# Las Amenazas Cibernéticas

El alcance y la gravedad de las amenazas cibernéticas globales y la forma en que respondemos a ella tendrá consecuencias de largo alcance para el futuro de Internet.

## Introducción

"Los ataques contra empresas y países llegan a los titulares con tanta frecuencia que ya no nos impresiona el volumen ni la velocidad con que se aceleran las amenazas cibernéticas".[1] Sin embargo, a medida que aumenta nuestra dependencia de Internet, el alcance y la gravedad de los desafíos y vulnerabilidades de seguridad se intensificarán cada vez más. La ciberseguridad será el desafío más imperativo en la próxima década. Hasta el momento, las respuestas han sido completamente insuficientes y los costos están aumentando.

Los ataques y delitos cibernéticos darán forma a Internet y a nuestra relación con la misma. Una inadecuada gestión de las amenazas cibernéticas aumentará los riesgos a los que se enfrentan los usuarios, socavará la confianza en Internet y pondrá en peligro su capacidad para actuar como motor de innovación económica y social. Las respuestas desinformadas o desproporcionadas de los gobiernos amenazan las libertades y contribuyen a un clima de temor e incertidumbre. Cómo respondemos al aumento de los ataques y delitos cibernéticos es una pregunta fundamental: la respuesta determinará en gran medida el futuro de Internet.

**El crecimiento continuo de Internet dependerá de cómo respondamos colectivamente al volumen y la escala de las amenazas cibernéticas.**

**A medida que los gobiernos se ven sometidos a presiones para responder a las amenazas cibernéticas, existe el riesgo muy real de que las libertades en línea y la conectividad global queden en segundo plano con respecto a la seguridad nacional.**

**Se necesitan urgentemente nuevos modelos de rendición de cuentas, incentivos y responsabilidad, no solo para aumentar la preparación para la ciberseguridad y reducir las vulnerabilidades, sino también para garantizar la seguridad del usuario final.**

**La complejidad y el alcance de los ataques cibernéticos requieren que se multipliquen las respuestas promovidas por múltiples partes interesadas y basadas en la experiencia para que la economía digital prospere y que se recupere la confianza en Internet.**

[1] 2016 Norton Cyber Security Insights Report https://us.norton.com/cyber-security-insights

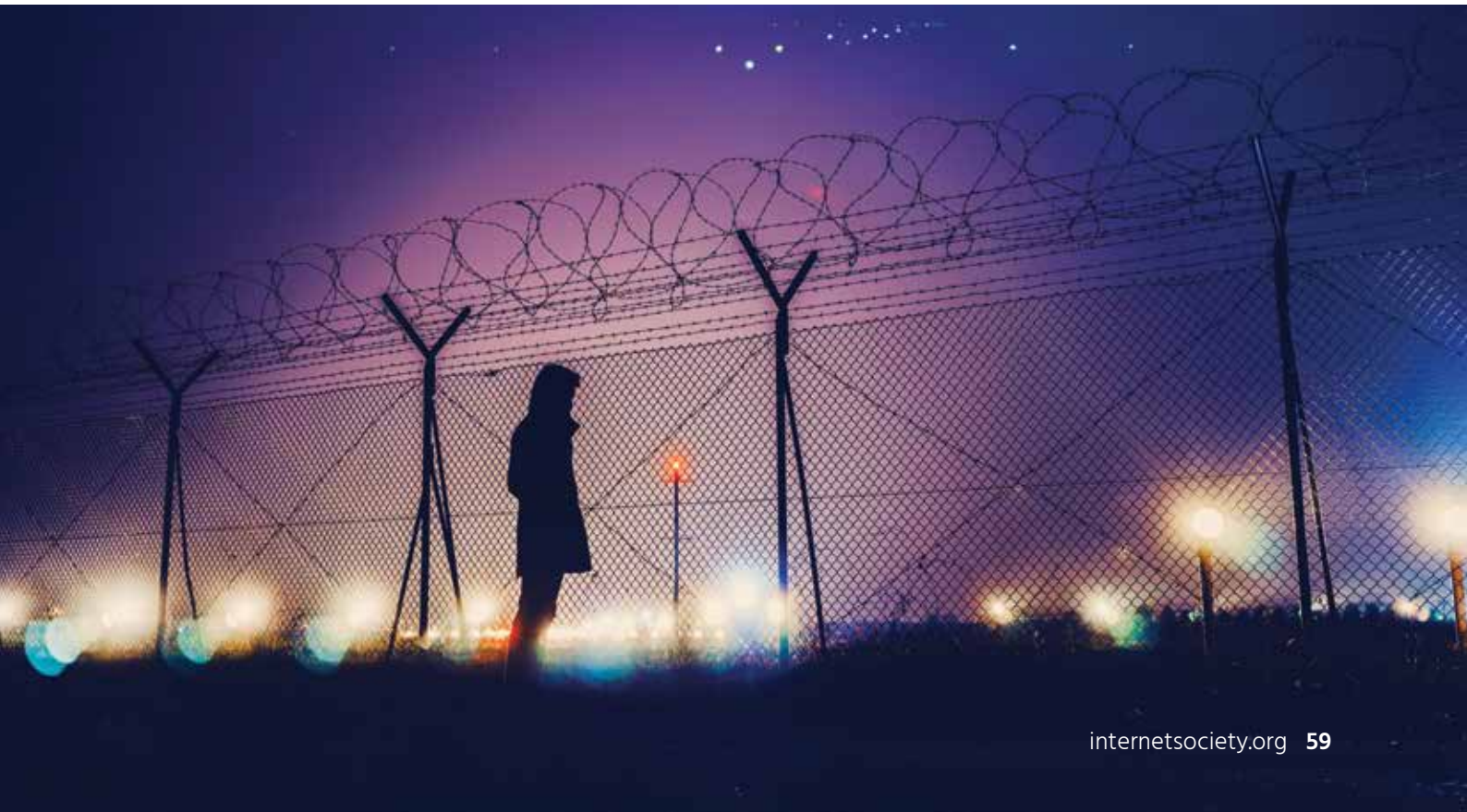
## Una creciente gama de amenazas cibernéticas

La escala de los ataques cibernéticos crece constantemente y muchos anticipan la probabilidad de ciberataques catastróficos en el futuro. Ya estamos viendo ataques a escala nacional, por lo que no es exagerado imaginar una pandemia digital con ataques que paralicen a economías enteras. Como dijo un analista de la industria norteamericana, "Se acerca el Pearl Harbor digital..."

A medida que Internet se entrelace con la seguridad nacional, el ciberdelito y las estrategias de defensa darán forma a la futura Internet tanto para la industria como para los usuarios individuales. Hoy en día se considera que el ciberespacio es el quinto dominio de la guerr[2], pero son pocas las reglas de combate acordadas.

La amenaza de un conflicto cibernético destructivo aumentará en la próxima década. Los conflictos serán iniciados no solo por los estados nacionales, sino también por sus "representantes" y por movimientos políticos independientes y actores privados. Los actos de agresión cibernéticos se sumarán a acciones de desinformación y propaganda destinadas a desestabilizar estados y economías. Los recientes ataques cibernéticos que parecen haber sido diseñados para desestabilizar un sistema político son especialmente alarmantes y apuntan a un futuro en el que socavar las estructuras de gobernanza —y por lo tanto los valores que representan— se volverán más comunes.

[2] http://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html



> “En respuesta a la creciente amenaza de ciberataques], los gobiernos están asignando mayor importancia a las cuestiones de seguridad cibernética y están reforzando la adopción de diferentes medidas de protección, entre ellas tecnología, políticas y fortalecimiento de la cooperación internacional.
>
> Tecnólogo, Asia-Pacífico

> Me preocupan los intentos de utilizar marcos regulatorios del siglo XX para abordar los problemas de Internet en el siglo XXI.
>
> Sociedad civil, América Latina y el Caribe

A medida que la red digital se entrelaza con todo lo que nos rodea —desde las luces hasta la atención de la salud pasando por los automóviles—, los usuarios son cada vez más vulnerables a los ataques cibernéticos. El enfoque que hoy se aplica para la protección de la infraestructura crítica será ineficaz en una sociedad y una economía hiperconectadas en que toda la infraestructura digital será crítica.

> Creo que los gobiernos van a contratar hackers éticos o incentivar a los hackers para que se conviertan en hackers de sombrero blanco.
>
> Miembro de ISOC, Medio Oriente

Los modelos de negocio dependerán cada vez más de las fuentes de datos y de los datos interconectados y su análisis, creando así una mayor cantidad de vectores de ataque. Si “los datos son el nuevo petróleo”[3], el creciente mercado para la piratería y el robo de datos pone en riesgo los cimientos de nuestra futura economía. Para que la Internet abierta siga siendo una plataforma para el crecimiento social y económico, los usuarios deben poder confiar en que las agencias gubernamentales y las empresas que recogen y utilizan sus datos son resilientes y abordarán adecuadamente las amenazas de seguridad cibernética.

> En este momento hay demasiados modelos de negocio que giran en torno a la recolección y la ‘minería’ de datos pero sin comprender cómo se mantendrá la seguridad de estos datos, especialmente una vez que la entidad que los recoge se estanque o se quede sin dinero. Las administraciones públicas no son una excepción y pueden llegar a ser el blanco más fácil.
>
> Tecnólogo, Europa

Perteneciente a: El papel de los gobiernos; Internet y el mundo físico; La economía de Internet

[3] http://fortune.com/2016/07/11/data-oil-brainstorm-tech/

## Respuestas inadecuadas y su impacto en la confianza

Desde el hackeo de redes para robar información personal como detalles financieros y contraseñas, hasta violaciones de la seguridad que afectan el mundo físico y ataques que afectan los procesos democráticos, el creciente alcance de los ciberataques significa que toda la sociedad está en riesgo —no solo quienes están en línea—. Las amenazas cibernéticas no socavan solo la confianza en Internet, sino también en las instituciones y los procesos políticos de los que dependen los ciudadanos.

**Si bien todas las regiones y partes interesadas creen que los beneficios de Internet seguirán superando a sus riesgos, existe una percepción general de que los riesgos están aumentando.[4]**

> “Todavía no ha habido ningún movimiento ‘Día sin Internet. La tendencia será continuar utilizando Internet a pesar de las preocupaciones con respecto a la confianza.
>
> Sector privado, Europa

Independientemente de su grupo de interés y región, todos nuestros encuestados esperan ver en el futuro gran inversión e innovación en el área de la seguridad de Internet. Esto concuerda con la opinión de Gartner Research, que pronostica que en 2017 se invertirán 92 mil millones de dólares en ciberseguridad y en 2020 más de 113 mil millones.[5] Sin embargo, si las partes interesadas no colaboran, esta inversión no estará a la altura del desafío.

> “En un mundo ideal, la seguridad digital se convertiría en la base de todo, la idea tomaría vuelo, la gente lo entendería... la seguridad para la red, los usuarios, los datos, la infraestructura, está interrelacionada y forma parte de la seguridad nacional. Quienes piensan sobre seguridad de forma más amplia y profunda lo comprenden, entienden que no se puede socavar la seguridad en un caso pequeño sin afectar el panorama general.
>
> Académico, América del Norte

Ni el gobierno ni el sector privado pueden manejar por sí solos el alcance y la escala de las amenazas cibernéticas. Dada la naturaleza interconectada de Internet, aunque necesarias, las acciones aisladas de las partes interesadas harán poco para mitigar o eliminar las amenazas cibernéticas. Impulsados por la necesidad de aparentar que “están haciendo algo” frente a ataques cibernéticos cada vez más audaces, anticipamos que las respuestas de los gobiernos a los desafíos en materia de ciberseguridad serán cada vez más reactivas. Sin embargo, tales respuestas no podrán mitigar con eficacia las amenazas y probablemente darán lugar a una regulación desproporcionada. Las acciones eficaces y el fortalecimiento de la resiliencia de las redes frente a las amenazas cibernéticas solo se logrará mediante el intercambio de información, pensamiento estratégico y esfuerzos conjuntos de las partes interesadas.

[4] Future of the Internet Survey 2 - Question 20: “To what extent do people see a tradeoff between the social and economic benefits of the Internet versus potential security and social risks posed by the Internet”?
[5] http://www.gartner.com/newsroom/id/3638017

> Si no somos capaces de combatir estas amenazas, nos espera un futuro pesimista.
>
> Tecnólogo, África

La forma en que las partes interesadas se adapten a futuros ataques cibernéticos podría hacer que Internet cambie de un entorno abierto y colaborativo a uno fragmentado, cerrado pero "seguro". Un cambio fundamental en la arquitectura y los principios que subyacen a Internet podría terminar en un futuro distópico de jardines vallados, acceso filtrado y visibilidad total del usuario (sin cifrado, anonimato ni privacidad).[6]

> Se habla mucho sobre seguridad y cifrado, pero los usuarios no están dispuestos a usar nada que les genere siquiera la más mínima molestia. Sospecho que en cinco años todavía estaremos hablando de la importancia de la seguridad, pero las cosas serán aún más inseguras.
>
> Tecnólogo, América del Norte

En este mundo, los intereses de la seguridad nacional eclipsarán las libertades y los derechos. Pase lo que pase, creemos que continuará la lucha entre los intereses de seguridad nacional y las medidas de seguridad de los usuarios finales (por ejemplo, el cifrado).

> Los resultados del choque entre la seguridad y la privacidad son inciertos. Algunos países podrían prohibir el cifrado mientras que otros lo recibirán con los brazos abiertos. Las implicancias para el flujo transfronterizo de datos son potencialmente enormes y perjudiciales.
>
> Sector privado, Europa

Cualquier dilución o denegación de libertades y derechos socavará la confianza en Internet y su capacidad para impulsar la innovación económica y social.

[6] It's important to note that this drive toward walled gardens could come through a security lens and not, as typically expected, through lack of competition [community data result].

> “Temo que, con el pretexto de proteger su seguridad nacional y su soberanía, los gobiernos censuren cada vez más e interrumpan Internet cada vez con mayor frecuencia. Acabaremos con una Internet diferente, controlada por los gobiernos de cada país.
>
> Sociedad Civil, África

Existe una alternativa realista a esta visión distópica de redes cerradas. Si al enfrentarse a las amenazas cibernéticas las partes interesadas responden de forma constructiva y con respuestas coordinadas, cooperando mutuamente en los delitos cibernéticos, convocando plataformas multisectoriales para colaborar mejor en las estrategias nacionales de ciberseguridad y garantizando el respeto por los derechos humanos, entonces los riesgos cibernéticos se podrán gestionar y mitigar mejor y se restablecerá la confianza.

Las amenazas y el impacto de los ataques y delitos cibernéticos también puede dar origen a avances técnicos. Por ejemplo, los avances logrados en las tecnologías de cifrado han aumentado la seguridad de los dispositivos y servicios que utilizan los usuarios, lo que les permiten realizar actividades más sensibles en línea. Como señaló un tecnólogo, “La tendencia negativa es el aumento de la actividad cibercriminal. La tendencia positiva es nuestra capacidad de construir dispositivos y protocolos que harán que esta actividad sea cada vez más difícil”.

> “[Existe la] necesidad de DNSSEC, así como de nuevos estándares como DANE y STS (Strict Transport Security) y todo lo que sea necesario para evitar la distribución de malware y mantener el spam bajo control. Creo que las nuevas tecnologías en realidad harán que Internet sea más segura y la mantendrán funcionando de manera estable.
>
> Gobierno, Europa

Perteneciente a: El papel de los gobiernos; Los derechos y las libertades personales; Redes, estándares e interoperabilidad; La economía de Internet

## Nuevas respuestas y nuevos modelos

El trabajo tendiente a desarrollar normas de comportamiento, marcos legales o incluso tratados se acelerará en los próximos años, a medida que los gobiernos intenten abordar la vertiginosa variedad de desafíos que se presentan en el ciberespacio. La presión para imponer reglas continuará, pero no está claro si los gobiernos priorizarán la cooperación transfronteriza por sobre la soberanía nacional y la seguridad. Además, una pregunta crucial: ¿los tratados o normas realmente frenarían el comportamiento nocivo de los gobiernos o entidades privadas, o simplemente servirían para poder decir que están “haciendo algo”?

> “La falta de un cuerpo normativo nacional e internacional permitirá la proliferación de crímenes y abusos.
>
> Tecnólogo, América del Norte

La necesidad de una cultura global de ciberseguridad se viene discutiendo hace mucho tiempo y cobrará nueva relevancia y sentido de urgencia a medida que la ciberseguridad se convierta en responsabilidad de todos. Desde los mercados financieros hasta los

procesos electorales y pasando por los servicios de salud, en el futuro ningún sistema será inmune a los ciberataques y la ciberdelincuencia. La idea de que "la red es solo tan fuerte como su eslabón más débil" adquiere un nuevo significado en un mundo hiperconectado, donde los dispositivos conectados de un individuo podrían socavar la infraestructura crítica. El ataque a Dyn en 2016 mostró cómo un simple dispositivo conectado puede ser utilizado como parte de una botnet para atacar la infraestructura crítica.[7]

A medida que avancemos, será fundamental contar con nuevas líneas de base para la seguridad, además de modelos de responsabilidad e incentivos. Será incluso más urgente aumentar la alfabetización en seguridad e integrar seguridad en los dispositivos conectados. Se debe crear un mercado para la seguridad de manera de garantizar mayor seguridad para las redes y los dispositivos. Por ejemplo, podrían surgir modelos de responsabilidad que exijan que quienes socavan la red a través de vulnerabilidades en los dispositivos o acciones maliciosas deban hacerse cargo de los daños. Las prácticas de contratación pública deberían incentivar la seguridad.

En un mundo conectado en que la vulnerabilidad a los ciberataques está en aumento, la ciberseguridad ya no puede permanecer únicamente en manos de los gobiernos. De hecho, gran parte de la infraestructura global de Internet es desarrollada, propiedad de, y mantenida por el sector privado. La complejidad y el alcance de los ataques cibernéticos significa que los gobiernos por sí solos no serán capaces de proporcionar las respuestas regulatorias inclusivas e impulsadas por expertos que necesitamos.

> "La otra perspectiva incierta es el uso de armas y guerras cibernéticas para obtener rédito político entre las principales potencias. Esto ya está ocurriendo, pero no queda claro si llevará a grandes interrupciones de la red o si reducirá la confianza de los usuarios de Internet.
>
> Académico, Medio Oriente

No existe un remedio fácil contra los ciberataques y el delito cibernético. Las características de apertura, alcance global e innovación sin permiso son fundamentales para el éxito de Internet. Sin embargo, estas mismas características hacen que sea más fácil y barato lanzar un ciberataque. Esto sin duda representa un desafío formidable para el futuro.

Perteneciente a: Internet y el mundo físico; El papel de los gobiernos; La economía de Internet

[7] The 2016 Dyn attack saw a botnet (a controlled network of devices) used to attack the domain name service provider Dyn. The attack, carried out by a large number of infected IoT devices, caused some Internet platforms and services to be unreachable by parts of the Internet.