurídicos, con el fin de mantener el ritmo del rápido avance tecnológico y también pedirles cuentas a los Estados sobre la adecuada protección de los datos. Además, una reciente sentencia del Tribunal de Justicia de la Unión Europea ha anulado el acuerdo de larga data de las normas de protección de datos "de puerto seguro" (*safe harbor*) entre la UE y EE.UU. La decisión ejecutiva de Puerto Seguro había permitido que las empresas estadounidenses se auto-certificaran para proporcionarles "protección adecuada" a los datos de los usuarios europeos de acuerdo con la directiva europea de protección de datos y con derechos fundamentales europeos, tales como la privacidad. Si bien las negociaciones están en curso para actualizar Puerto Seguro, no se ha previsto un tiempo para la realización, lo que complica aún más las negociaciones TTIP.[78] En la actualidad, la Cámara Americana de Comercio de la Unión Europea estima que revertir el Puerto Seguro podría costarle a la Unión Europea hasta el 1,3 por ciento del PIB.[79]

Actualmente se encuentra en proceso de negociación otro acuerdo de libre comercio con base regional, la Asociación Económica Integral Regional (RCEP), entre los Estados miembros de la ASEAN, China, India, Japón, Corea, Australia y Nueva Zelanda. Los dieciséis países RCEP participantes representan casi la mitad de la población mundial, casi el 30 por ciento del PIB mundial y más de una cuarta parte de las exportaciones mundiales. El objetivo de la RCEP es reducir las barreras comerciales, promover la cooperación económica y técnica, proteger la propiedad intelectual, fomentar la competencia, facilitar la solución de controversias y mejorar el acceso al mercado de los exportadores de bienes y servicios. En el marco de estas negociaciones, algunos países están tratando de incluir mecanismos que protegen sus datos, afirmando el derecho a la soberanía de datos para fines de seguridad nacional.[80]

También hay toda una serie de negociaciones en curso en el campo de la seguridad, centrándose en las tecnologías. Por ejemplo, el Acuerdo de Wassenaar sobre control de exportaciones de armas convencionales y tecnologías y bienes de doble uso, que tiene cuarenta y un firmantes a saber EE.UU., Reino Unido, Rusia y la mayoría de estados de la UE, recientemente se comprometió con frenar la venta de "sistemas de vigilancia de las comunicaciones" y "software de intrusión" de Internet que están diseñados especialmente o modificados para evitar ser detectados por instrumentos de seguimiento, o para derrotar a las contramedidas de protección.[81] Los estados tienen diferentes preocupaciones

sobre las aplicaciones de doble uso de estas tecnologías. Por ejemplo, una herramienta de evaluación de la vulnerabilidad a menudo utiliza aprovechamientos de día cero para descubrir vulnerabilidades en red. Estas mismas técnicas pueden ser utilizadas como armas. Por lo tanto, incluir estas tecnologías en los regímenes de control de exportaciones refleja la creencia de que las tecnologías avanzadas pueden derrotar las defensas nacionales de los países y presentar un riesgo para la seguridad nacional.

Otras negociaciones diplomáticas y discusiones están en curso que buscan establecer un entendimiento común y/o normas para aumentar la estabilidad y la seguridad en el entorno mundial de las TIC. Esto incluye el fortalecimiento de los mecanismos de cooperación para abordar los incidentes de seguridad de las TIC y abordar las solicitudes relacionadas con la infraestructura de TIC (por ejemplo, la actividad ilegal que se emite desde un país debido a una infección-botnet). También se está utilizando la diplomacia para definir los tipos de actividad cibernética que se deben o no permitir (por ejemplo, las normas para la conducta estatal responsable), a los que comúnmente se refieren como *normas de comportamiento cibernéticos*. Por ejemplo, el Grupo de Expertos Gubernamentales de las Naciones Unidas (GEG) destacó recientemente la naturaleza global del entorno de las TIC, amenazas existentes y potenciales en el ámbito de la seguridad de la información y posibles medidas de cooperación para afrontar esas amenazas. El GEG encontró que la adhesión al derecho internacional, en particular a las obligaciones de la Carta de la ONU, ofrece un marco esencial para el uso de las TIC por parte de los Estados. El Grupo acordó seguir un marco para normas cibernéticas, reglas o principios de conducta estatal responsable y medidas de fomento de la confianza (CBM).[82] Entre las medidas de fomento de la confianza, el GEG acordó fortalecer los mecanismos de cooperación entre los organismos estatales pertinentes con el fin de abordar los incidentes de seguridad de las TIC y desarrollar mecanismos técnicos, legales y diplomáticos adicionales para abordar las solicitudes relacionadas con la infraestructura de las TIC (por ejemplo, establecer un CSIRT u otra organización oficial para cumplir con esas funciones). Más recientemente, el presidente estadounidense Barack Obama y el presidente chino, Xi Jinping, acordaron (en principio) seguir las recomendaciones del GEG y adherirse a las normas establecidas por las Naciones Unidas sobre conducta en línea, especialmente las que regulan el uso de ataques cibernéticos para dañar la infraestructura crítica del otro en tiempos de paz.[83]

La seguridad cibernética está entrelazada en todos los componentes de la política y comercio exterior.

Basándose en algunos de los temas comunes del GEG, los líderes de Brasil, Rusia, India, China y Sudáfrica (BRICS) acordaron cooperar entre sí con el fin de abordar los retos comunes de seguridad TIC. Acordaron compartir información y mejores prácticas relacionadas con la seguridad del uso de las TIC, coordinarse contra la delincuencia cibernética, establecer una red de puntos de contacto en los Estados miembros y establecer la cooperación entre BRICS utilizando los CSIRT existentes. También instaron a la comunidad internacional a centrar sus esfuerzos en las CBM, la creación de capacidades, la no utilización de la fuerza y la prevención de conflictos facilitados por las

TIC.[84] Por otra parte, en enero de 2015, la OCS introdujo un código internacional de conducta revisado para la seguridad de la información a la Asamblea General de la ONU, que se proponía identificar los derechos y responsabilidades de los Estados en el espacio de información, promover una conducta constructiva y responsable, y mejorar la cooperación para afrontar las amenazas mutuas de las TIC.[85] La OCS revisó el lenguaje del Código de Conducta de 2011 con el lenguaje de los informes del GEG de 2012 y 2013 con el fin de ampliar el atractivo del Código de Conducta para los miembros del G-77.

Otros espacios internacionales mezclan temas económicos, de desarrollo y seguridad a medida que persiguen objetivos específicos. La UIT, por ejemplo, lleva a cabo debates regulares internacionales sobre el entorno político, tecnológico y regulatorio de las TIC y de Internet en cuatro de sus reuniones mundiales: la Cumbre Mundial sobre la Sociedad de la Información (CMSI), la Conferencia Mundial de Telecomunicaciones Internacionales (CMTI), la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT) y la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT).[86] Además, la OEA y el BID han unido sus fuerzas para trabajar con sus Estados miembros para abordar sistemáticamente la seguridad cibernética como parte de tres áreas temáticas: (1) el desarrollo que sea tanto socialmente incluyente como ambientalmente sostenible; (2) las TIC como una herramienta para generar ingresos y empleo, proporcionar acceso a los negocios e información, permitir el aprendizaje electrónico y facilitar las actividades del gobierno; y (3) la seguridad de sus infraestructuras básicas y servicios de cara al ciudadano.[87]

Claramente, las cuestiones de seguridad cibernética están surgiendo a través de una amplia variedad de espacios diplomáticos. La seguridad cibernética no es solo un problema de seguridad: es un elemento fundamental del comercio, la política exterior y económica y el potencial de crecimiento económico futuro de un país. Un componente clave de la capacidad de un país para participar diplomáticamente de manera efectiva en cuestiones relacionadas con cibernética es el establecimiento de un conjunto de profesionales dedicado y entrenado, estructuras organizativas y financiación que se centre en las nuevas cuestiones cibernéticas en una amplia variedad de compromisos y negociaciones de relaciones internacionales. Por ejemplo, Israel y la República Checa han designado agregados cibernéticos en sus embajadas en ciudades clave, que incluyen Washington DC y Bruselas.[88] Además, Estados Unidos realizó un programa de sensibilización cibernética sobre formación, de una semana, para el personal diplomático asignado a Asia.[89] El desarrollo de este conjunto de profesionales es cada vez más esencial para que un país pueda realizar su futura política exterior, política económica, comercio y metas de crecimiento económico.

Los elementos de una capacidad de compromiso de seguridad cibernética diplomática válida deben incluir:

Declaración:

A. La identificación anunciada de la seguridad cibernética como un elemento esencial de la política exterior y la seguridad nacional (por ejemplo, debates oficiales que involucran típicamente líderes políticos y militares de alto nivel en discusiones bilaterales y multilaterales);

B. La identificación anunciada de las TIC y la seguridad cibernética como un elemento esencial de la política económica internacional, las negociaciones y el comercio;

Organización:

A. El establecimiento de personal especializado y capacitado en la oficina de asuntos exteriores del país u organización equivalente cuya misión principal incluye la participación activa internacional en la diplomacia de seguridad cibernética;

B. La coherencia demostrada entre la cantidad y el rango del personal diplomático cibernético extranjero dedicado y el compromiso anunciado de un país a participar en la diplomacia de seguridad cibernética como una cuestión de primer nivel de importancia nacional;

Recursos:

A. La identificación de los recursos financieros y humanos solicitados y asignados para el compromiso diplomático cibernético;

Implementación:

A. Prueba de la participación en la definición, la firma y la aplicación de los acuerdos internacionales, multinacionales, regionales y/o bilaterales que buscan soluciones mutuamente aceptables a los problemas comunes; y

B. Evidencia demostrada de las gestiones realizadas para influir en las negociaciones comerciales y el comercio internacional que se refieren a la utilización de las TIC o los aspectos compartidos a nivel internacional, regional y/o nacional de la infraestructura cibernética, servicios críticos y tecnologías.

Los hallazgos iniciales de este elemento esencial se basan en una revisión de si un país ha designado o establecido, de manera explícita, una oficina gubernamental o les ha asignado a unas personas responsabilidades diplomáticas que incluyen tanto los aspectos económicos como de seguridad de los asuntos cibernéticos. El CRI 2.0 se basa en fuentes primarias y secundarias para determinar si, y en qué medida, la (s) oficina (s) gubernamental (es) o los particulares participan e influyen en las negociaciones internacionales sobre cuestiones relativas a la seguridad cibernética. Las actualizaciones de este elemento esencial supervisarán, realizarán un seguimiento y evaluarán los desarrollos sustantivos y notables.

7. RESPUESTA DE CRISIS Y DEFENSA

El séptimo y último elemento de la preparación cibernética es la capacidad que tienen las fuerzas armadas nacionales de un país y/o agencia de defensa relacionada para la defensa del país frente a las amenazas que emanan del ciberespacio. Los países interesados en este tipo de capacidad están dándoles la orden a sus fuerzas de defensa de establecer la capacidad o experticia para responder a las amenazas informáticas que llegan al punto de considerarse conflictos "por cibernética" críticos a nivel nacional.[90]

Los países están cada vez más conectados y dependen más de Internet y eso, a su vez, está haciendo que sean más vulnerables a actividades cibernéticas disruptivas y destructivas. Las posturas defensivas de la mayoría de los países son débiles frente a ataques cibernéticos sofisticados. La naturaleza

globalmente conectada de las competencias y conflictos modernos animan a adversarios que se habilitan por la cibernética a moverse lateralmente a través de sistemas nacionales y se dirigen a organizaciones comerciales y no estatales de un país. Por ejemplo, en agosto de 2012, Saudi Aramco sufrió un ataque dirigido que utilizó software malicioso para destruir datos e hizo daños en casi el 75 por ciento de la infraestructura de TI de la empresa.[91] Funcionarios corporativos afirmaron que el incidente se proponía afectar la producción de aceite. Unos meses después, en marzo de 2013, varias instituciones financieras en Corea del Sur, incluido el Shinhan Bank –el cuarto mayor banco del país– sufrió daños por programas maliciosos similares a los utilizados contra Saudi Aramco. Los servicios electrónicos del banco fueron interrumpidos y los datos fueron destruidos. Se estimaron los daños económicos de este incidente en aproximadamente 800 000 millones de dólares.[92] En diciembre de 2014, hackers manipularon con éxito e interrumpieron los sistemas de control en una fábrica de acero alemán, y lograron que su alto horno se apagara de forma inadecuada, lo que resultó en daños significativos.[93] Más recientemente, Sony pictures fue víctima de un ataque cibernético, cuando fueron copiadas ilegalmente películas inéditas, correos electrónicos corporativos fueron robados y luego filtrados, y documentos financieros fueron expuestos. Los datos sensibles sobre decenas de miles de empleados de Sony fueron copiados y casi el 80 por ciento de los activos de TI de la compañía fueron destruidos, desde datos a hardware, por malware virulento.[94]

Los países deben estar preparados para defender sus intereses en red y conectados en conflictos actuales y futuros. La velocidad y el alcance de Internet conecta todos los aspectos de la sociedad y ofrece fácil acceso a armas cibernéticas de grado militar, dándoles una ventaja asimétrica a muchos. De hecho, la diversidad de actores maliciosos, incluidos activistas políticos, delincuentes, terroristas, actores estatales y no estatales –todos con diferentes motivos– pone de relieve la necesidad de prepararse para los peores escenarios. En la actualidad, más de sesenta países han desarrollado capacidades para espionaje y ataque cibernético, a la vez que demuestran un gran interés en la adquisición o el desarrollo de capacidades ofensivas y defensivas con derecho de preferencia.[95] Además, los países han comenzado a diseñar diferentes estrategias y herramientas para mejorar sus defensas cibernéticas a nivel nacional. La mayoría de los gobiernos han deseado instintivamente aumentar las capacidades defensivas existentes de sus organismos de seguridad que ya pueden operar en, a través de y según lo habilita el ciberespacio fuera de sus fronteras nacionales (es decir, la organización de defensa o servicios de inteligencia). Otros han buscado colocar estas capacidades en las organizaciones de seguridad que no se encuentren directamente dentro de su estructura militar.[96]

Actividades cibernéticas disruptivas y destructivas requieren una defensa cibernética creíble.

Por ejemplo, en 2010 EE.UU. estableció una unidad de las fuerzas armadas dedicada, el comando cibernético de EE.UU., para defenderse de las amenazas cibernéticas

en la infraestructura militar. Su misión se amplió en 2015, cuando el Departamento de Defensa (DoD) publicó su segunda Estrategia Cibernética como guía para el desarrollo de las fuerzas cibernéticas del Departamento de Defensa (bajo el mando y control del Comando Cibernético de Estados Unidos) y para reforzar sus defensas cibernéticas y la postura de disuasión cibernética. Esta nueva estrategia pone de relieve la necesidad de estar "preparados para defender la patria estadounidense y los intereses vitales de Estados Unidos de ataques cibernéticos perjudiciales o destructivos de gran importancia", y construir, mantener y utilizar las opciones cibernéticas viables para controlar la escalada del conflicto y darle forma al entorno de combate en todas las etapas.[97]

Del mismo modo, en diciembre de 2014, la Federación Rusa dio a conocer su nueva doctrina militar que resalta el desarrollo de las capacidades de guerra cibernética de Rusia, tanto para fines ofensivos como defensivos, así como "la disuasión no nuclear."[98] El Libro Blanco de 2011 del Ministerio de Defensa de Rusia, dedicado a los conceptos sobre las actividades de las Fuerzas Armadas de la Federación Rusa en el espacio de la información, contiene paralelos con aspectos de la Doctrina de Defensa de Rusia, pero también incluye explícitamente la opinión pública y la necesidad de mantener a los medios de comunicación al tanto de las situaciones de conflicto que evolucionan para propósitos de des-escalarlos.[99] Según la prensa rusa, la dirigencia rusa planea lanzar una nueva Doctrina de Seguridad de la Información en 2016, que aparentemente propondrá el desarrollo de fuerzas para la guerra de información y sistemas de información para la disuasión estratégica y la prevención de conflictos.[100]

La República de Corea del Sur y Brasil también han establecido organizaciones militares similares destinadas a garantizar las capacidades ofensivas, defensivas y de respuesta, así como garantizar la victoria total en la guerra cibernética.[101] Corea del Sur ha estado expandiendo sus capacidades cibernéticas y se dice que adelanta la formación de más de cuatrocientos nuevos soldados cibernéticos para su Comando de Defensa Cibernética surcoreano, lo que eleva el total a alrededor de mil.[102]

Además, si bien la República Popular de China no ha emitido públicamente ninguna doctrina estratégica formal para aplicaciones militares de información o cibernéticas, sí ha publicado directrices estratégicas militares que proporcionan orientación para la política de defensa.[103] El Libro Blanco de 2013 de China, que versa sobre el empleo diversificado de las Fuerzas Armadas de China, y el dictamen sobre mayor fortalecimiento del trabajo de seguridad de la información de 2014 hacen énfasis en el desarrollo de capacidades cibernéticas defensivas. Los documentos se centran en que el Ejército de Liberación Popular no atacará a menos que sea atacado, pero si es atacado, contraatacará en el ciberespacio.[104]

Una agencia de defensa cibernética no tiene que ser una agencia uniformada al interior de las fuerzas militares de la nación. La policía nacional y las fuerzas de inteligencia pueden ser la sede de la capacidad central de defensa de un gobierno en el ciberespacio, aunque las fuerzas armadas también deberán ser modernizadas y preparadas cibernéticamente para afrontar conflictos más tradicionales. Por ejemplo, Islandia ha concentrado sus respuestas cibernéticas fuera de sus fuerzas armadas. En el pasado, se dividieron las

responsabilidades de seguridad cibernética de Islandia de manera informal entre el Ministerio del Interior, la Administración de Correos y Telecomunicaciones, la Autoridad de Protección de Datos y la Policía de Islandia. Sin embargo, en 2015 Islandia centralizó todas sus capacidades cibernéticas bajo el Comisionado Nacional de la Policía de Islandia.[105] La estrategia cibernética nacional de Islandia de junio de 2015 también destacó el papel integral de la alianza de la OTAN a la defensa cibernética de Islandia.[106]

Por último, si bien Israel no tiene actualmente una "comando cibernético" formalizado, sus capacidades de seguridad cibernética existen y están distribuidas entre la Fuerza de Defensa de Israel (IDF) y la Dirección de Inteligencia Militar. La Dirección de Inteligencia Militar se encarga de la capacidad ofensiva, mientras que los servicios se ocupan de la protección. Shin Bet, el servicio de seguridad interna de Israel, es responsable de la defensa de los sistemas de gobierno y la infraestructura nacional crítica, y el National Cybernetic Taskforce asegura las redes críticas y la industria privada contra la piratería y el espionaje.[107] Esto puede cambiar, sin embargo, debido a que en junio de 2015, el teniente general Gadi Eisenkot, comandante del Ejército israelí, informó sobre su intención de establecer un nuevo cuerpo de la Fuerza de Defensa de Israel –a la par con la Armada y la Fuerza Aérea– responsable de toda la actividad cibernética. En caso de que el Ministro de Defensa apruebe el nuevo cuerpo, el nuevo ejército cibernético israelí podría estar funcionando en dos años. Una vez en funcionamiento, el nuevo Comando Cibernético integrará capacidades defensivas actualmente prestadas por el ejército israelí con capacidad ofensiva y de inteligencia, llevada a cabo por la Unidad de 8200 y otras comunidades de inteligencia militar.[108] Esto se alinea con "Gideon", el nuevo plan de cinco años de la Fuerza de Defensa de Israel, que fue publicado en agosto de 2015. "Gideon" específicamente requiere el aumento de iniciativas para protegerse de ataques cibernéticos y otras amenazas asimétricas, que pueden emanar de grupos no estatales y terroristas en la región.[109]

Una capacidad de defensa cibernética es necesaria para un país para garantizar su seguridad nacional y económica. A medida que los países se vuelven más dependientes de los sistemas de Internet y de las TIC, más vulnerables serán a las amenazas cibernéticas de "bajo nivel" y a la actividad asimétrica. Los países se enfrentan a un dilema: una mayor implantación de las TIC es esencial para el crecimiento, pero cuanto más conectado esté un país, incurrirá en más riesgos. Ya no es una opción optar por estar fuera de la economía de Internet. Los países deben estar preparados para defenderse en el ciberespacio. Si un país no puede defenderse, no está preparado cibernéticamente.

Los elementos del compromiso de un país para desarrollar y desplegar unidades de defensa nacionales dedicadas con capacidades/ responsabilidades de defensa cibernética pueden incluir:

Declaración:

A. La publicación de declaraciones nacionales que le asignan a una organización la misión nacional de defensa cibernética como una misión de primer nivel;

B. El establecimiento de políticas para que la organización de defensa cibernética responda a las amenazas cibernéticas;

C. La articulación de declaraciones nacionales que obligan a la organización de defensa cibernética desarrollar la capacidad de responder a las amenazas dentro o fuera del territorio soberano;

Organización:

A. El establecimiento de una organización a nivel nacional, dentro de las fuerzas militares, cuya misión principal es la defensa cibernética de la nación;

B. El establecimiento de una organización a nivel nacional, no dentro de las fuerzas militares, cuya misión principal es la defensa cibernética de la nació;

Recursos:

A. La identificación de los recursos financieros y humanos solicitados y asignados a la organización, dentro de las fuerzas militares, cuya misión incluye explícitamente la defensa cibernética de la nación;

B. La identificación de los recursos financieros y humanos solicitados y asignados a la organización, no dentro de las fuerzas militares, cuya misión incluye explícitamente la defensa cibernética de la nación;

Implementación:

A. Evidencia de ejercicios realizados a nivel de gobierno que demuestran la preparación de defensa cibernética nacional;

B. Evidencia de ejercicios realizados a nivel nacional entre entidades comerciales afectadas que demuestran la preparación de defensa cibernética nacional;

C. Evidencia de ejercicios realizados con socios internacionales (por ejemplo, la defensa mutua de OTAN o el simulacro APCERT) que demuestran la cooperación a través del intercambio de información y asistencia;

D. El establecimiento de normas para el comportamiento estatal responsable en el ciberespacio y la identificación de los umbrales que permitan la participación de la defensa cibernética; y

E. El establecimiento de mecanismos de asistencia rápida (independientes de los CERT o equivalentes) para las industrias específicas o el gobierno en caso de graves incidentes cibernéticos.

Los resultados iniciales de este elemento esencial se basan en una revisión de si un país ha declarado oficialmente que establecerá fuerzas de defensa cuya misión de alto nivel incluye la defensa cibernética de la nación. El CRI 2.0 se basa en fuentes primarias y secundarias para determinar el nivel de madurez operacional. Las actualizaciones de este elemento esencial supervisarán, realizarán un seguimiento y evaluarán los desarrollos sustantivos y notables.

CONCLUSIÓN

Ningún país esta preparado cibernéticamente.

Las amenazas a nuestras infraestructuras y sistemas en red son reales y crecientes y les imponen costos en términos económicos a los países y a la sociedad. Las agendas de seguridad

nacional y económica deben alinearse para aportarle transparencia a la inseguridad cibernética. El evidenciar esta asociación vital puede despertar el interés nacional y mundial en abordar esta erosión económica. La metodología CRI 2.0 integral, comparativa, y basada en la experiencia ofrece un modelo para evaluar la madurez y el compromiso de cualquier país para asegurar sus servicios e infraestructura cibernéticas nacionales de las que dependen su crecimiento y futuro digital.

El modelo CRI 2.0 identifica más de setenta indicadores de datos únicos a través de siete elementos esenciales: estrategia nacional, respuesta a incidentes, delito electrónico y aplicación de la ley, intercambio de información, inversión en I+D, diplomacia y comercio, y defensa y respuesta a la crisis. Estos indicadores y elementos esenciales proporcionan un marco para que un país desarrolle una postura de seguridad más fuerte que pueda defender contra la erosión del PIB. En efecto, el CRI 2.0 desafía la sabiduría convencional de que la seguridad cibernética es predominantemente un problema de seguridad nacional. El CRI 2.0 puede demostrar cómo está estrechamente entrelazada la seguridad nacional con la conectividad a Internet y la rápida adopción de las TIC, que cuando es segura, puede conducir al crecimiento económico y la prosperidad.

En lugar de simplemente estudiar el problema, el CRI 2.0 ofrece un marco para que un país evalúe la fuerza de su capacidad para prevenir la erosión económica por la inseguridad cibernética. El CRI 2.0 se actualizará anualmente y agregará criterios de evaluación en forma de preguntas sin perder la validez comparativa con evaluaciones previas. De esa manera, el CRI 2.0 mostrará el avance y la evolución de los países hacia el aseguramiento de los servicios e infraestructura cibernéticas de las que dependen su futuro digital y crecimiento.

Ningún país puede permitirse la inseguridad cibernética y las pérdidas que conlleva. Los datos y la metodología CRI 2.0 pueden ayudar a los líderes nacionales a trazar un camino hacia una economía más resiliente y más segura en un mundo profundamente cibernético, competitivo y conflictivo.

Para más información o para proporcionar datos a la metodología CRI 2.0, por favor póngase en contacto con:

CyberReadinessIndex2.0@potomacinstitute.org

BIBLIOGRAPHY

1. El Índice de Preparación Cibernética 2.0 se basa en el anterior Índice de Preparación Cibernética 1.0, que proporciona un marco metodológico para evaluar la preparación cibernética a través de cinco elementos esenciales, a saber: estrategia nacional cibernética, respuesta a incidentes, delito electrónico y capacidad jurídica, el intercambio de información y la investigación y desarrollo cibernético. El Índice de Preparación Cibernética 1.0 aplicó esta metodología a un conjunto inicial de treinta y cinco países. Para obtener más información sobre el Índice de Preparación Cibernética 1.0, consulte: Melissa Hathaway, "Cyber Readiness Index 1.0", *Hathaway Global Strategies LLC* (2013), *http://belfercenter.ksg.harvard.edu/files/cyber-readiness-index-1point0.pdf*.

2. El entrelazamiento de Internet - infraestructura es la interdependencia de conectividad a Internet para la prestación de servicios esenciales como el agua, la electricidad, el transporte, las comunicaciones, la salud, etc. Para más información sobre el entrelazamiento Internet - infraestructura, consulte: Melissa Hathaway, "Connected Choices: How the Internet Is Challenging Sovereign Decisions," American Foreign Policy Interests 36, no. 5 (November 2014): 301. Para más información sobre el entrelazamiento Internet - infraestructura, consulte: Melissa Hathaway, "Connected Choices: How the Internet Is Challenging Sovereign Decisions," *American Foreign Policy Interests* 36, no. 5 (November 2014): 301.

3. Ejemplos de estrategias económicas habilitadas por las TIC que se adelanten alrededor del mundo incluyen: Europe's *Digital Single Market*; India's *Digital India* (ID); China's *Internet Plus (+)*; and the ITU *Connect 2020*.

4. Consejo de Estado de China, "Internet Plus," *Guo Fa* 40 (2015). Traducido por el Departamento de Estado de EE.UU.

5. Gobierno de la India, "Programme Pillars," *Digital India: Power to Empower*, *http://www.digitalindia.gov.in/content/programme-pillars*.

6. Comisión Europea, "Digital Single Market: Bringing down the barriers to unlock online opportunities," *http://ec.europa.eu/priorities/digital-single-market/*.

7. Melissa Hathaway y Francesca Spidalieri, "Sustainable and Secure Development: A Framework for Resilient Connected Societies," en *Observatory of Cyber Security in Latin America and the Caribbean* (publicación próxima de la Organización de los Estados Americanos, diciembre 2015).

8. Banco Mundial, "Overview," *Information & Communication Technologies Program*, modificado por última vez 02 de octubre 2014, *http://worldbank.org/en/topic/ict/overview*.

9. David Dean et al., "The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy," *Boston Consulting Group report* (January 2012): 2.

10. Peter C. Evans y Marco Annunziata, "Industrial Internet: Pushing the Boundaries of Minds and Machines," *General Electric* (26 November 2012): 13.

11. Melissa Hathaway, "Cyber Readiness Index 2.0 & Lessons Learned in the Design of national Cyber Security Strategies," (presentación en el Taller Regional de la OEA-BID sobre Políticas de Seguridad Cibernética, Washington D.C., 23 de Octubre de 2014).

12. Frontier Economics London, Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report commissioned by Business Action to Counterfeiting and Piracy, (London, Frontier Economics Ltd, 2011): 47.

13. La Oficina Nacional de Investigación de Asia, "The IP Commission Report: The report of the commission on the theft of American intellectual property," National Bureau of Asian Research (May 2013).

14. Melissa Hathaway, "Connected Choices: How the Internet Is Challenging Sovereign Decisions," American Foreign Policy Interests 36, no. 5 (November 2014): 301.

15. Se le atribuye a Harvey Poppel la invención de las bolas de Harvey en la década de 1970, mientras trabajaba como consultor en Booze Allen Hamilton como consultor.

16. Basado en el ranking de 2013 del PIB del Banco Mundial.

17. OECD, *OECD Digital Economy Outlook 2015* (Paris, France: OECD Publishing, 2015), *http://dx.doi.org/10.1787/9789264232440-en*.

18. Melissa Hathaway, "Transparency, Trust, and Our Internet," (presentación en la Conferencia GTEC, Ottawa, Canadá, 20 de Octubre de 2015).

19. La adopción de infraestructura de TIC incluye segmentos de mercado fijos y móviles (voz y datos) –tanto las suscripciones como el acceso a datos de los hogares– y la inversión en, e ingresos por, el sector de las telecomunicaciones.

20. Una autoridad competente es cualquier persona u organización que tiene la autoridad, la capacidad o el poder legalmente delegado o conferido para realizar una función designada.

21. Unión Internacional de Telecomunicaciones, "National Strategies," *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx*.

22. Los términos CSIRT y CERT se refieren a un equipo de expertos en seguridad de TI designados para responder a incidentes de seguridad informática. Ambos términos se utilizan indistintamente, pero CSIRT es el término más preciso.

23. La Unión Internacional de Telecomunicaciones, "CIRT Programme," *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx*.

24. John Haller, Samuel Merrell, Matthew Butkovic, y Bradford Willke, *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0* (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2011), *http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9999*.

25. Olaf Kruidhof, "Evolution of National and Corporate CERTs – Trust, the Key Factor," in *Best Practices in Computer Network Defense: Incident Detection and Response*, ed. Melissa E. Hathaway, (Amsterdam: NATO Science for Peace and Security Series, IOS Press, February 2014).

26. Equipo de Respuesta de Emergencia Informática de Singapur, "FAQs," *https://www.csa.gov.sg/singcert/about-us/faqs*.

27. Ministerio de Comunicaciones, "Portaria Interministerial N 147, de 31 de Maio de 1995," *http://cgi.br/portarias/numero/147*.

28. cert.br, "About CERT.br," *http://www.cert.br/about/*.

29. "Documents," APCERT. APCERT.org, 13 de octubre de 2015. *http://www.apcert.org/documents/index.html*.

30. "Asia Pacific Computer Emergency Response Team Operational Framework" APCERT. APCERT.org, 13 de octubre de 2015. *http://www.apcert.org/documents/pdf/OPFW(26Mar2013).pdf*.

31. Melissa Hathaway, "Best Practices in Computer Network Defense: Incident Detection and Response," Global Cyber Security Center (September 2013): 12.

32. Ingvar Hellquist (Coronel ret.), Asesor Senior y Lars Nicander, Director del Centro de Estudios de Amenazas Asimétricas, Universidad Sueca de Defensa, "CATS Course and Cyber Exercise," (entrevista por Melissa Hathaway en Estocolmo, Suecia, 17 de octubre de 2012) y el Colegio de Defensa Nacional sueco, "CATS Newsletter," *CATS Center for Asymmetric Threat Studies* (primavera de 2013).

33. Dusan Navratil, Director de la Autoridad de Seguridad Nacional de la República Checa y Robert Kahofer, Asistente Especial, "Cyber Czech 2015 - National Technical Cyber Security Exercise," (entrevista por Melissa Hathaway, en Washington D.C., Octubre de 2015).

34. "South Korea says Nuclear Worm is nothing to worry about," TheRegister.co.uk, 30 December 2014, *https://www.hackbusters.com/news/stories/206721-south-korea-says-nuclear-worm-is-nothing-to-worry-about* y "Activists Hack KNHP's computer systems," World Nuclear News, 22 December 2014, *http://www.world-nuclear-news.org/C-Activists-hack-KHNPs-computer-systems-2212141.html*.

35. Departamento de Seguridad Nacional, "Cyber Storm: Securing Cyber Space," *http://www.dhs.gov/cyber-storm-securing-cyber-space*.

36. Comisión Europea, "Cyber Strategy of the European Union: An Open, Safe, and Secure Cyberspace," *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, (July 2013): 7 y la Agencia de Seguridad de

las Redes y de la Información de la Unión Europea, "Cyber Europe," *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe*.

37. Doug Drinkwater, "Hundreds of companies face 2,000 cyber-attacks in EU exercise," SC Magazine, 31 de octubre de 2014 en ENISA, "ENISA Cyber Europe 2014: Media Coverage," *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/cyber-europe-2014-media-coverage*.

38. Agencia Europea de Defensa, "Complex Cyber Crisis Management Exercise in Vienna," 16 September 2015, *https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/09/16/complex-cyber-crisis-management-exercise-in-vienna* and NATO, "Largest ever NATO cyber defence exercise gets underway," 21 de noviembre de 2014, *http://www.nato.int/cps/en/natohq/news_114902.htm?selectedLocale=en*.

39. Katie Bo Williams, "US, UK to test finance sector cybersecurity this month," *The Hill*, 2 November 2015, *http://thehill.com/policy/cybersecurity/258827-us-uk-to-test-finance-sector-cybersecurity-this-month*.

40. CNCERT/CC, "2nd China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response was held in Korea," *www.cert.org.cn/publish/english/55/2014/20140961457392959960 84/20140916145739295996084_html*.

41. Carnegie Mellon University, "List of National CSIRTs," División CERT, *http://www.cert.org/incident-management/national-csirts/national-csirts.cfm*.

42. Agencia Europea de Seguridad de las Redes y de la Información (ENISA), "ENISA- CERT Inventory: Inventory of CERT teams and activities in Europe," ENISA Versión 2.16 (junio de 2014), *http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe*.

43. Foro de Equipos de Respuesta a Incidentes de Seguridad Informática (FIRST), "FIRST Members," *http://www.first.org/members/teams*.

44. Consejo de Europa, *Convention on Cybercrime* (23 November 2001) y la Organización de Cooperación de Shanghai, *Cooperation in the Field of Information Security*, sesión plenaria 61 (16 de junio de 2009).

45. *Ibid*.

46. Organización de Cooperación de Shanghai, *Cooperation in the Field of Information Security*, sesión plenaria 61 (16 de junio de 2009), https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf.

47. Juez Stein Schjolberg y Amanda M. Hubbard, "Harmonizing National Legal Approaches on Cybercrime," Unión Internacional de Telecomunicaciones (1 de julio de 2005): 6.

48. Los veinte países que firmaron el informe GGE, incluyen: Belarús, Brasil, China, Colombia, Egipto, Estonia, Francia, Alemania, Ghana, Israel, Japón, Kenia,

Malasia, México, Pakistán, Corea, Rusia, España, Reino Unido, y EE.UU. Véase: Naciones Unidas, Informe del Grupo de Expertos Gubernamentales sobre el desarrollo en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional, A/65/201 and A/68/98 (26 de junio de 2015).

49. Ernesto U. Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement, and Research (Dordrecht, The Netherlands: Springer, 2004): 50.

50. Centro Superior de Investigación, Desarrollo y Capacitación en Derecho Cibernéticos y Forense, "Academic Programs," *National Law School of India University*, *https://www.nls.ac.in/index.php?option=com_content&view=article&id=502&Itemid=32*.

51. INTERPOL, "The INTERPOL Global Complex for Innovation," Consultado el 17 de septiembre de 2015, *http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation*.

52. Madan M. Obero, "Dark Web and Crypto-Currency," (presentación en Cyber 360: A Synergia Conclave, Bangalore, India, 30 de septiembre de 2015).

53. Un bot es una forma maliciosa de software que puede utilizar su computadora para enviar spam, alojar un sitio de phishing, o robar su identidad mediante el control de las pulsaciones del teclado. Los computadores infectados son entonces controlados por terceros y pueden ser utilizados para ataques cibernéticos. Para obtener más información, consulte: Melissa Hathaway y John Savage, "Stewardship of Cyberspace: Duties of Internet Service Providers," Cyber Dialogue 2012 (marzo de 2012).

54. Alastair Stevenson, "Botnets infecting 18 systems per second, warns FBI," *V3.cok.uk*, 16 July 2014, *http://www.v3.co.uk/v3-uk/news/2355596/botnets-infecting-18-systems-per-second-warns-fbi*.

55. Bell Canada et all, "The Dark Space Project," *Security Telecommunications Advisory Committee* (2011): 13, *https://citizenlab.org/cybernorms2012/cybersecurityfindings.pdf*.

56. Yurie Ito, "Cyber Clean Center," (entrevista a distancia con el equipo Cyber Readiness Index, Washington D.C., 10 de noviembre de 2015).

57. Ministerio de Asuntos Internos y Comunicaciones y el Ministerio de Economía, Comercio e Industria, "What is the Cyber Clean Center," *Cyber Clean Center*, *https://www.telecom-isac.jp/ccc/en_index.html* y Michael M. Losavio, J. Eagle Shutt, y Deborah Wilson Keeling, "Changing the Game: Social and Justice Models for Enhanced Cyber Security," en Tarek Saadawi, Louis H Jordan Jr., y Vincent Boudreau, Cyber Infrastructure Protection Volume II (U.S. Army War College, Strategic Studies, 2013): 101.

58. Telecom-ISAC Japan, "Chairman's Message," 12 de mayo de 2011, *https://www.telecom-isac.jp/english/index.html*.

59. Iniciativa de Seguridad de Internet de Australia (AISI), "Overview of the Australian Internet Security

Initiative," *http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative*.

60. McAfee, "McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies," 9 de junio de 2014, *http://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx* y The National Bureau of Asian Research, 4/q2 IP Commission Report: The report of the commission on the theft of American intellectual property," National Bureau of Asian Research (May 2013).

61. Melissa Hathaway, "Why Successful Partnerships are Critical for Promoting Cybersecurity," The New New Internet, 7 de mayo de 2010.

62. Ministerio de Seguridad y Justicia de los Países Bajos, "National Cyber Security Centre (NCSC)," *https://www.ncsc.nl/english*.

63. En febrero de 2007, el Centro de Coordinación de Seguridad Nacional de Infraestructura del Reino Unido se fusionó con el Centro de asesoramiento de Seguridad Nacional (NSAC) para conformar el Centro para la Protección de la Infraestructura Nacional (CPNI). Para más información sobre el CPNI, consulte: Center for Protection of National Infrastructure, *http://www.cpni.gov.uk*.

64. Agencia de Promoción de Información-tecnología (IPA), Centro de seguridad de TI de Japón, *Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) Annual Activity Report FY2012*, (Abril de 2013).

65. Centro de Análisis e Intercambio de Información y Servicios Financieros, "Overview of the FS-ISAC," Consultado el 17 de septiembre de 2015, *https://www.fsisac.com/sites/default/files/FS-ISAC_Overview_2011_05_09.pdf*.

66. National Cyber-Forensics & Training Alliance, "Become a NCFTA Partner," *https://www.ncfta.net/*

67. Raphael Mandarino, "MT2: Private Public Partnership," Gabinete de Seguridad Institucional del Departamento de Seguridad de la Información y las Comunicaciones, Oficina del Presidente, (presentación en la primera Conferencia de Seguridad de INTERPOL, Hong Kong, 15-17 de septiembre de 2010).

68. Instituto Nacional de Estándares y Tecnología, "National Vulnerability Database," *https://nvd.nist.gov*.

69. El Reino Unido y Brasil tienen mecanismos para desclasificar la información de inteligencia y compartirla con sus sectores críticos, mucho mejor que como lo hace EE.UU.

70. Comisión Europea, "ICT Research & Innovation," *Horizon 2020: The EU Framework Programme for Research and Innovation*, *http://ec.europa.eu/programmes/horizon2020/en/area/ict-research-innovation*.

71. Para más información sobre el Programa de Investigación y Desarrollo de Tecnología de Redes y la Información (NITRD) y sus áreas de investigación, véase: *www.nitrd.gov/Index.aspx* y NITRD, "The Networking and Information Technology and Research Development Program," *Supplement to*

the President's Budget FY 2016 (Febrero de 2015), *https://www.whitehouse.gov/sites/default/files/microsites/ostp/fy2016nitrdsupplement-final.pdf*.

72. Consulado General de Israel en Nueva York, "Cabinet approves tax break for National Cyber Park," Consulado General de Israel en Nueva York, 7 de junio de 2014, *http://embassies.gov.il/wellington/NewsAndEvents/Pages/Cabinet-approves-tax-break-for-National-Cyber-Park-6-Jul-2014.aspx*.

73. Ciencia Sin Fronteras, "FAQ", *http://www.cienciasemfronteiras.gov.br/web/csf-eng/faqEGTI_2013-2105_v1-3*, Coordination for the Improvement of Higher Education Personnel (CAPES), "Coordination for the Improvement of Higher Education Personnel (CAPES)", http://www.iie.org/Programs/CAPES, and CNPq, "Programas Institucionais de Iniciação Científica e Tecnológica," *http://www.cnpq.br/web/guest/piict*.

74. "Cyber Security," *The Hague Security Delta*, *https://www.thehaguesecuritydelta.com/cyber-security*.

75. Zach Cutler, "5 Growing Cyber-Security Epicenters Around the World," *Entrepreneur*, 3 September 2015, *http://www.entrepreneur.com/article/250024*.

76. Comisión Europea, "About TTIP," *Trade*, *http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/*.

77. "Welcome to the U.S.-EU Safe Harbor," *http://www.export.gov/safeharbor/eu/eg_main_018365.asp*.

78. Tribunal de Justicia de la Unión Europea, "The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid," *Press Release* 117/15 (6 October 2015), *http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf*.

79. Cámara Americana de Comercio con la Unión Europea, "EU Courts of Justice's decision in the Schrems case could disrupt transatlantic business, hurt the EU economy and jeapordise a Digital Single Market," *Press Release*, 6 October 2015, *http://www.amchameu.eu/sites/default/files/press_releases/press_-_ecj_decision_on_schrems_will_disrupt_transatlantic_business.pdf*.

80. Hathaway, "Connected Choices: How the Internet Is Challenging Sovereign Decisions," 302 y Arun Mohan Sukmar, "The New Great Game in Asia," *The Hindu*, 25 August 2015, visitada el 16 de septiembre 2015, *http://www.thehindu.com/opinion/op-ed/arun-mohan-sukumar-column-the-new-great-game-in-asia/article7575755.ece*.

81. "Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies" última actualización 16 de septiembre 2015, *http://www.wassenaar.org/index.html*.

82. Naciones Unidas, *Report of the Group of Government Experts On Development in the Field of Information and Telecommunications In the Context of International Security*, A/65/201 y A/68/98 (26 June 2015).

83. La Oficina del Secretario de Prensa de la Casa Blanca, "FACT SHEET: President Xi Jinping's State Visit to the United

States," 25 de septiembre de 2015, *https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states*.

84. University of Toronto, "VII: BRICS Summit 2015 Ufa Declaration," *BRICS Information Centre*, 9 July 2015, *http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html*.

85. Naciones Unidas, Asamblea General, "Letter dated 9 January 2015 from Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General," *Developments in the field of information and telecommunications in the context of international security*, A/69/723 (13 de enero de 2015), *http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement*.

86. Melissa Hathaway, "Discussion Paper for the Global Commission of Internet Governance," (documento presentado en Estocolmo Suecia, el 27 de Mayo de 2014).

87. Banco Interamericano de Desarrollo, "IDB and OAS join efforts to promote better cybersecurity policies in Latin America and the Caribbean," 22 de octubre de 2014, *http://www.iadb.org/en/news/news-releases/2014-10-22/cybersecurity-workshop-for-latin-america,10957.html*.

88. Dusan Navratil, Director de la Autoridad de Seguridad Nacional de la República Checa y Robert Kahofer, Asistente Especial, "Cyber Czech 2015 - National Technical Cyber Security Exercise," (entrevista por Melissa Hathaway, en Washington D.C., Octubre de 2015) y Rueuven Azar, Jefe Adjunto de Misión y el Dr. Eviatar Matania, Jefe de la Oficina Nacional Cibernética (entrevista por Melissa Hathaway en Rockville, MD 2 de junio de 2015).

89. Craig L. Hall, Consulado General de EE.UU., Kolkata, India, (entrevista realizada por Melissa Hathaway en Calcuta, India 23 de septiembre de 2015).

90. Un conflicto por cibernética difiere de la guerra cibernética o la batalla cibernética. Esta última es totalmente tecnológica y podría, en principio, realizarse en su totalidad dentro de una red. Normalmente es un componente de la primera. "Cybered conflicts are those nationally significant aggressive and disruptive conflicts for which seminal events determining the outcome could not have occurred without 'cyber' (meaning networked technologies) mechanisms at critical junctures in the determining course of events." Chris Demchak, "Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World," en Securing Cyberspace: A New Domain for National Security, editado por Nicholas Burns y Jonathon Price, (Washington, DC: The Aspen Institute, 2012).

91. Christopher Bronk, "The Cyber Attack on Saudi Aramco," Survival 55 (Abril-Mayo de 2013) 81-96.

92. Melissa Hathaway y John Stuart, "Cyber IV Feature: Taking Control of our Cyber Future," *Georgetown Journal of International Affairs* (25 July 2014).

93. Robert M. Lee, Michael J. Assante, and Tim Conway, "German Steel Mill Cyber Attack," *Industrial Control Systems* (30 December 2014).

94. "The Reality of the Sony Pictures Breach," *TrendMicro*, 22 December 2014, *http://blog.trendmicro.com/reality-sony-pictures-breach/*, Sean Fitz-Gerald, "Everything That's Happened in the Sony Leak Scandal," *Vulture*, 22 December 2014, http://www.vulture.com/2014/12/everything-sony-leaks-scandal.html#, y "Sony Breach May Have Exposed Employee Healthcare, Salary Data," *Krebson Security*, 2 de deciembre de 2014, *http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/*.

95. Jennifer Valentino-Devries y Danny Yadron, "Cataloging the World's Cyberforces," The Wall Street Journal, 11 de octubre de 2015, *http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710* y Asamblea General de las Naciones Unidas, *Developments in the Field of Information and Telecommunications in the context of International Security: Report to the Secretary General*, A/70/172 (22 de Julio de 2015), *http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172*.

96. James Lewis y Katrina Timlin, "Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization," *UNIDIR Resource and Center for Strategic and International Studies* (2011): 3.

97. Departamento de Defensa, "The Department of Defense Cyber Strategy," (Abril de 2015): 7-8.

98. Presidente de la Federación de Rusia, "Military Doctrine of the Russian Federation," *Russian Government* (2014) traducido por Thomas Moore, *https://www.scribd.com/doc/251695098/Russia-s-2014-Military-Doctrine*.

99. Ministerio de Defensa de la Federación Rusa, "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space," (2011) traducido por el Departamento de Estado de Estados Unidos.

100. "The new doctrine of information security pointed out the danger of destabilization via the Internet," *Russian News*, 10 de septiembre de 2015, *http://en.news-4-u.ru/the-new-doctrine-of-information-security-pointed-out-the-danger-of-destabilization-via-the-internet.html*.

101. El Ministerio de Defensa de Brasil también ha recientemente ordenado al Estado Mayor Conjunto de las Fuerzas Armadas (EMCFA) mejorar la defensa nacional cibernética a través de la creación de un Comando de Defensa Cibernética de servicio tripartito (ComDCiber). Si bien el ComDCiber comprenderá los tres servicios, el Ejército lo liderará. ComDCiber se basará en el previamente establecido Núcleo del Centro de Defensa Cibernética brasileño (NU CDCiber) en Brasilia. Ver eelnigo Guevara, "Brazil to stand up Cyber Defence Command," IHS Jane's Defence Weekly, 4 November 2014 y Diego Rafael Canabarro y Thiago Borne, "Brazil and the Fog of (Cyber) War," National Center for Digital Governance (2013): 5. Sobre las capacidades cibernéticas de Corea, ver: Republic of Korea, "Defense White Paper," (2014), 57, *http://www.*

mnd.go.kr/user/mnd_eng/upload/pblictn/PBLICTNEBOOK_20150616115616457O.pdf.

102. Zachary Keck, "South Korea Seeks Offensive Cyber Capabilities," *The Diplomat*, 11 de octubre de 2014, *http://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites/*.

103. Para tener una visión general de la estrategia cibernética de China, véase: Amy Chang, "Warring States," *The Center for New American Security*, (December 2014).

104. Oficina de Información del Estado, "White Paper: The Diversified Employmenet of China's Armed Forces," Abril de 2013, *http://eng.mod.gov.cn/Database/WhitePapers/* and Xi Jinping, Cental Military Commission, "Opinion on Further Strengthening Military Information Security Work," traducción parcial de Amy Chang, "Warring States," The Center for New American Security, (December 2014): 20.

105. Directores Generales del Consejo Nórdico, "Icelandic Cyber Responsibilities," (reunión entre Melissa Hathaway y Directores Generales y las respectivas delegaciones del Consejo Nórdico que son responsables de Equipos Nacionales de Respuesta a emergencias informáticas, Estocolmo, Suecia, 19 de Noviembre de 2014).

106. El Ministro del Interior, "Icelandic National Cyber Security Strategy 2015-2026: Plan of Action," *Icelandic Minister of the Interior* (June 2015), *http://eng.innanrikisraduneyti.is/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf*.

107. Yaakov Katz, "Security and Defense," *The Jerusalem Post*, 8 October 2010 en James Lewis y Katrina Ti-mlin, "Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization," *UNIDIR Resource and Center for Strategic and International Studies* (2011), 14 y "Eye on tech exports, Israel launches cyber command," *Reuters*, 18 de mayo de 2011, *http://www.reuters.com/article/2011/05/18/us-israel-security-cyber-idUSTRE74H27H20110518*.

108. Mitch Ginsburg, "Army to establish unified cyber corps," *The Times of Israel*, Junio 16 de 2015.

109. Michael Herzog, "New IDF Strategy Goes Public," The Washington Institute: Policy Watch 2479(28 de agosto de 2015), *http://www.washingtoninstitute.org/policy-analysis/view/new-idf-strategy-goes-public*.

SOBRE LOS AUTORES

Melissa Hathaway es experta destacada en la política del ciberespacio y seguridad cibernética. Es Miembro Senior y miembro de la Junta de Regentes del Instituto Potomac de Estudios de Política y es Asesora Senior en el Belfer Center for Science and International Affairs del Harvard Kennedy School. Ella también es Miembro Distinguido en el Centre for International Governance Innovation en Canadá y fue nombrada en la Comisión Mundial sobre la Gobernanza de Internet (Comisión Bildt). Ella trabajó en dos administraciones presidenciales, donde encabezó la Revisión de las Políticas de Ciberespacio para el presidente Barack Obama y dirigió la Iniciativa Integral de Seguridad Cibernética Nacional para el presidente George W. Bush. Desarrolló una metodología única para evaluar y medir el nivel de preparación de ciertos riesgos de seguridad cibernética, conocido como el Cyber Readiness Index. Ella publica regularmente artículos en materia de seguridad cibernética que afectan a las empresas y países. La mayoría de sus artículos se pueden encontrar en la siguiente página web: *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html*.

Chris Demchak es experta en la materia en el proyecto de Cyber Readiness Index del Instituto Potomac de Estudios de Política. Sus áreas de investigación son la resistencia digital, conflicto cibernético, y las estructuras y los riesgos del espacio cibernético. Diseñó un modelo de organización digitalizada conocida como "Atrium" que ayuda a las grandes empresas responder a e incluir las sorpresas en sus sistemas. También es autora de *Wars of Disruption and Resilience: Cybered Conflict*, *Power and National Security*.

Jason Kerben es experto en la materia en el proyecto de Cyber Readiness Index del Instituto Potomac de Estudios de Política. También se desempeña como Asesor Senior de varios departamentos y agencias en asuntos relacionados con la seguridad de la información y la seguridad cibernética. En particular, se centra en los regímenes legales y reglamentarios que afectan la misión de una organización. Desarrolla metodologías y enfoques para evaluar y gestionar los riesgos de seguridad cibernética y asesora en muchas actividades específicas de seguridad cibernética, incluyendo los principios internacionales que rigen las tecnologías de la información y comunicaciones, gestión de acceso e identidad, diagnósticos continuos y la mitigación y el seguro cibernético.

Jennifer McArdle es Miembro en el Centro de Pensamiento Científico Revolucionario en el Instituto Potomac de Estudios de Política. Su investigación académica se centra en la guerra cibernética, la guerra de información, y la geopolítica de Asia. Actualmente es estudiante de doctorado en el Kings College de Londres en el departamento de Estudios de Guerra.

Francesca Spidalieriis es experta en la materia en el proyecto Cyber Readiness Index del Instituto Potomac de Estudios de Política. Ella también se desempeña como Miembro Senior para Liderazgo Cibernético en el Centro Pell, de la Universidad Salve Regina. Sus investigaciones y publicaciones académicas se han centrado en el desarrollo de liderazgo cibernético, la gestión de riesgos cibernéticos, la educación y la conciencia cibernética y el desarrollo del personal de seguridad cibernética. Recientemente publicó un informe sobre el Estado de los Estados sobre seguridad cibernética, que utiliza el Cyber Readiness Index 1.0 a nivel estatal de Estados Unidos.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org