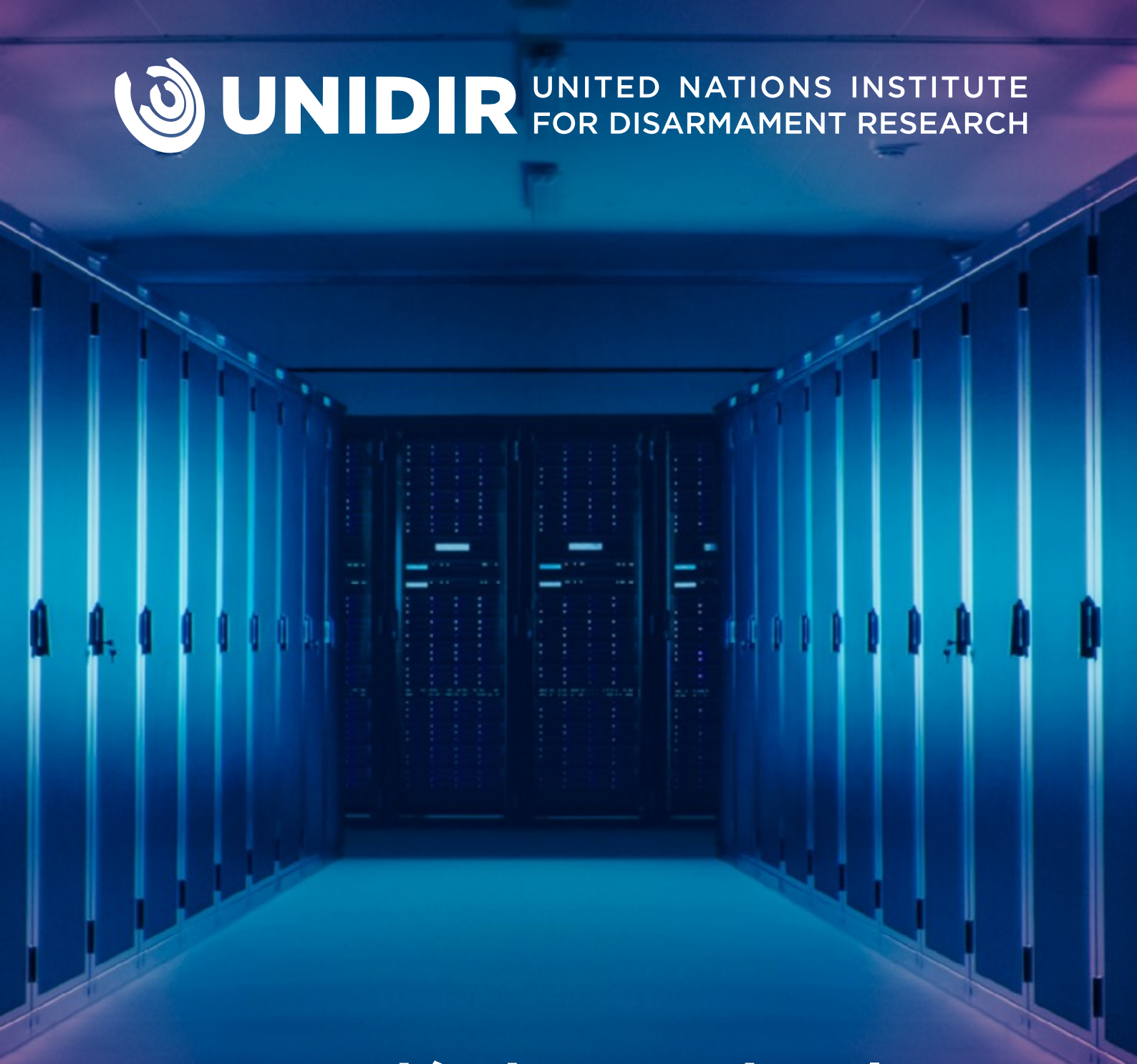
UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH



Cooperación internacional para mitigar las operaciones cibernéticas contra la infraestructura crítica

Expectativas normativas y buenas prácticas emergentes

ANDRAZ KASTELIC

Agradecimientos

El apoyo de los principales proveedores de fondos de UNIDIR constituye la base de todas las actividades del Instituto. Este estudio fue producido por el grupo de trabajo de Estabilidad Cibernética del Programa de Seguridad y Tecnología de UNIDIR, financiado por los Gobiernos de Francia, Alemania, los Países Bajos, Noruega y Suiza, y Microsoft. El autor desea agradecer a los siguientes individuos por su valioso asesoramiento y asistencia en la producción de este informe: Kerry-Ann Barrett (Organización de los Estados Americanos); Giacomo Persi Paoli (UNIDIR) y los participantes de nuestro diálogo de múltiples partes interesadas, "Operacionalización de las normas cibernéticas: Protección de infraestructuras críticas," llevado adelante el 3 de julio de 2020: Oleg Abdurashitov (Kaspersky), Kaja Ciglic (Microsoft), Marc Henauer (Centro Nacional de Seguridad Cibernética, Suiza), Wolfram von Heynitz (Ministerio Federal de Relaciones Exteriores, Alemania), Daniel Klingele (Departamento Federal de Asuntos Exteriores, Suiza), Timo S. Koster (Ministerio de Relaciones Exteriores, Países Bajos), Chris Kubecka (HypaSec) y Andre Salgado (Grupo CITI). También agradece a Evgeny Goncharov, Gleb Gritsai y Anastasiya Kazakova de Kaspersky por compartir su visión de la industria.

Diseño y formato de la publicación: Eric M. Schulz
Gráficos: Uros Podgorelec

Nota

Las designaciones empleadas en esta publicación y la forma en que en ella aparecen presentados los datos no implican, por parte de la Secretaría de la Organización de las Naciones Unidas, juicio alguno sobre la condición jurídica de países, territorios, ciudades o zonas, o de sus autoridades, ni respecto de la delimitación de sus fronteras o límites. Las opiniones expresadas en esta publicación son responsabilidad exclusiva de su autor. No reflejan necesariamente los puntos de vista u opiniones de la Organización de las Naciones Unidas, de UNIDIR o de sus funcionarios o patrocinadores.

Tabla de contenidos

Resumen ejecutivo vi

1 Contexto y problema 1

1.1. Prevalencia de incidentes cibernéticos que afectan la infraestructura crítica 1

1.2. Consecuencias de una disrupción en la infraestructura crítica 3

1.3. Desafíos relacionados con la gestión de las amenazas cibernéticas contra la infraestructura crítica 4

1.4. Protegiendo la infraestructura crítica: introducción de normas 6

1.5 Definición del alcance de este informe 7

2 Aplicación de la norma: acciones de preparación a nivel nacional 9

2.1 ¿Qué infraestructura es de hecho crítica? 9

2.2 Designación de sectores y subsectores pertinentes 10

2.3 Compilación y mantenimiento de una lista de activos críticos 10

2.4 Establecimiento de redes nacionales de resolución de crisis 12

3 Implementación mediante la participación de la comunidad internacional 13

3.1 Transparencia e intercambio de información 13

3.2 Puntos de contacto únicos 14

3.3 Realización de ejercicios (inter)nacionales de ciberseguridad 15

4 Respuesta a un incidente cibernético en el contexto de la norma 17

4.1 Mejores prácticas para la comunicación internacional 17

4.2 Enfoque de respuesta inclusivo y de múltiples partes interesadas 18

4.3 La diferencia entre asistencia y mitigación 18

5 Conclusión 21

Referencias 23

Sobre el autor

ANDRAZ KASTELIC es el principal investigador de Ciberestabilidad del Programa de Seguridad y Tecnología de UNIDIR. Antes de incorporarse a UNIDIR ocupó diversos puestos de investigación en organizaciones internacionales e instituciones de investigación en diferentes partes del mundo.

Sobre UNIDIR

El Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) es un instituto autónomo dentro de la Organización de las Naciones Unidas, financiado con contribuciones voluntarias. Es uno de los pocos institutos especializados del mundo que se centra en el desarme; genera conocimiento y promueve el diálogo y la acción en materia de desarme y seguridad. Con sede en Ginebra, UNIDIR ayuda a la comunidad internacional a desarrollar las ideas prácticas e innovadoras necesarias para encontrar soluciones a problemas críticos de seguridad.

Abreviaturas y siglas

GEG	GRUPO DE EXPERTOS GUBERNAMENTALES
TIC	TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN
GTCA	GRUPO DE TRABAJO DE COMPOSICIÓN ABIERTA
ONU	ORGANIZACIÓN DE LAS NACIONES UNIDAS
UNIDIR	INSTITUTO DE LAS NACIONES UNIDAS DE INVESTIGACIÓN SOBRE EL DESARME

Resumen ejecutivo

Las operaciones cibernéticas maliciosas suponen una amenaza para las infraestructuras críticas y, por lo tanto, para el bienestar de nuestras sociedades. Los incidentes graves tienen el potencial de desestabilizar Estados y poner en peligro la paz y la seguridad internacionales.

Para hacer frente al riesgo de las cada vez más complejas y eficaces amenazas cibernéticas dirigidas a infraestructuras críticas, la comunidad internacional busca promover la cooperación haciendo uso de las normas de comportamiento esperado de los Estados en el ciberespacio. Este informe investiga la norma —como fue propuesta en 2015 por el Grupo de Expertos Gubernamentales de la Organización de las Naciones Unidas sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional— que insta a los Estados a responder a las solicitudes internacionales de asistencia o mitigación frente a operaciones cibernéticas maliciosas contra infraestructuras críticas.[1]

Para implementar esta norma, el informe sugiere que los Estados y la comunidad internacional deberían adoptar las siguientes medidas:

- Los Estados deben desarrollar una definición clara de su infraestructura crítica nacional e internacional, identificar sectores cuyos productos o servicios califiquen como infraestructura crítica y mantener una lista de activos críticos. Estas definiciones y designaciones deben compartirse con la comunidad internacional como medida de fomento de la confianza.
- Los Estados deben establecer redes de resolución de crisis que incluyan a los actores nacionales pertinentes.
- La comunidad internacional debe establecer una red de puntos de contacto únicos en las entidades nacionales competentes y autorizarlos a comunicarse con sus contrapartes internacionales.
- Los Estados deben realizar ejercicios internacionales de ciberseguridad periódicos para probar su capacidad de comunicación con otros Estados y su capacidad de responder a las solicitudes de asistencia y mitigación (canales de comunicación, protocolos y procedimientos, en particular).

1 AGNU (2015b, III: párr. 13(h)).

- Al comunicar solicitudes de asistencia o mitigación, los Estados no necesitan buscar establecer protocolos internacionales universales, sino que deben seguir las mejores prácticas existentes relativas a la notificación de incidentes en los contextos nacionales e internacionales pertinentes.
- Aquellos Estados que participen de esfuerzos de cooperación en respuesta a operaciones cibernéticas maliciosas contra infraestructuras críticas deben utilizar las redes nacionales de resolución de crisis de múltiples partes interesadas preestablecidas y apoyarse en los conocimientos especializados en materia de mitigación proporcionados por el Estado y agentes no estatales en caso de enfrentarse a una operación cibernética de este tipo.
- Las expectativas normativas de asistencia y mitigación dependen del contexto. En caso de que se produzca una operación cibernética maliciosa contra la infraestructura crítica, el Estado desde el cual se inicia la operación (es decir, el Estado de emanación) debe adoptar medidas razonables para poner fin a la operación cibernética en cuestión o reducir al mínimo la propagación del código malicioso central de la operación cibernética.
- Los Estados que reciban una solicitud de asistencia debe hacer todo lo posible para proporcionar ayuda en la forma solicitada por el Estado afectado. El concepto de asistencia no se limita a la acción directa contra la operación cibernética maliciosa, sino que puede entrañar cualquier forma de ayuda que minimice las consecuencias de la operación cibernética contra la infraestructura crítica.



1. Contexto y problema

Las operaciones cibernéticas maliciosas contra la infraestructura crítica, es decir los activos esenciales para el mantenimiento de funciones vitales para el bienestar de una sociedad determinada,[2] suponen una amenaza no solo para el bienestar del Estado atacado, sino también para la paz y la seguridad internacionales.[3] Sectores normalmente incluidos en definiciones de infraestructura crítica incluyen energía, transporte, atención sanitaria, gobierno, producción y suministro de alimentos, abastecimiento de agua, servicios financieros, telecomunicaciones y fabricación crítica.[4]

Aunque el alcance y los efectos específicos de los incidentes cibernéticos que afectan a la infraestructura crítica no pueden establecerse de forma confiable, las instancias registradas atestiguan el potencial devastador de tales incidentes. Debido a la naturaleza esencial de la infraestructura crítica, los incidentes cibernéticos que la afectan pueden tener consecuencias nefastas para nuestras sociedades, incluyendo ramificaciones económicas, daños materiales e incluso lesiones en los seres humanos.

En 2015, el Grupo de Expertos Gubernamentales (GEG) de las Naciones Unidas sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional propuso una norma internacional destinada a facilitar la cooperación internacional en caso de una operación cibernética contra la infraestructura crítica. Este informe tiene por objeto ayudar a comprender cómo poner en práctica dicha norma, y está estructurado de la siguiente manera:

- El resto de la primera sección detalla los desafíos asociados con la protección de infraestructuras críticas frente a ciberamenazas y describe la norma antes mencionada.
- En la segunda sección se enumeran medidas preparatorias que los Estados deberían considerar implementar antes de que ocurra un incidente cibernético.
- En la tercera sección se recomiendan medidas a implementarse a nivel internacional.
- En la cuarta sección se proponen medidas para implementar la norma del GEG tras la ocurrencia de un incidente cibernético.
- En la quinta sección se indican algunas preguntas no resueltas y se sugieren orientaciones para futuros debates internacionales o proyectos de investigación.

1.1 Prevalencia de incidentes cibernéticos que afectan infraestructuras críticas

Recientemente, varias operaciones cibernéticas notorias paralizaron infraestructuras críticas diversas.[5] Sin embargo, sigue siendo difícil determinar el número exacto de tales incidentes y, por lo tanto, determinar si se están volviendo más frecuentes o disruptivos. Este desafío se debe a:

---

2 No existe una definición acordada a nivel internacional de infraestructura crítica. Este informe adopta una definición de trabajo inspirada en el Consejo de la Unión Europea (2008, art. 2(a)), aunque se dan algunos ejemplos alternativos (véase la sección 2.1).
3 GTCA (2021, párr. 18).
4 Los sectores que se consideran críticos depende del contexto. Véase la sección 2.2.
5 Véase, por ejemplo, Steffen (2016) sobre una serie de operaciones cibernéticas contra hospitales alemanes; Gallagher (2020) sobre operaciones cibernéticas contra instituciones sanitarias en todo el mundo; la Agencia de Seguridad Cibernética e Infraestructura de Estados Unidos (2020) sobre operaciones cibernéticas que causan pérdida de productividad e ingresos en un instalación de compresión de gas natural; y Statt (2021) sobre una operación cibernética que interfirió con una planta de tratamiento de agua.

- Variaciones de definición entre países y sectores.
- Diferentes enfoques para medir la frecuencia y el impacto de las operaciones cibernéticas.
- Gran incertidumbre respecto del número real de operaciones cibernéticas.

La primera razón por la que cuantificar es desafiante es que el concepto de infraestructura crítica no está ni clara ni universalemente definido; su significado depende significativamente del contexto nacional. Por ejemplo, si bien algunos Estados confían en el sector turístico para una parte considerable de su producto bruto interno y, por lo tanto, podrían calificar su infraestructura de base como crítica,[6] es posible que el mismo sector no sea tan crucial para otros Estados. Por ende, cualquier estadística que exponga las tendencias de los incidentes cibernéticos contra "infraestructura crítica" definida de manera general debe leerse con precaución.

Además, el concepto `infraestructura crítica´ es multifacético, y distintos sectores muestran diferentes tendencias de incidentes cibernéticos. Sería una generalización decir que las operaciones cibernéticas maliciosas dirigidas a todos los sectores de la infraestructura crítica están en aumento o en declive: una evaluación plena de la evolución del panorama de amenazas requiere un análisis más detallado y específico de cada sector.

Por último, muchas de las operaciones cibernéticas maliciosas que afectan la infraestructura crítica puede que sucedan sin ser detectadas o notificadas. Por lo tanto, la cantidad de incidentes cibernéticos que afectan las infraestructuras críticas podría ser superior que lo que indicarían las estadísticas e informes disponibles. Kaspersky reporta que la mayoría de los incidentes cibernéticos que afectan infraestructuras críticas no son revelados y por ende no son de conocimiento público, ya sea como resultado de solicitudes explícitas de los operadores de infraestructura o porque los operadores de infraestructura no pueden revelar tales incidentes conforme la legislación local.[7] Del mismo modo, el Comité Internacional de la Cruz Roja hace hincapié en "la dificultad de evaluar cuántas operaciones no fueron detectadas, realmente cuánto alcance han tenido los atacantes en la infraestructura, o si se han establecido accesos encubiertos para uso futuro, como interruptores de corte, por ejemplo."[8]

Por lo tanto, tal vez no sea sorprendente que las investigaciones realizada por distintas empresas de seguridad reflejen tendencias diferentes y a veces contradictorias. Por ejemplo:

- IBM informa de que el número de incidentes cibernéticos que afectan a los sistemas de control industrial y a las redes de tecnología operativa, utilizados con frecuencia por la infraestructura crítica, fue mayor en 2019 que en los tres años anteriores combinados.[9]
- La investigación realizada por Kaspersky indica que la proporción de códigos maliciosos dirigidos a ordenadores de sistemas de control industrial en realidad ha disminuido en el segundo semestre de 2019 y el primer semestre de 2020. La tendencia se ha invertido recién en el segundo semestre de 2020.[10]

---

6 Véase, por ejemplo, República de Mauricio (2014).
7 Correspondencia personal con Evgeny Goncharov, director de Kaspersky Lab ICS CERT, octubre de 2020.
8 [Traducción no oficial]. Gisel & Olejnik (2019, 25).
9 Servicios de Inteligencia de Amenazas y Respuesta a Incidentes IBM X-Force (2020, 6).
10 CERT de Kaspersky ICS (2020b, 13, 15); CERT de Kaspersky ICS (2021).

1.2 Consecuencias de una disrupción en la infraestructura crítica

Independientemente del número exacto de operaciones cibernéticas contra infraestructuras críticas, se han producido suficientes incidentes para justificar la preocupación por mantener la seguridad de una infraestructura crítica cada vez más conectada. A principios de 2020, por ejemplo, una operación cibernética maliciosa dirigida al Hospital Universitario Brno en Chequia lo obligó a suspender sus cirugías programadas y remitir a sus pacientes a centros vecinos.[11] Cuatro años antes, la compañía de distribución de electricidad de Ucrania reportó un corte de red de varias horas como consecuencia de una operación cibernética dirigida a sus ordenadores y sistemas de control de supervisión y adquisición de datos. Aproximadamente 225.000 clientes experimentaron cortes de energía.[12]

No todas las operaciones cibernéticas contra infraestructura crítica provocan interrupciones en los servicios críticos, aunque sí permiten vislumbrar las posibles graves consecuencias. Por ejemplo, en abril de 2020 las autoridades israelíes informaron sobre una operación cibernética contra los sistemas de tratamiento de agua del país que tenían como objetivo estropear las vías navegables regionales.[13] Se registró un incidente similar a principios de 2021 en una instalación de tratamiento de agua en Florida.[14]

Durante la última década, cada vez más gobiernos nacionales se han unido a empresas privadas[15] y profesionales de seguridad[16] en reconocer que este tipo de incidentes se encuentra entre los problemas de ciberseguridad más destacados. En 2015, el GEG señaló en su informe que "el riesgo de ataques dañinos de esta naturaleza [de las tecnologías de la información y las comunicaciones] contra infraestructuras fundamentales es a la vez real y grave."[17]

Por definición, una disrupción de la infraestructura crítica podría tener consecuencias de gran alcance, socavar peligrosamente las funciones vitales de las que dependen las sociedades, así como provocar destrucción física y lesiones humanas o muertes.[18] Por ejemplo, una operación cibernética bien ejecutada contra los elementos clave de distribución de energía podrían, al menos en teoría, privar a todo un país de electricidad.[19] Aunque se desconozcan las consecuencias exactas de la operación cibernética contra el sistema de suministro eléctrico ucraniano mencionada anteriormente, las ramificaciones económicas que se han producido tras otros cortes de energía locales[20] y nacionales[21] han sido documentados en detalle. También se ha comprobado que los cortes de energía producen un aumento de los niveles de mortalidad no accidental.[22]

---

11 Khalili (2020).
12 Lee et al. (2016).
13 Cimpanu (2020).
14 Statt (2021).
15 Siemens Gas & Power (2019).
16 ENISA (2019, 109); Security Magazine (2020).
17 AGNU (2015b, II: párr. 5).
18 Durante las reuniones del Grupo de Trabajo de Composición Abierta sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional de 2020, los Estados hicieron hincapié en que los ataques a infraestructuras críticas "suponen una amenaza no solo para la seguridad, sino también para el desarrollo económico y los medios de subsistencia, y en última instancia, la seguridad y el bienestar de las personas" [traducción no oficial] (GTCA, 2020, párr. 22).
18 Smith et al. (2019).
20 Shuaia et al. (2018).
21 Schmidthaler & Reichl (2016).
22 Anderson & Bell (2012).

Las operaciones cibernéticas dirigidas a otras infraestructuras pueden no resultar directamente en lesiones a los seres humanos, pero pueden paralizar gravemente a una sociedad. Por ejemplo si se utiliza para atacar a los sistemas financieros nacionales e internacionales, el uso malintencionado de las tecnologías de la información y las comunicaciones (TIC) podría "poner en peligro la estabilidad financiera"[23] y, por lo tanto, a los aspectos de las funciones de una una sociedad que dependan de flujos financieros estables. La operación cibernética de 2007 contra, entre otras cosas, el sector bancario de Estonia, impidió a la población utilizar la banca en línea. A pesar de que la infraestructura de la red informática de Estonia no sufrió daños físicos, se dijo que el país, en el que el 97 % de las transacciones bancarias se realizan en línea,[24] estuvo temporalmente paralizado.[25]

1.3 Desafíos relacionados con la gestión de las amenazas cibernéticas contra la infraestructura crítica

El riesgo de las nefastas consecuencias de un incidente a una infraestructura crítica se ve agravado por la evolución del panorama de amenazas cibernéticas, el que se caracteriza por una serie de factores:

- Ataques nuevos y cada vez más complejos.[26] Actores maliciosos idean nuevos vectores de ataque y desarrollan nuevas formas de explotación continuamente. Hoy en día, el software malicioso dirigido a la infraestructura crítica se adapta cada vez más al objetivo y, por ende es más sofisticado.

- Expansión rápida de la superficie de ataque.[27] Esto se debe principalmente a la creciente interconexión de los sistemas TIC que se emplean en activos de infraestructura crítica. Los arreglos de teletrabajo implementados como respuesta a la pandemia del COVID-19 han acelerado o agravado este problema.[28]

- Sistemas obsoletos heredados que no son lo suficientemente resistentes a nuevas amenazas y contribuyen a la creciente vulnerabilidad de la infraestructura crítica. Por ejemplo, según un informe del Congreso estadounidense, los sistemas informáticos de control industrial, parte integral de la infraestructura crítica, son "puntos específicos de vulnerabilidad, ya que la ciberseguridad de estos sistemas previamente no era percibida como una prioridad alta."[29] Evaluaciones similares han sido promovidas, por ejemplo, por Microsoft[30] y en contribuciones académicas.[31]

---

23 [Traducción no oficial]. G-20 (2017, párr. 7).
24 Herzog (2011, 51).
25 Ilves (2007).
26 "El panorama de amenazas se está volviendo extremadamente difícil de trazar. No solo los atacantes están desarrollando nuevas técnicas para evadir los sistemas de seguridad, sino que las amenazas aumentan en complejidad y precisión en los ataques dirigidos" [traducción no oficial] (ENISA, 2020c). Y, como señala Kaspersky, "las amenazas están cada vez más centradas y focalizadas y, como resultado, son más variadas y complejas" [traducción no oficial] (Kaspersky ICS CERT, 2020b).
27 Por ejemplo, según Bhunia & Tehranipoor (2019, cap. 1), "La superficie de ataque es la suma de todas las posibles exposiciones a riesgos de seguridad" [traducción no oficial]. En otras palabras, la superficie de ataque representa el conjunto de puntos de acceso potenciales que los actores maliciosos pueden explotar durante una operación cibernética. Véase también las predicciones de ENISA (2020c, 10).
28 Véase, por ejemplo, CISA de EE. UU. (2020b).
29 [Traducción no oficial]. Shea (2004).
30 "Tradicionalmente, las redes de tecnología operativas (TO) utilizadas en entornos de infraestructura industrial y crítica se encuentran aisladas de las redes de TI corporativas y del Internet, pero la transformación digital ha aumentado tanto la conectividad como el número de dispositivos en estos entornos, lo que ha generado un mayor riesgo. Muchos de los protocolos y dispositivos de IoT [Internet de las cosas] /TO integrados en estos entornos se diseñaron hace años, y no cuentan con controles modernos, tales como el cifrado, la autenticación sólida y pilas de software reforzadas, lo que incrementa aún más el riesgo." [traducción no oficial]. (Microsoft, 2020, 31).
31 Por ejemplo, "las organizaciones sanitarias y las universidades a menudo carecen de recursos para protegerse contra los ciberataques" [traducción no oficial], según argumenta Muthuppalaniappan & Stevenson (2020).



– Insuficientes recursos asignados a esfuerzos de prevención.[32] Por ejemplo, la operación cibernética de 2018 que afectó gravemente la capacidad de brindar asistencia del Servicio Nacional de Salud del Reino Unido[33] podría haberse evitado si los operadores hubieran dedicado recursos a mantener los sistemas informáticos actualizados (y por ende inmunizados) antes del incidente.[34] La falta de diligencia ciertamente no es exclusiva de este ejemplo; también se puede observar en otras jurisdicciones y sectores de infraestructura crítica.[35] Según Microsoft, el 71 % de los sistemas de control industrial dependen de versiones obsoletas del sistema operativo Windows que Microsoft[36] ya no actualiza regularmente con parches de seguridad.

– Imprevisibilidad de los efectos, incluido su alcance. Las interdependencias entre infraestructuras críticas son un fenómeno bien documentado, y los incidentes cibernéticos pueden tener consecuencias negativas impredecibles y de amplio alcance, extiendéndose más allá de las fronteras de un país. El efecto de estas interdependencias puede observarse en la falla del elemento de la red eléctrica de Alemania en noviembre de 2006, el que ocasionó una escasez de energía en 20 países de Europa y más allá, afectando alrededor de 15 millones de hogares.[37] Aunque este incidente no fue el resultado de una operación cibernética, es ilustrativo de la posible interrupción generalizada que podrían causar las operaciones cibernéticas contra la infraestructura crítica.

---

32 BBC (2017); Maglaras et al. (2018, 42).
33 Ghafur et al. (2019).
34 Morse (2017).
35 Véase, por ejemplo, DOE de los EE.UU. (2019).
36 Microsoft (2020, 31).
37 Van der Vleuten y Lagendijk (2010).

1.4 Protegiendo la infraestructura crítica: introducción de normas

Todos los factores descritos en la sección anterior apuntan a la necesidad de colaboración internacional para prevenir o mitigar las operaciones cibernéticas maliciosas dirigidas a infraestructuras críticas. Un enfoque al que la comunidad internacional se ha dedicado en la última década para asegurar las infraestructura críticas, elevar la seguridad (inter)nacional y evitar posibles desastres y daños a los seres humanos se centra en las normas de comportamiento responsable en el ciberespacio.[38]

Para "reducir los riesgos para la paz, la seguridad y la estabilidad internacionales"[39] y, en particular para minimizar el impacto de las operaciones cibernéticas maliciosas contra la infraestructura crítica, el GEG de 2015 propuso tres normas específicas de comportamiento estatal responsable en el ciberespacio, elaborando las expectativas del comportamiento de Estados en relación con la seguridad de la infraestructura crítica en la era cibernética. Estas normas indican que los Estados deben:

- Abstenerse de realizar operaciones cibernéticas contra infraestructuras críticas que se encuentren bajo jurisdicción extranjera.
- Proteger su propia infraestructura crítica frente a operaciones cibernéticas maliciosas.
- Considerar la cooperación internacional en caso de que se produzca una operación cibernética maliciosa contra la infraestructura crítica.[40]

Otras normas de comportamiento estatal responsable en el contexto de la infraestructura crítica

El que la comunidad internacional coloque la protección de la infraestructura crítica en la parte superior de la lista de preocupaciones vinculadas con la ciberseguridad internacional se evidencia también en el surgimiento de normas similares o relacionadas, concebidas y promovidas por varias asociaciones. Por ejemplo, los miembros del Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio se comprometieron a trabajar juntos en foros existentes y a través de organizaciones, instituciones, mecanismos y procesos pertinentes, a ayudarse mutuamente e implementar medidas de cooperación, en particular para prevenir y recuperarse de actividades cibernéticas maliciosas que amenacen o causen daños significativos, indiscriminados o sistémicos a las personas y a la infraestructura crítica.[41] Estas normas ayudarían a cerrar la brecha digital, ejemplificar la buena vecindad, aumentar la eficacia de las respuestas a incidentes[42] y contribuir en general a la estabilidad y seguridad del mundo interconectado. Esto sucede en especial si el elemento crítico de la infraestructura se extiende más allá de las fronteras de una nación, como es el caso de la infraestructura crítica internacional o supranacional,[43] tal como el núcleo público de Internet.[44]

---

38 Las soluciones tecnológicas, el derecho internacional, las medidas de creación de capacidad y el fomento de la confianza, también desempeñan un papel importante, aunque su exploración esté fuera del alcance de este informe. Véase, por ejemplo, Baker et al. (2020, 503); Gusev (2020, 314); AGNU (2015b, V).
39 AGNU (2015b, párr. 10).
40 AGNU (2015b, párr. 12(f)–(h)).
41 Ministerio de Europa y Asuntos Exteriores, Francia (2018).
42 NIST (2012, 45).
43 GTCA (2020, 17).
44 Gobierno de los Países Bajos (2017; 2020, 2).

1.5 Definición del alcance de este informe

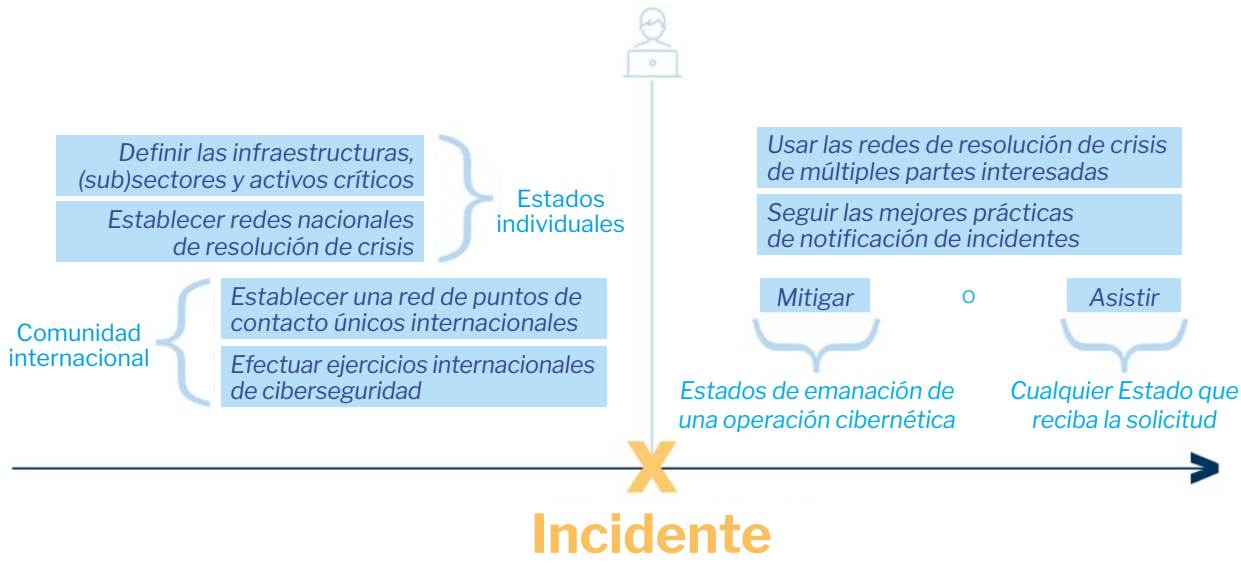
Si bien las tres normas incluidas en el informe del GEG de 2015, y descritas anteriormente, están interconectadas y se refuerzan mutuamente, **este informe se centra en la cuestión de la asistencia internacional y, más específicamente**, en cómo los Estados pueden estar mejor preparados para solicitar o responder a dicha asistencia cuando sea necesario.

Aunque existe una gran cantidad de estudios sobre la protección de la infraestructura crítica,[45] los requisitos internacionales de asistencia y mitigación en el contexto de la protección de la infraestructura crítica no han sido registrados, en especial no en el contexto de la norma pertinente del GEG. Si bien esta norma se centra en la respuesta a actos maliciosos de TIC contra infraestructuras críticas, su implementación se basa en una serie de acciones y actividades a nivel nacional, regional e internacional llevadas adelante antes y después de que se produzca el incidente. Estas actividades, que se analizan en detalle a lo largo del informe, se resumen en la Figura 1.

Muchas de las acciones y actividades discutidas en este informe son relevantes para mejorar las capacidades nacionales para prevenir, mitigar y responder o recuperarse de los actos cibernéticos maliciosos contra infraestructuras críticas. Sin embargo, el informe se centra en las modalidades de cooperación internacional y, por ende las medidas descritas no abarcan toda la gama de factores a tener en cuenta en el contexto más amplio del desarrollo de la capacidad cibernética. En particular, en el informe no se analizan las medidas preventivas que los Estados podrían adoptar para evitar que el incidente cibernético se materialice en primer lugar.

Figura 1:

Acciones sugeridas por este informe para garantizar la puesta en práctica de la norma del GEG analizada



45 Véase, por ejemplo, ENISA (2020a).



2. Aplicación de la norma: acciones de preparación a nivel nacional

Para garantizar un nivel suficiente de preparación, la operacionalización de la norma del GEG requiere el desarrollo previo de marcos estructurales nacionales habilitadores, antes de un posible evento cibernético malicioso. Por ende, **los Estados deben adoptar una definición general de infraestructura nacional crítica, identificar los (sub)sectores que califiquen y elaborar una lista de activos relevantes; también deben establecer redes nacionales de resolución de crisis**.

Los Estados que busquen orientación sobre el proceso de definición de infraestructura, sectores y activos críticos nacionales pueden utilizar diversos programas de asistencia,[46] documentación de referencia[47] y recopilaciones de buenas prácticas nacionales existentes[48] compiladas por organizaciones internacionales.

2.1 ¿Qué infraestructura es de hecho crítica?

Determinar el alcance de la infraestructura crítica es una prerrogativa soberana de los Estados. Esto no solo se alinea con el principio de soberanía del derecho internacional, sino que también ha sido confirmado explícitamente por la resolución 2341 del Consejo de Seguridad de las Naciones Unidas, afirmando que "cada Estado decide qué constituye su infraestructura vital".[49]

Dicho esto, la infraestructura puede clasificarse como crítica en función de su finalidad, sobre la base de los efectos de la interrupcións de los activos o servicios que habilita la infraestructura, o sobre la base de un híbrido de los dos principios.[50] Se han propuesto varios intentos regionales para especificar el alcance de la infraestructura crítica, los que pueden servir de guía para los Estados. Por ejemplo, en el Acuerdo de Cooperación para garantizar la seguridad internacional de la información entre los Estados miembros de la Organización de Cooperación de Shanghái, la infraestructura crítica se define como "instalaciones, sistemas e instituciones del Estado, cuyo impacto puede tener consecuencias que afecten directamente la seguridad nacional, incluida la seguridad de una persona, de la sociedad y del Estado".[51] Otros marcos internacionales y regionales proporcionan definiciones generales similares del concepto, como la Declaración de la Organización de los Estados Americanos sobre la protección de la infraestructura crítica frente a amenazas emergentes[52] y el Convenio de la Unión Africana sobre seguridad cibernética y protección de datos personales.[53]

46 Véase, por ejemplo, CICTE (2015, párr. 9)
47 OCDE (2008b); Suter (2007).
48 UNCTED & OLCT (2018).
49 CSNU (2017, 2). La prerrogativa nacional ha sido adoptada por ciertos marcos regionales, como la Unión Africana (2014, art. 24). Véase también, por ejemplo, la UIT (2010).
50 UNCTED & OLCT (2018, 58).
51 Organización de Cooperación de Shanghái (2009, 10).
52 CICTE (2015, párr. 11).
53 Unión Africana (2014, art. 1).

2.2 Designación de sectores y subsectores pertinentes

Siguiendo la adopción de una definición, **los Estados deben designar sectores (y posiblemente, subsectores) que califiquen y que serán considerados infraestructuras críticas nacionales**. Si bien las definiciones de infraestructura crítica probablemente muestren cierto grado de coherencia entre naciones, las listas de sectores designados como críticos serán sin duda diferentes.

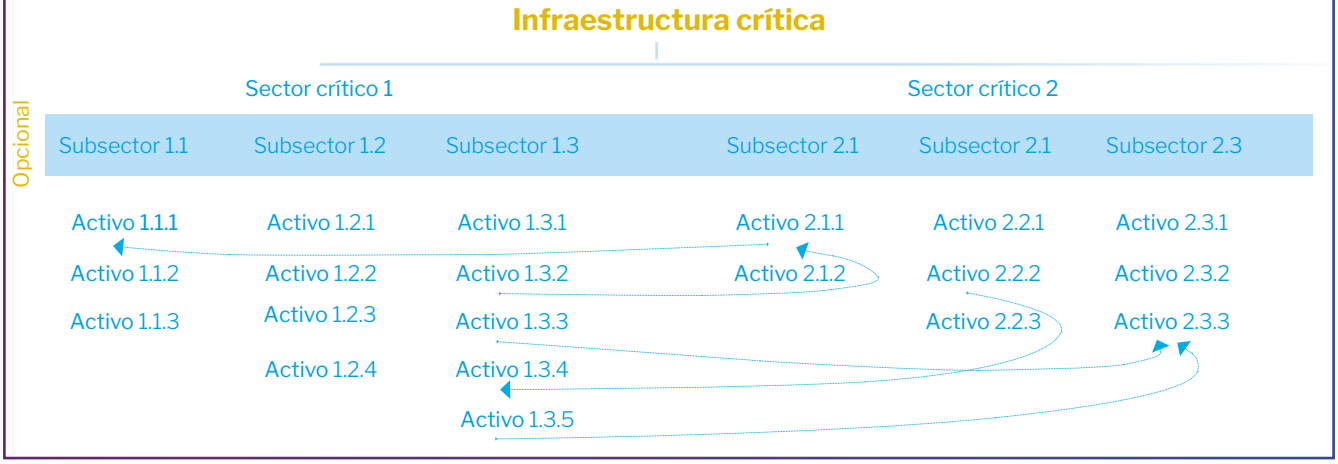
A menudo, los sectores considerados críticos son aquellos cuya perturbación podría provocar daños humanos, daños materiales generalizados e inestabilidad económica y social. En este contexto, es probable que sectores como el energético, el financiero, el abastecimiento de agua y alimentos, el transporte, las TIC y el gubernamental sean considerados críticos por la mayoría de los Estados.[54] Sin embargo, sectores como el turismo solo serán identificados como críticos por aquellos Estados cuyas economías dependan en gran medida de esos sectores.[55]

2.3 ¿Qué infraestructura es de hecho crítica?

Los Estados deben compilar y mantener una lista de activos críticos nacionales. Esta lista debe incluir entidades o activos específicos que permitan el funcionamiento de los (sub)sectores críticos determinados anteriormente. Teniendo en cuenta el carácter delicado de dicha lista debido a sus posibles implicaciones para la seguridad nacional, los Estados deben garantizar la adecuada comunicación e intercambio de información con las partes pertinentes, incluyendo los propietarios o gestores de activos. La lista también debería organizarse en diferentes grupos prioritarios en función de la vulnerabilidad de los activos y de la gravedad del impacto que tendría su mal funcionamiento. La lista también puede incluir activos calificados como infraestructura crítica internacional, situados fuera de la jurisdicción de un Estado específico, pero considerados críticos para el funcionamiento de su sociedad. Es imprescindible que los Estados revisen periódicamente sus listas de activos críticos junto con las asignaciones de grupos prioritarios para mantenerse al tanto de cambios en las circunstancias nacionales, así como la evolución del panorama de las amenazas cibernéticas.[56]

Figura 2:

Estructura teórica de la infraestructura crítica nacional (sectores, subsectores, activos), y sus interdependencias

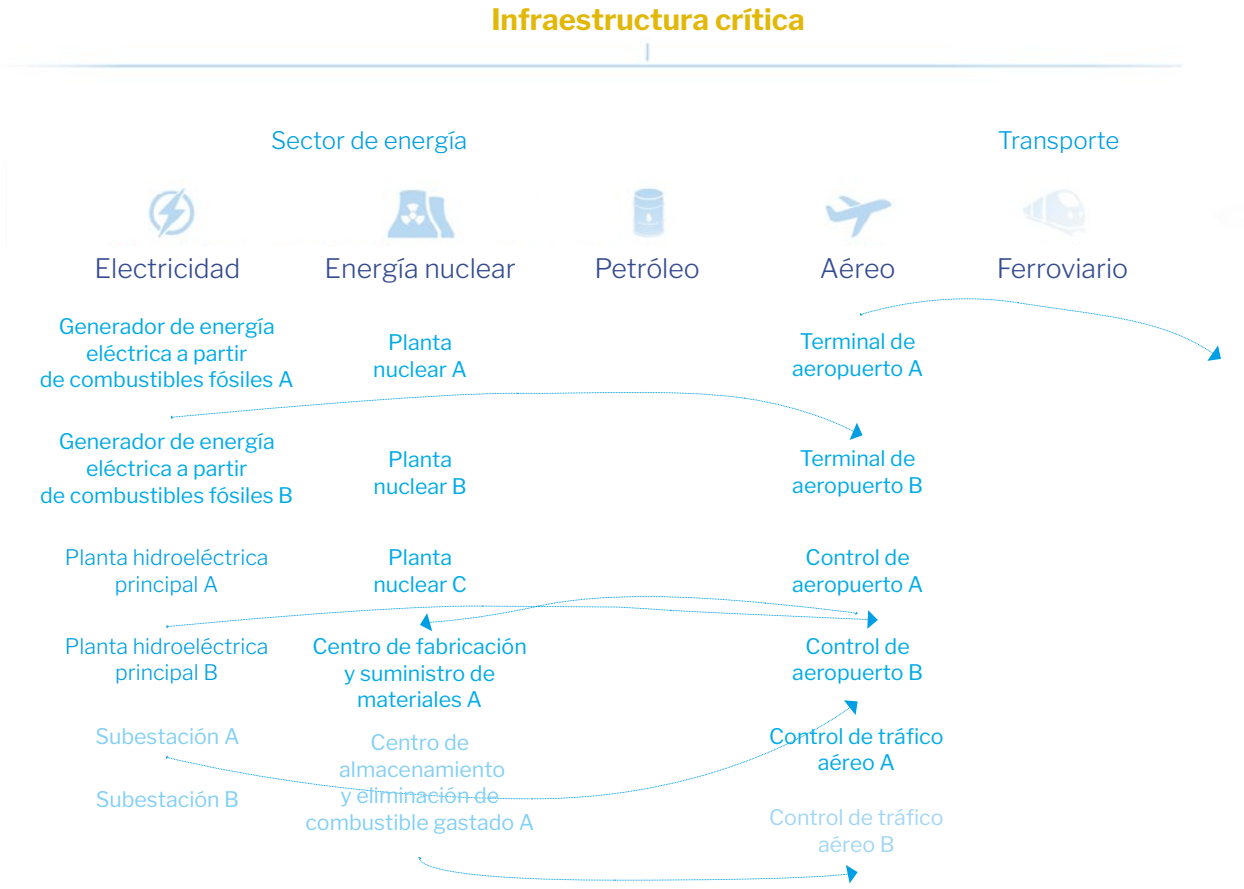


54 Véase, por ejemplo, Oficina Federal de Protección Civil, Suiza (2020).
55 Véase, por ejemplo, República de Mauricio (2014, 11).
56 Centro Global de Capacidad de Seguridad Cibernética (2016).

Puede haber interdependencias entre ciertos activos. Si, por ejemplo, una operación cibernética deshabilita una instalación específica de transición eléctrica de alta tensión, es probable que los activos pertenecientes a un sector diferente también se vean gravemente afectados, tal vez incluso deshabilitados, en ausencia de redundancias apropiadas.

Figura 3:

Ejemplo de estructura de infraestructura critica nacional, que muestra sectores, activos e interdependencias, activos e interdependencias



El progreso inherente, la consiguiente deflación de los precios de la tecnología y los rápidos procesos de digitalización, acelerados por la pandemia del COVID-19 están impulsando el aumento del número de activos considerados críticos, ampliando así el alcance de la infraestructura crítica. Sin embargo, los Estados deben evitar la tentación de extender el concepto de infraestructura nacional crítica más allá de sus límites: cuanto más amplio sea el alcance definido de la infraestructura crítica, mayor será la inversión estratégica necesaria del gobierno y de los operadores de infraestructura crítica para proteger esa infraestructura.[57] Por este motivo, los Estados deberían considerar la posibilidad de limitar el concepto de infraestructura crítica a los activos y sectores que sean verdaderamente vitales para el bienestar de la sociedad.

57 Este informe no aborda la puesta en práctica de la norma que sugiere que los Estados inviertan en proteger su infraestructura crítica. Existen muchos intentos de esbozar la protección de la infraestructura crítica. Véase, por ejemplo, Ministerio Federal del Interior, Alemania (2009); OCDE (2008a).



2.4 Establecimiento de redes nacionales de resolución de crisis

Además de definir el concepto de infraestructura crítica, los Estados deberían **considerar la posibilidad de establecer redes de resolución de crisis de múltiples partes interesadas entre los actores nacionales pertinentes**. Estas deben ser de naturaleza inclusiva e involucrar activamente a las entidades estatales y representantes del sector privado, entre otros, los operadores de infraestructura crítica, equipos privados de respuesta a emergencias informáticas y otros actores competentes dispuestos y capaces de contribuir a la resolución exitosa de un incidente cibernético que afecte la infraestructura crítica en el país o en el extranjero. Además, este tipo de redes también podría contribuir a los esfuerzos de prevención.

Aparte de los canales de comunicación establecidos, se necesitan protocolos y procedimientos nacionales ajustados y documentados que permitan un rápido flujo de información desde el operador de infraestructura crítica o la autoridad nacional competente (por ejemplo, un equipo de respuesta a emergencias informáticas) a un punto de contacto nacional para la emisión efectiva de una solicitud internacional de asistencia o mitigación. Al igual que las entidades colaborativas en el ámbito internacional, las partes interesadas nacionales deberían estar familiarizadas con los protocolos y procesos acordados.[58]

58 En UNCTED y OLCT (2018, 58) se hacen sugerencias similares.

3. Implementación mediante la participación de la comunidad internacional

Además de los esfuerzos domésticos por establecer redes nacionales de resolución de crisis, la eficiencia, la eficacia y la puntualidad de la cooperación internacional en respuesta a un acto de TIC malicioso contra la infraestructura crítica se beneficiarían de las siguientes acciones regionales e internacionales:

- Mayor transparencia e intercambio de información sobre el tema de la infraestructura crítica, incluyendo definiciones y alcance.
- Establecimiento de canales de comunicación específicos entre puntos de contacto claramente identificados.
- Desarrollo de protocolos y procedimientos para facilitar los flujos de información en canales de comunicación nacionales e internacionales.
- Ejercicios regionales e internacionales periódicos para probar el correcto funcionamiento de las redes de puntos de contacto, los protocolos y procedimientos.

3.1 Transparencia e intercambio de información

Los Estados deben practicar la transparencia y fomentar el intercambio periódico de información relativa a las conceptualizaciones nacionales de la infraestructura crítica. Con ese fin, el GEG de 2015 instó a los Estados a que suscriban la "presentación voluntaria por los Estados de sus opiniones nacionales sobre las categorías de infraestructura que consideran fundamentales y de las medidas nacionales para protegerlas, incluida información sobre leyes y políticas nacionales para la protección de datos y de infraestructuras sustentadas en las TIC".[59] El intercambio de información es uno de los principales facilitadores de la cooperación, la asistencia y la mitigación internacionales en el contexto de una disrupción de la infraestructura crítica por una operación cibernética maliciosa. No solo ayuda a los Estados a comunicar mejor sus necesidades en tiempos de crisis, sino que también permite evaluar mejor la respuesta requerida por parte de los Estados que reciben solicitudes de asistencia (o mitigación).

Existen varios repositorios regionales e internacionales para facilitar este intercambio de información. Uno de esos proyectos es el "Cyber Policy Portal" [Portal de Políticas Cibernéticas] de UNIDIR,[60] un repositorio digital de políticas nacionales de ciberseguridad de los Estados Miembros de la Organización de las Naciones Unidas, las organizaciones intergubernamentales regionales y los marcos multilaterales. Otro ejemplo es el National Cybersecurity Strategies Repository [Repositorio de Estrategias de Ciberseguridad Nacionales] de la Unión Internacional de Telecomunicaciones.[61]

59 AGNU (2015b, párr. IV(d)).
60 www.cyberpolicyportal.org
61 UIT (2020).

3.2 Puntos de contacto únicos

Los canales de comunicación establecidos e institucionalizados entre los miembros pertinentes de la comunidad internacional ayudarán a garantizar el flujo eficaz y rápido de información en caso de que se produzca una disrupción de la infraestructura crítica de un miembro. **La comunidad internacional debe intentar establecer una red global de puntos de contacto únicos dentro de las entidades nacionales competentes, autorizados a comunicarse con sus contrapartes internacionales** cuando la situación lo requiera.[62] Un ejemplo de dicha red es la lista de puntos de contacto únicos establecida por la Directiva NIS de la Unión Europea,[63] la que se actualiza periódicamente y está disponible libremente en línea.[64]

El informe del GEG de 2015 recomendó que los Estados consideren la posibilidad de establecer el directorio de puntos de contacto "en los niveles técnicos y de políticas."[65] Durante el debate del Grupo de Trabajo de Composición Abierta sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional (GTCA) en febrero de 2020, varias delegaciones[66] hablaron a favor de establecer una lista global de puntos de contacto, pero no adoptaron una posición unificada sobre la naturaleza o la competencia de las entidades de este directorio. Algunas delegaciones argumentaron a favor de puntos de contacto políticos; otras prefirieron una lista con múltiples puntos de contacto que representaran entidades de respuesta a emergencias informáticas, organismos de seguridad y orden público y otras partes interesadas pertinentes.[67] El informe sustantivo final del GTCA incluyó una recomendación de que los Estados establecieran un directorio global de puntos de contacto.[68]

La asistencia y la mitigación pueden adoptar muchas otras formas no técnicas.[69] Sin embargo, para reducir el riesgo de confusión e incertidumbre en momentos de crisis, se sugiere que cualquier lista futura de puntos de contacto incluya solo a las entidades nacionales oficialmente respaldadas que posean un conocimiento técnico y operativo adecuados para solicitar o facilitar asistencia y mitigación internacionales.

---

62 Actas del Diálogo de múltiples partes interesadas sobre la puesta en funcionamiento de las normas cibernéticas: protección de infraestructura crítica, 3 de julio de 2020 [archivos privados del autor]. La idea también ha sido promovida por el informe del GEG de 2015: véase AGNU (2015b, IV (a)).
63 UE (2016, art. 8).
64 CE (2020). Véase también G-7 (2019); Consejo Permanente de la OSCE (2013, art. 8). Aunque ocurra en un contexto ligeramente diferente y estrecho, la Convención sobre la Ciberdelincuencia también exige a los Estados que designen puntos de contacto nacionales para facilitar la lucha contra la ciberdelincuencia. Véase CdE (2004, art. 35).
65 AGNU (2015b, párr. 16(a)).
66 Argentina, Australia, Brasil, Canadá, Chile, Colombia, Ecuador, Estonia, Francia, Ghana, Malawi, Malasia, México, Nueva Zelanda, Federación de Rusia, Eslovenia, Suiza y República Árabe Siria (Gavrilović, 2020).
67 Gavrilović (2020).
68 GTCA (2021, párr. 51).
69 Consulte la sección 4.3.

3.3 Realización de ejercicios (inter)nacionales de ciberseguridad

La cooperación internacional exitosa está condicionada a redes funcionales de resolución de crisis y a protocolos y canales de comunicación eficaces. Por lo tanto, se sugiere que los Estados **realicen ejercicios de ciberseguridad nacionales e internacionales** con regularidad, los que pondrán a prueba su capacidad para comunicar o responder a solicitudes de asistencia y mitigación.

Los ejercicios nacionales de ciberseguridad evaluarán y fortalecerán la preparación de las redes nacionales de resolución de crisis y su capacidad para transmitir solicitudes de asistencia y mitigación apropiadas a otros Estados. Además, estos ejercicios fortalecerán la capacidad de ayudar a otro Estado en caso de una operación cibernética contra infraestructuras críticas.[70]

Los ejercicios internacionales de ciberseguridad también ayudan a desarrollar la capacidad de los Estados para comunicar eficazmente una solicitud de asistencia o mitigación, pero en particular a fortalecer los canales de comunicación entre los puntos de contacto, así como los protocolos y procedimientos internacionales utilizados. Además, los ejercicios internacionales de ciberseguridad también facilitan a fomentar la confianza entre Estados. La Unión Internacional de Telecomunicaciones, por ejemplo, ayuda con regularidad a los Estados a realizar ejercicios regionales de ciberseguridad.[71]

70 La OEA (2021) y la OSCE (2018), por ejemplo, apoyan a los Estados en la realización de ejercicios nacionales de ciberseguridad.
71 UIT (2021).


NEW YORK
SYDNEY

4. Respuesta a un incidente cibernético en el contexto de la norma

En su forma actual, la norma del GEG que solicita la cooperación internacional en un esfuerzo por detener una operación cibernética maliciosa contra infraestructuras críticas indica que no hay expectativas de diligencia debida ni ningún requisito de que la comunidad internacional se comunique proactivamente con el Estado afectado. Según la norma, el Estado cuya infraestructura crítica ha sido objeto de una operación cibernética tiene la responsabilidad de emitir una solicitud de asistencia o mitigación adecuada.

En este contexto, para garantizar la puesta en práctica de la norma, hay que determinar qué solicitudes constituyen "solicitudes de asistencia [o mitigación] apropiadas de otro Estado cuyas infraestructuras fundamentales fueran objeto de actos malintencionados relacionados con las TIC."[72]

4.1 Mejores prácticas para la comunicación internacional

En su interacción, los puntos de contacto deben seguir protocolos y procesos comúnmente reconocidos. Dados los desafíos de crear protocolos y procesos universales de comunicación, los **Estados deben seguir las mejores prácticas existentes relativas a la presentación de informes de incidentes en los contextos internacional y nacional**. Esto permitirá una comunicación óptima entre las partes involucradas y, por lo tanto, facilitará una resolución eficiente de incidentes.

La Guía de Buenas Prácticas de la Agencia para la Ciberseguridad sobre Informes de Incidentes de la Unión Europea[73] *y las Directrices Federales de Notificación de Incidentes del equipo de Preparación para Emergencias Informáticas de los Estados Unidos*[74] son ejemplos de marcos para el reporte de incidentes que podrían aprovecharse para este propósito. Ejemplos de protocolos técnicos que podrían utilizarse en el mismo contexto incluyen la Política de Intercambio de Información 2.0 y el Protocolo de Semáforos, ambos publicados por el Foro de Respuesta a Incidentes y Equipos de Seguridad.[75]

Además, una solicitud de asistencia y mitigación apropiada debe incluir no solo información sobre el incidente, sino también medidas específicas sugeridas que debe adoptar el Estado al que se dirige la solicitud.

72 AGNU (2015b, III: párr. 13 (h)).
73 ENISA (2009).
74 US-CERT (2015).
75 FIRST (2019).

4.2 Enfoque de respuesta inclusivo y de múltiples partes interesadas

Los Estados que participen en la lucha cooperativa de una operación cibernética maliciosa contra infraestructuras críticas deben **utilizar las redes nacionales de resolución de crisis de múltiples partes interesadas mencionadas anteriormente y apoyarse en la experiencia de mitigación proporcionada por el Estado y los actores no estatales pertinentes**. El sector privado posee una amplia experiencia en ciberseguridad y a menudo controla las tecnologías de infraestructura crítica relevantes. Por ende, cualquier intento de resolución de crisis sin la participación del sector privado es probable que logre resultados subóptimos.[76] Una vez más, es importante que los Estados inviertan en establecer redes nacionales de colaboración y resolución de crisis que incluyan canales de comunicación bien definidos y establezcan claramente las funciones y responsabilidades de los miembros de la red.

4.3 La diferencia entre asistencia y mitigación

Según lo estipulado en la norma en cuestión, los Estados "deberían atender las solicitudes de asistencia apropiadas" o "solicitudes apropiadas para mitigar toda actividad malintencionada relacionada con las TIC originada en su territorio contra infraestructuras fundamentales de otro Estado".[77] No se espera que los Estados que reciban solicitudes de asistencia o mitigación actúen más allá sus medios, simplemente se espera que hagan todo lo posible para proporcionar ayuda con los recursos disponibles en ese momento. Pero, ¿cuál es la diferencia entre asistencia y mitigación?

En primer lugar, cuando no se puede determinar el origen de una operación cibernética o cuando una operación cibernética emana de la infraestructura de un Estado distinto del que recibe la solicitud, **se insta a los Estados a los que se les pide ayuda que proporcionen cualquier ayuda o apoyo posible para minimizar las consecuencias no deseadas de la operación cibernética maliciosa contra la infraestructura crítica**. Los Estados también pueden proporcionar asistencia para poner fin a la operación cibernética o para robustecer los sistemas de red informática de la infraestructura crítica afectada. La ayuda puede suministrarse de diversas formas y no se limita a la asistencia técnica. Si una operación cibernética, por ejemplo, entorpece la producción de electricidad en un Estado determinado, este puede solicitar asistencia en forma de suministro adicional de electricidad. Cuando se solicita asistencia, se espera que el Estado afectado por la operación cibernética estipule las necesidades o especifique la solicitud, incluyendo el alcance y los métodos de asistencia. Es importante que los Estados involucrados en dicha interacción y cooperación se comuniquen y actúen de buena fe y dentro de los límites del principio jurídico internacional de soberanía y de las obligaciones resultantes.

76 Véase, por ejemplo, UIT et al. (2018, 44).
77 AGNU (2015b, párr. 13(h)).

En segundo lugar, si la solicitud se realiza al Estado del cual se cree que procede la operación cibernética maliciosa (el Estado de emanación), ese Estado debe responder intentando mitigar la operación cibernética en sí misma. La mitigación, en comparación con la asistencia, parece ser un concepto más restringido y se refiere al acto de limitar[78] la operación cibernética contra la infraestructura crítica. Como tal, la mitigación usualmente está reservada a acciones de naturaleza técnica y relacionadas con la operación cibernética en sí misma. **En este contexto, se espera que los Estados de emanación adopten medidas razonables para poner fin o minimizar la propagación del código malicioso subyacente**. Aunque su alcance sea más restringido que la asistencia, la mitigación señala el importante papel que desempeñan los Estados de emanación en la limitación de la propagación de la operación cibernética y los daños resultantes. Mitigación y asistencia no son mutuamente excluyentes; un Estado al que se le pide mitigar una operación cibernética que se origina en su territorio también podría estar prestando asistencia.

Dicho esto, la norma no tiene en cuenta el papel de los Estados de tránsito, cuya infraestructura puede ser un importante eslabón habilitante en la cadena de la operación maliciosa y que, por lo tanto, potencialmente también podría estar en condiciones de mitigar la operación cibernética contra la infraestructura crítica de otro Estado. La comunidad internacional podría ahondar en el análisis del papel de los Estados de tránsito a la vez que continúa avanzando en los debates sobre las normas de comportamiento responsable de los Estados en foros multilaterales.

En tercer lugar, los esfuerzos de asistencia y mitigación no deben estar centrados en la cuestión de atribución técnica. En la respuesta inmediata a una operación cibernética contra infraestructura crítica, las actividades destinadas a descubrir al culpable solo deben llevarse a cabo en la medida en que limiten los daños de la operación cibernética en curso. Esto no significa que los actores que se hayan unido a esta respuesta colaborativa deban descuidar cualquier evidencia digital encontrada durante la fase de resolución de incidentes; dichas pruebas podrían resultar útiles en una etapa posterior y permitirles tomar medidas de conformidad con el derecho penal nacional o el derecho internacional de responsabilidad del Estado. No obstante, la atribución no debe convertirse de ninguna manera en el esfuerzo central de las partes cooperantes, ya que puede descarriarlas del objetivo principal de la cooperación: detener la propagación de la operación cibernética y minimizar sus consecuencias no deseadas.

78 CIJ (1997, párr. 80).



Conclusión

Para minimizar el impacto de las amenazas a la infraestructura crítica, la comunidad internacional busca promover la paz y la seguridad por medio de normas voluntarias de comportamiento estatal responsable en el ciberespacio. En 2015, la Asamblea General de las Naciones Unidas adoptó un conjunto de normas elaboradas por el GEG, promoviendo, entre otras cosas, la cooperación entre los Estados en el caso de una operación cibernética disruptiva contra la infraestructura crítica, afirmando que los Estados deben responder a las solicitudes de asistencia apropiadas o, en algunos casos, de mitigación de otro Estado cuya infraestructura crítica esté expuesta a actos de TIC maliciosos.

Para facilitar y apoyar a los Estados en la implementación de esa norma, este informe explica su alcance y contenido, aclarando las expectativas de la normativa, la práctica de los Estados y las buenas prácticas emergentes relacionadas con la norma. Específicamente, el informe sugiere que los Estados:

- Definan la infraestructura crítica, incluidos sus (sub)sectores y una base de datos de activos que califiquen como tal.
- Establezcan mecanismos nacionales de resolución de crisis de múltiples partes interesadas.
- Compartan información sobre la conceptualización de la infraestructura crítica con la comunidad internacional.
- Intenten establecer una red global de puntos de contacto.
- Realicen periódicamente ejercicios (inter)nacionales de ciberseguridad.
- Sigan las buenas prácticas relacionadas con la comunicación al enviar o responder a una solicitud de asistencia o mitigación.
- Hagan todo lo posible para prestar asistencia al Estado afectado en la forma solicitada y, si se los identifica como Estado de emanación de una operación cibernética maliciosa, que hagan todo lo posible para mitigar la operación en sí.

Sin embargo, varios aspectos de la norma quedan aún por desarrollar por la comunidad internacional. En consecuencia, los Estados deben seguir intercambiando puntos de vista sobre la puesta en práctica de la norma, o proporcionando niveles adicionales de entendimiento por medio de buenas prácticas y compartiendo sus experiencias con la implementación de la norma.

Además, al reflexionar sobre la implementación del actual marco normativo, la comunidad internacional debería considerar la posibilidad de explorar el papel de los Estados de tránsito, prestando especial atención a su potencial para contribuir en los esfuerzos de mitigación en caso de que se produzca una operación cibernética contra la infraestructura crítica.

La comunidad internacional también debería considerar la posibilidad de elaborar el concepto de infraestructura crítica internacional o transnacional y definir las expectativas hacia los distintos Estados para mitigar las operaciones cibernéticas maliciosas dirigidas a dicha infraestructura.

Por último, la comunidad internacional debería considerar cómo aprovechar los esfuerzos actuales y futuros de creación de capacidades,[79] a fin de fortalecer las competencias nacionales de cada Estado, habilitándolos a proteger su propia infraestructura y a mitigar operaciones cibernéticas maliciosa dirigidas a la infraestructura crítica de otro Estado, o a ayudar a un Estado necesitado.

79 AGNU (2015b, párr. 23).

Referencias

Unión Africana. 2014. Convención sobre Ciberseguridad y Protección de Datos Personales. 27 de junio.

Anderson, Brooke G. y Michelle L. Bell. 2012. 'Lights Out: Impact of the August 2003 Power Outage on Mortality in New York, NY' [Luces Apagadas: Impacto del Corte Eléctrico de 2003 en la Mortalidad en el Mes de Agosto en Nueva York, NY] *Epidemiology*, 23 (2): 189–193. Disponible en: https://journals.lww.com/epidem/Fulltext/2012/03000/Lights_Out___Impact_of_the_August_2003_Power.3.aspx

Axelrod, Robert. 1984. *The Evolution of Cooperation* [La Evolución de la Cooperación]. Nueva York: Basic Books.

Baker, Thar, Muhammad Asim, Áine MacDermott, Farkhund Iqbal, Faouzi Kamoun, Babar Shah, Omar Alfandi y Mohammad Hammoudeh. 2020. 'A Secure Fog-Based Platform for SCADA- Based IoT Critical Infrastructure' [Una Plataforma Segura Basada en Niebla para la Infraestructura Crítica de IoT Basada en SCADA]. *Número especial: Software Tools and Techniques for Fog and Edge Computing* [Herramientas y Técnicas de Software para la Computación de Niebla y Borde] 50 (5): 503. Disponible en: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.2688

BBC. 2017. 'NHS "Could Have Prevented" WannaCry Ransomware Attack.' [El Servicio Nacional de Salud "Podría Haber Evitado" el Ataque de Ransomware de WannaCry] BBC News, 27 de octubre. Disponible en: https://www.bbc.com/news/technology-41753022

Bhunia, Swarup y Mark Tehranipoor. 2019. *Hardware Security: A Hands-on Learning Approach* [Seguridad de Hardware. Un Enfoque Práctico de Aprendizaje]. Cambridge: Elsevier.

Burgstaller, Markus. 2005. *Theories of Compliance with International Law* [Teorías de Cumplimiento con Derecho Internacional]. Leiden: Brill Academic.

Cimpanu, Catalin. 2020. 'Two More Cyber-Attacks Hit Israel's Water System' [Dos Ciberataques Más Golpean el Sistema Hídrico de Israel]. ZDNet, 20 de julio. Disponible en: https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system

Consejo de Europa (CdE). 2004. Convención sobre el Delito Cibernético, ETS 185.

Consejo de la Unión Europea. 2008. *Directiva 2008/114/CE del Consejo del 8 de diciembre de 2008 Relativa a la Identificación y Designación de las Infraestructuras Críticas Europeas y la Evaluación de la Necesidad de Mejorar su Protección*.

———. 2017. *The Manual on Law Enforcement Information Exchange* [Manual Sobre Intercambio de Información en la Aplicación de la Ley) 6261/17, 4 de julio. Disponible en: https://data.consilium.europa.eu/doc/document/ST-6261-2017-INIT/en/pdf

Downs, George W. y Michael A. Jones. 2002. 'Reputation, Compliance, and International Law' [Reputación, Cumplimiento y Derecho internacional]. *Journal of Legal Studies* 31 (S1): S96.

Edison Electric Institute. 2018. 'Electric Distribution System Cybersecurity Is Critical in Today's Interconnected Society' [La Ciberseguridad del Sistema de Distribución Eléctrico es Fundamental en la Sociedad Interconectada Actual] Abril. Disponible en: https://www.eei.org/issuesandpolicy/Documents/EEI_Cybersecurity_Considerations_Distribution.pdf

Comisión Europea (CE). 2020. 'List of SPOCS & Competent authorities – NIS Directive' [Lista de SPOCS y Autoridades Competentes — Directiva NIS]. Disponible en: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53682

Unión Europea (UE). 2016. *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, del 6 de julio de 2016, relativa a las medidas para un nivel de seguridad común alto de las redes y los sistemas de información en toda la Unión*.

Agencia de la Unión Europea para la Ciberseguridad (ENISA). 2009. 'Good Practices on Reporting Security Incidents' [Buenas Prácticas para Informes de Incidentes de Seguridad]. Diciembre. Disponible en: https://www.enisa.europa.eu/publications/good-practice-guide-on-incident-reporting-1/at_download/fullReport

———. 2019. *ENISA Threat Landscape Report 2018* [Informe de ENISA sobre el Panorama de Amenazas 2018]. Atenas: ENISA. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

———. 2020a. 'Critical Infrastructures and Services' [Infraestructuras y Servicios Críticos]. Disponible en: https://www. enisa.europa.eu/topics/critical-information-infrastructures-and-services?tab=publications

———. 2020b. *Sectoral/Thematic Threat Analysis: ENISA Threat Landscape* [Análisis de Amenazas Sectoriales/Temáticas: Panorama de Amenazas ENISA]. Atenas: ENISA. Disponible en: https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis

———. 2020c. *The Year in Review: ENISA Threat Landscape* [Revisión del Año: Panorama de amenazas ENISA]. Atenas: ENISA. Disponible en: https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport

Ministerio Federal del Interior, Alemania. 2009. *National Strategy for Critical Infrastructure Protection (CIP Strategy)* [Estrategia Nacional de Protección de Infraestructuras Críticas (Estrategia PIC)]. Berlín: Gobierno de Alemania. Disponible en: https://www.bmi. bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.html

Oficina Federal de Protección Civil, Suiza. 2020. 'Critical Infrastructures' [Infraestructuras Críticas]. Disponible en: https://www.babs.admin.ch/en/aufgabenbabs/ski/kritisch.html

Foro de Equipos de Seguridad y Respuesta ante Incidentes (FIRST). 2019. 'Information Exchange Policy 2.0 Framework Definition' [Definición del Marco de la Política de iIntercambio de Información 2.0]. Disponible en: https://www.first.org/iep/iep_framework_2_0

———. 2020. 'Traffic Light Protocol (TLP): FIRST Standards Definitions and Usage Guidance – Version 1.0.' [Protocolo de Semáforo (TLP): Definiciones de Estándares FIRST y Orientación para su Uso – Versión 1.0). Disponible en: https://www.first.org/tlp

G-20. 2017. 'Communiqué – G20 Finance Ministers and Central Bank Governors Meeting' [Comunicado – Reunión de Ministros de Finanzas y Gobernadores de Bancos Centrales del G20]. Baden-Baden, Alemania, 17 y 18 de marzo de 2017.

G-7. 2019. 'Cyber Norm Initiative Synthesis of Lessons Learned and Best Practices' [Síntesis de Lecciones Aprendidas y Mejores Prácticas de la Iniciativa de Normas Cibernéticas). 26 de agosto. Disponible en: https://www.diplomatie.gouv.fr/IMG/pdf/_eng_synthesis_cyber_norm_initiative_cle44136e.pdf

Gallagher, Ryan. 2020. 'Hackers "Without Conscience" Demand Ransom from Dozens of Hospitals and Labs Working on Coronavirus' [Los Piratas Informáticos "Sin Conciencia" Exigen Rescate de Docenas de Hospitales y Laboratorios que Trabajan en el Coronavirus] *Fortune*, 1 de abril. Disponible en: https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus

Gavrilović, Andrijana. 2020. 'Confidence-Building Measures' [Medidas de Fomento de la Confianza]. Geneva Internet Platform, febrero de 2020. Disponible en: https://dig.watch/events/open-ended-working-group-oewg-second-substantive-session/confidence-building-measures

Ghafur, Saira S. Kristensen, K. Honeyford, G. Martin, A. Darzi y P. Aylin. 2019. 'A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS' [Un Análisis Retrospectivo del Impacto del Ciberataque de WannaCry en el Servicio Nacional de Salud] *NPJ Digital Medicine* 98 (2).

Gisel, Laurent y Lukasz Olejnik. 2019. *The Potential Human Cost of Cyber Operations* [El Potencial Costo Humano de las Operaciones Cibernéticas]. Ginebra: Comité Internacional de la Cruz Roja. Disponible en: https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf

Comisión Global sobre la Estabilidad del Ciberespacio. 2019. *Advancing Cyberstability* [Promoviendo la Ciberestabilidad]. Informe final, noviembre. Disponible en: https://cyberstability.org/wp-content/ uploads/2020/02/GCSC-Advancing-Cyberstability.pdf

Centro Global de Capacidad de Seguridad Cibernética. 2016. *Cybersecurity Capacity Maturity Model for Nations (CMM)* [Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM)] – Edición Revisada. Oxford: Universidad de Oxford. Disponible en: https://gcscc.ox.ac.uk/files/cmmrevisededition090220171pdf

Gobierno de Australia. 2019. 'Australian Implementation of Norms of Responsible State Behaviour in Cyberspace' [Implementación Australiana de Normas de Comportamiento Estatal Responsable en el Ciberespacio]. Disponible en: https://www.dfat.gov.au/sites/default/files/ how-australia-implements-the-ungge-norms.pdf

Gobierno de Canadá. 2019. 'Canada's Implementation of the 2015 GGE Norms' [Implementación por Parte de Canadá de las Normas del GEG de 2015]. Disponible en: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/canada- implementation-2015-gge-norms-nov-16-en.pdf

Gobierno de los Países Bajos. 2017. 'Building Digital Bridges: International Cyber Strategy' [Construyendo Puentes Digitales: Estrategia Cibernética Internacional]. 2 de febrero. Disponible en: https://www.government.nl/documents/ parliamentary-documents/2017/02/12/international-cyber-strategy

———. 2020. 'The Netherlands' Position Paper on the UN Open-ended Working Group "on Developments in the Field of Information and Telecommunications in the Context of International Security" and the UN Group of Governmental Experts "on Advancing responsible State behavior in cyberspace in the context of international security."' [Documento de Posición de 'Los Países Bajos' sobre el Grupo de Trabajo de Composición Abierta de las Naciones Unidas "sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional" y el Grupo de Expertos Gubernamentales de las Naciones Unidas "sobre la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional"]. Febrero. Disponible en: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg- kingdom-of-the-netherlands.pdf

Gusev, Alexey. 2020. 'New Cyberattacks Vectors of Russian Critical Infrastructure Enterprises: Domestic Private Banking Sector View within AI Protection Methods' [Nuevos Vectores de Ciberataques de Empresas Rusas de Infraestructura Crítica: Vista del Sector Bancario Privado Nacional dentro de los Métodos de Protección de Inteligencia Artificial]. *Procedia Computer Science* 169: 314. Disponible en: https://www.sciencedirect.com/science/article/pii/S1877050920303124

Guzman, Andrew T. 2002. 'A Compliance Based Theory of International Law' [Una Teoría del Derecho Internacional Basada en el Cumplimiento]. *California Law Review* 90(6): 1823. Disponible en: https://digitalcommons.law.uga.edu/cgi/viewcon tent.cgi?article=1216&context=gjicl

Herzog, Stephen. 2011. 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses' [Repasando los Ciberataques en Estonia: Amenazas Digitales y Respuestas Multinacionales] *Journal of Strategic Security* 4(2): 49.

Servicios de Inteligencia y Respuesta ante Incidentes de IBM X-Force. 2020. 'X-Force Threat Intelligence Index 2020' [Índice de Inteligencia de Amenazas X-Force 2020]. Febrero. Disponible en: https://www.ibm.com/security/digital-assets/xforce-threat-intelligence-index-map/#

Ilves, Thomas Hendrik. 2007. 'Discurso de Toomas Hendrik Ilves, Presidente de la República de Estonia, ante el 62º período de sesiones de la Asamblea General de las Naciones Unidas (25 de septiembre de 2007)'. Disponible en: https://www.un.org/webcast/ga/62/2007/pdfs/estonia-eng.pdf

Comité Interamericano contra el Terrorismo (CICTE). 2015. *Declaration: Protection of Critical Infrastructure from Emerging Threats* [Declaración: Protección de la Infraestructura Crítica Frente a Amenazas Emergentes]. Documento CICTE CICTE/doc.1/15, 23 de marzo de 2015. Disponible: https://www.oas.org/en/sms/cicte/documents/sessions/2015/CICTE%20DOC%201%20DECLARATION%20CICTE00955E04.pdf

Corte Internacional de Justicia (CIJ). 1997. *Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, ICJ Reports 1997* [Proyecto Gabčíkovo-Nagymaros (Hungría/Eslovaquia), Sentencia, Informes de la Corte Internacional de Justicia 1997], p. 7.

Unión Internacional de Telecomunicaciones (UIT). 2010. *Question 22-1: Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity* [Pregunta 22-1: Protección de las Redes de Información y Comunicación: Prácticas Recomendadas para Desarrollar una Cultura de Ciberseguridad] (informe final). Ginebra: UIT. Disponible en: https://www.itu.int/pub/D-STG-SG01.22-2010

———. 2020. 'National Cybersecurity Strategies Repository' [Repositorio de Estrategias Nacionales de Ciberseguridad]. Disponible en: https:// www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

———. 2021. 'CyberDrills' [Cibersimulacros]. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/ Pages/cyberdrills.aspx

Unión Internacional de Telecomunicaciones (UIT), Banco Mundial, Secretaría del Commonwealth, Organización de Telecomunicaciones del Commonwealth, Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN. 2018. *Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity* [Guía para Desarrollar una Estrategia Nacional de Ciberseguridad: Participación Estratégica en la Ciberseguridad]. Ginebra: UIT.

INTERPOL. 2020. 'Preventing Crime and Protecting Police: INTERPOL's COVID-19 Global Threat Assessment' [Prevención de la Delincuencia y Protección de la Policía: Evaluación Mundial de Amenazas COVID-19 de INTERPOL]. 6 de abril. Disponible en: https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment

CERT de Kaspersky ICS. 2020a. 'Cyberthreats for ICS in Energy in Europe. Q1 2020' [Ciberamenazas para ICS en Energía en Europa. 1° TRIMESTRE DE 2020]. Disponible en: https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-2020Q1-Threats- to-energy-industry-in-Europe.pdf

———. 2020b. 'Threat Landscape for Industrial Automation Systems H1 2020' [Panorama de Amenazas para los Sistemas de Automatización Industrial en el Primer Semestre de 2020]. 24 de septiembre. Disponible en: https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

———. 2021. 'Threat Landscape for Industrial Automation Systems. Statistics for H2 2020' [Panorama de Amenazas para los Sistemas de Automatización Industrial. Estadística para el Segundo Semestre de 2020]. 25 de marzo. Disponible en: https://securelist.com/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2020/101299

———. Próximamente. 'Threat Landscape for ICS in Water Management Industry' [Panorama de Amenazas para ICS en la Industria de Gestión del Agua].

Khalili, Joel. 2020. 'Coronavirus Hospital Suspends Activity over Cyberattack' [El Hospital de Coronavirus Suspende la Actividad por Ciberataque] *Techradar.Pro*, 16 de marzo. Disponible en: https://www.techradar.com/news/coronavirus-hospital-suspends-activity-over-cyberattack

Lauber, Jurg. 2019. 'Chair's Summary: Informal Consultative Meeting of the Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' [Resumen del Presidente: Reunión Consultiva Informal del Grupo de Expertos Gubernamentales (GEG) sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional]. Del 5 al 6 de diciembre. Disponible en: https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meet- ing-5-6-dec-20191.pdf

Lee, Robert M., Michael J. Assante y Tim Conway. 2016. 'Analysis of the Cyber Attack on the Ukrainian Power Grid' [Análisis del Ciberataque a la Red Eléctrica Ucraniana]. *SANS & E-ISAC*, 18 de marzo. Disponible en: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Maglaras, Leandros A., Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras y Tiago J. Cruz. 2018. 'Cyber Security of Critical Infrastructures' [Seguridad Cibernética de las Infraestructuras Críticas]. *ICT Express* 4: 42–45.

Microsoft. 2020. 'Microsoft Digital Defense Report' [Informe de Defensa Digital de Microsoft]. Septiembre. Disponible en: https://www.microsoft.com/en-us/download/details.aspx?id=101738

Ministerio de Europa y Asuntos Exteriores, Francia. 2018. 'Paris Call for Trust & Security in Cyberspace' [Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio]. 11 de diciembre. Disponible en: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf

Morse, Amyas. 2017. *Investigation: WannaCry Cyber Attack and the NHS* [Investigación: Ciberataque de WannaCry y el Servicio Nacional de Salud]. Londres: Oficina Nacional de Auditoría. Disponible en: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs

Muthuppalaniappan, Menaka y Kerrie Stevenson. 2020. 'Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health' [Ciberataques Sanitarios y Pandemia de COVID-19: una Amenaza Urgente para la Salud Global] *International Journal for Quality in Health Care* 33 (1). Disponible en: https://academic.oup.com/intqhc/advance-article/doi/10.1093/intqhc/mzaa117/5912483

Nebenzia, Vassily. 2020. 'Statement by Vassily Nebenzia, Permanent Representative of the Russian Federation to the United Nations, at the "Arria-formula" VTC of the UNSC Members on Cyber-Attacks against Critical Infrastructure' [Declaración de Vassily Nebenzia, Representante Permanente de la Federación Rusa ante las Naciones Unidas, Videoconferencia sobre "Fórmula Arria" de los Miembros del CSNU sobre Ataques Cibernéticos contra Infraestructuras Críticas]. Misión Permanente de la Federación Rusa ante las Naciones Unidas, 26 de agosto. Disponible en: https://russiaun.ru/en/news/ arria_260820

Grupo de Trabajo de Composición Abierta (GTCA) sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. 2020. 'Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security' [Segundo "pre-borrador" del informe del GTCA sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional]. 27 de mayo. Disponible en: https://front.un-arm.org/wp-content/ uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

———. 2021. 'Final Substantive Report' [Informe Sustantivo Final]. 10 de marzo de 2021, documento de las Naciones Unidas A/AC.290/2021/ CRP.2. Disponible en: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Organización de Cooperación y Desarrollo Económicos (OCDE). 2008a. 'Protection of "Critical Infrastructure" and the Role of Investment Policies Relating to National Security' [Protección de la "Infraestructura Crítica" y el Rol de las Políticas de Inversión Relacionadas con la Seguridad Nacional]. Mayo. Disponible en: https://www.oecd.org/daf/inv/investment-policy/40700392.pdf

———. 2008b. *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures* [Recomendación de la OCDE del Consejo sobre la Protección de las Infraestructuras de Información Críticas]. Documento C (2008) de la OCDE 35. París: OCDE. Disponible en: http://www.oecd.org/sti/40825404.pdf

Consejo Permanente de la Organización para la Seguridad y la Cooperación en Europa (OSCE). 2013. 'Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' [Decisión N.° 1106: Conjunto Inicial de Medidas de Fomento de la Confianza de la OSCE para Reducir los Riesgos de Conflictos Derivados del Uso de Tecnologías de la Información y la Comunicación]. Documento PC.DEC/1106 de la OSCE, de 3 de diciembre de 2013.

———. 2018. 'OSCE Holds National Table Top Exercise in Kazakhstan on Protecting Critical Energy Infrastructure from Cyber-Related Terrorist Attacks' [La OSCE Lleva a Cabo un Ejercicio Nacional Teórico en Kazajstán sobre la Protección de la Infraestructura Energética Crítica de Ataques Terroristas Relacionados con Ciberataques]. 29 de noviembre. Disponible en: https://www.osce.org/programme-office-in-astana/404594

Organización de los Estados Americanos (OEA). 2021. 'Cybersecurity Program' [Programa de Ciberseguridad]. Disponible en: http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

Misión Permanente de la República de Indonesia ante las Naciones Unidas, Nueva York. 2020. 'Statement by H.E. Ambassador Dian Triansyah Djani Permanent Representative of the Republic of Indonesia: United Nations Security Council Arria-formula Meeting "Cyber Stability, Conflict Prevention, and Capacity Building' [Declaración de S.E. Embajador Dian Triansyah Djani Representante Permanente de la República de Indonesia: Reunión de Fórmula Arria del Consejo de Seguridad de las Naciones Unidas "Ciberestabilidad, Prevención de Conflictos y Creación de Capacidades]. Nueva York, 22 de mayo. Disponible en: https://kemlu.go.id/new-york-un/en/read/united-nations-security-council-arria-formula-meeting-cyber-stability-conflict-prevention-and-capacity-building/3645/etc-menu

Consejo Consultivo Nacional de Infraestructura (CCNI) del Presidente. 2017. 'Security Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure' [Activos Cibernéticos de Seguridad: Abordar las Amenazas Cibernéticas Urgentes para la Infraestructura Crítica]. Agosto. Disponible en: https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

República de Mauricio. 2014. 'National Cyber Security Strategy 2014 – 2019' [Estrategia Nacional de Ciberseguridad 2014 – 2019]. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Mauritius_2014_National%20Cyber%20Security%20Strategy%20-%202014%20-%20EN.pdf

Schmidthaler, Michael y Johannes Reichl. 2016. 'Assessing the Socio-Economic Effects of Power Outages Ad Hoc' [Evaluación Ad Hoc de los Efectos Socioeconómicos de los Cortes de Energía] Informática – Investigación y desarrollo 3131: 157–61. Disponible en: https://link.springer.com/article/10.1007/s00450-014-0281-9

Security Magazine. 2020. 'Critical Infrastructure Cyberattacks a Greater Concern Than Enterprise Data Breaches' [Los Ciberataques de Infraestructura Crítica Son más Preocupantes que las Violaciones de Datos Empresariales] *Security Magazine*, 26 de marzo. Disponible en: https://www.securitymagazine.com/articles/91992-critical-infrastructure-cyberattacks-a-greater-concern-than-enterprise-data-breaches

Organización de Cooperación de Shanghai. 2009. 'Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization' [Acuerdo de cooperación para garantizar la seguridad de la información internacional entre los Estados miembros de la Organización de Cooperación de Shanghái]. 16 de junio. Disponible en: http://eng.sectsco.org/load/207508

Shea, Dana A. 2004. 'Critical Infrastructure: Control Systems and the Terrorist Threat' [Infraestructura Crítica: los Sistemas de Control y la Amenaza Terrorista]. Informe CRS para el Congreso, RL31534, 20 de enero. Disponible en: https://apps.dtic.mil/sti/ pdfs/ADA467307.pdf

Shuaia, Mao, Wang Chengzhib, Yu Shiwena, Gen Haoa, Yu Jufanga y Hou Hui. 2018. 'Review on Economic Loss Assessment of Power Outages' [Revisión de la Evaluación de la Pérdida Económica de los Cortes de Energía]. *Procedia Computer Science* 130: 1158–63. Disponible en: https://www.sciencedirect.com/science/article/pii/S1877050918305131

Siemens Gas & Power. 2019. *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?* [Atrapado en el Punto de Mira: ¿Siguen las Empresas de Servicios Públicos el Ritmo de la Ciberamenaza Industrial?] Houston: Siemens. A 21 de octubre de 2020: https://assets.siemens-energy.com/siemens/assets/api/uuid:c723efb9-847f-4a33-9afa-8a097d81ae19/siemens-cybersecurity.pdf

Smith, Scott, Fabiola Sánchez y Christopher Torchia. 2019. 'Venezuela Buckles under Massive Power, Communications Outage' [Venezuela se Doblega Bajo un Corte Eléctrico y de las Comunicaciones]. *Associated Press*, 9 de marzo. Disponible en: https://apnews.com/6ba2f69b77e2457da64593a7b8eced16

Statt, Nick. 2021. 'Hackers Tampered with a Water Treatment Facility in Florida by Changing Chemical Levels' [Los Piratas Informáticos Manipularon una Instalación de Tratamiento de Agua en Florida al Cambiar los Niveles Químicos]. The Verge, 8 de febrero. Disponible en: https://www.theverge.com/2021/2/8/22273170/hackers-water-treatment-facility-florida-hacked-chemical-levels-changed

Steffen, Sarah. 2016. 'Hackers Hold German Hospital Data Hostage' [Los hackers tienen como rehenes de datos hospitalarios alemanes]. DW, 25 de febrero. Disponible en: https://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030

Suter, Manuel. 2007. *A Generic National Framework for Critical Information Infrastructure Protection (CIIP)* [Marco nacional genérico para la protección de la infraestructura de información crítica (CIIP)]. Zúrich: Centro de Estudios de Seguridad. Disponible en: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

Conferencia de las Naciones Unidas sobre Organización Internacional. 1945. *Charter of the United Nations and Statute of the International Court of Justice* [Carta de las Naciones Unidas y Estatuto de la Corte Internacional de Justicia]. San Francisco, 26 de junio.

Dirección Ejecutiva del Comité de las Naciones Unidas contra el Terrorismo (UNCTED) y Oficina de las Naciones Unidas Contra el Terrorismo (OLCT). 2018. *The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices* [La protección de las infraestructuras críticas contra los ataques terroristas: Compendio de buenas prácticas]. Junio. Disponible en: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

Asamblea General de las Naciones Unidas (AGNU). 1970. *Declaration on principles of international law concerning friendly relations and co-operation among States in accordance with the Charter of the United Nation* [Declaración sobre los principios del derecho internacional relativos a las relaciones amistosas y la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas]. Documento de las Naciones Unidas A/PV.1883, 24 de octubre de 1970.

———. 1999. *Review of the implementations of the recommendations and decisions adopted by the General Assembly at its tenth special session: Report of the Disarmament Commission* [Examen de la aplicación de las recomendaciones y decisiones adoptadas por la Asamblea General en su décimo período extraordinario de sesiones: Informe de la Comisión de Desarme]. Documento de las Naciones Unidas A/51/182/Rev.1, 9 de junio de 1999. Disponible en: https://www.un.org/disarmament/wp-content/uploads/2019/09/A-51-182-Rev.1-E.pdf#page=53

———. 2001. *Responsibility of States for internationally wrongful acts* [Responsabilidad del Estado por hechos internacionalmente ilícitos]. Documento de las Naciones Unidas A/ RES/56/83, 28 de enero de 2001.

———. 2010. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* [Grupo de Expertos Gubernamentales sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional]. Documento A/65/201 de las Naciones Unidas, 10 de julio de 2010.

———. 2015a. *Developments in the field of information and telecommunications in the context of international security* [Avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional]. Documento de las Naciones Unidas A/RES/70/237, de 23 de diciembre de 2015.

———. 2015b. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* [Grupo de Expertos Gubernamentales Sobre los Avances en el Ámbito de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional]. Documento de las Naciones Unidas A/70/174, 22 de julio de 2015.

Consejo de Seguridad de las Naciones Unidas (CSNU). 2017. Documento de las Naciones Unidas S/RES/2341 (2017), 13 de febrero de 2017.

Equipo de Preparación para Emergencias Informáticas de los Estados Unidos (US-CERT). 2015. 'US-CERT Federal Incident Notification Guidelines' [Pautas de Notificación de Incidentes Federales del CERT de EE. UU). Disponible en: https://us-cert.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines_2015.pdf

Agencia de Seguridad Cibernética e Infraestructura de los Estados Unidos (CISA). 2020a. 'Alert (AA20-049A) Ransomware Impacting Pipeline Operations' [Alerta (AA20- 049A) de Ransomware que Impacta las Operaciones de Canalización]. Departamento de Seguridad Nacional, 18 de febrero. Disponible en: https://us-cert.cisa.gov/ncas/alerts/aa20-049a

———. 2020b. 'Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response' [Orientación Sobre el Personal de Infraestructura Crítica Esencial: Grantizar la Resiliencia Comunitaria y Nacional en la Respuesta al COVID-19]. Versión 4.0, 18 de agosto. Disponible en: https://www.cisa.gov/sites/default/files/publications/ECIW_4.0_Guidance_on_Essential_Critical_Infrastructure_Workers_Final3_508_0.pdf

Departamento de Energía de los Estados Unidos (DOE). 2019. *Evaluation Report* [Informe de Evaluación]. DOE-OIG-20-12, 19 de noviembre. Washington, DC: DOE de EE. UU. Disponible en: https://www.energy.gov/sites/prod/files/2019/11/f68/DOE-OIG-20-12.pdf

Departamento de Seguridad Nacional de los Estados Unidos. 2020. 'National Infrastructure Protection Plan International Issues for CI/KR Protection' [Plan Nacional de Protección de Infraestructura, Cuestiones Internacionales para la Protección de la CI/KR]. Disponible en: https://www.dhs.gov/xlibrary/assets/nipp_international.pdf

Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST). 2012. Guía de Manejo de Incidentes de Seguridad Informática: Recomendaciones del Instituto Nacional de Normas y Tecnología. Publicación especial 800-61, revisión 2. Gaithersburg: NIST DE EE. UU. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Van der Vleuten, Erik y Vincent Lagendijk. 2010. 'Transnational Infrastructure Vulnerability: The Historical Shaping of the 2006 European "Blackout"' [Vulnerabilidad de Infraestructura Transnacional: La Configuración Histórica del "Apagón" Europeo de 2006]. *Enery Policy* 38 (4): 2042–2052.

Vidyarthi, Apratim y Anastasiya Kazakova. 2020. 'What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance' [Lo que la Formulación de Políticas de Ciberseguridad Puede Aprender de los Principios Normativos en la gobernanza global]. Documento de antecedentes, *Foro de Mejores Prácticas del IGF 2020 sobre Ciberseguridad*, septiembre de 2020.



Cooperación internacional para mitigar las operaciones cibernéticas contra la infraestructura crítica

Expectativas normativas y buenas prácticas emergentes

Las operaciones cibernéticas maliciosas suponen una amenaza para las infraestructuras críticas y, por lo tanto, para el bienestar de nuestras sociedades. Los incidentes graves tienen el potencial de desestabilizar Estados y poner en peligro la paz y la seguridad internacionales. Para hacer frente al riesgo de las cada vez más complejas y eficaces amenazas cibernéticas dirigidas a infraestructuras críticas, la comunidad internacional busca promover la cooperación haciendo uso de las normas de comportamiento esperado de los Estados en el ciberespacio. Este informe investiga la norma—como fue propuesta en 2015 por el Grupo de Expertos Gubernamentales de la Organización de las Naciones Unidas sobre los avances en información y las telecomunicaciones en el contexto de la seguridad internacional—que insta a los Estados a responder a las solicitudes internacionales de asistencia o mitigación frente a operaciones cibernéticas maliciosas contra infraestructuras críticas

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH