EL PRESIDENTE
COMITÉ CONSULTIVO DE SEGURIDAD NACIONAL EN MATERIA DE TELECOMUNICACIONES

Informe del NSTAC al Presidente sobre la resistencia de Internet y las comunicaciones

ÍNDICE DE CONTENIDOS

RESUMEN EJECUTIVO

Los ataques automatizados y distribuidos facilitados a través de botnets amenazan la seguridad y la resistencia del ecosistema de Internet y de las infraestructuras críticas del país. El tamaño y la escala de los ataques de denegación de servicio distribuidos (DDoS) facilitados a través de botnets ha aumentado drásticamente en los últimos años. Esta evolución aumenta la preocupación de que estos ataques puedan sobrecargar las infraestructuras críticas de Estados Unidos. Para agravar aún más el problema, la creciente combinación de dispositivos de la Internet de las Cosas (IoT) proporciona un entorno propicio para que los actores maliciosos lancen ataques globales automatizados utilizando dispositivos IoT comprometidos. Esta situación amenaza la seguridad del ecosistema de Internet.

En mayo de 2017, la Oficina Ejecutiva del Presidente (EOP) solicitó que el Comité Asesor de Telecomunicaciones de Seguridad Nacional del Presidente (NSTAC) examinara cómo el sector privado y el gobierno podrían mejorar la resiliencia del ecosistema de Internet y las comunicaciones. [1] La EOP, en apoyo de la Orden Ejecutiva 13800, *Fortalecimiento de la Ciberseguridad de las Redes Federales y la Infraestructura Crítica*, pidió específicamente al NSTAC que identificara formas de fomentar la colaboración para reducir las amenazas de ataques automatizados y distribuidos (por ejemplo, botnets). Este *Informe del NSTAC al Presidente sobre la resistencia de Internet y las comunicaciones* ("Informe") presenta el trabajo del NSTAC y sus recomendaciones.

PRINCIPALES LECCIONES APRENDIDAS

Es necesario un mayor sentido de la urgencia. La amenaza no hará más que aumentar a medida que crezca el número y el tipo de dispositivos de la IO y que dichos dispositivos sean más autónomos, capaces y omnipresentes.
Siempre que sea posible, el estudio, las pruebas y la aplicación de las posibles soluciones deben llevarse a cabo en paralelo y no de forma secuencial. Hay que esforzarse por adelantarse a las amenazas.

Las asociaciones público-privadas son fundamentales. Las asociaciones público-privadas, como el Financial Systemic Analysis & Resilience Center, así como los esfuerzos de la Oficina Federal de Investigación, Microsoft y los proveedores de servicios de Internet (ISP), demuestran que las redes de bots criminales y las estructuras de mando y control pueden ser desbaratadas con eficacia. La colaboración entre los sectores público y privado es vital para mitigar las redes de bots.

Las soluciones dependen de cada parte del ecosistema de Internet. Los ataques distribuidos son un reto complejo. Ningún segmento del ecosistema de Internet puede resolverlo por sí solo.

Las soluciones dependen tanto de las normas como de la innovación en la capa de infraestructura de la red e Internet. Aunque existe una variedad de normas y mejores prácticas, hay una falta de consistencia global en la adopción de estas prácticas. Las normas desempeñan un papel fundamental en la seguridad del ecosistema de Internet, pero con un entorno normativo fracturado y muchos dispositivos fabricados fuera de Estados Unidos, la implantación de las normas será probablemente desigual. Se necesitan soluciones emergentes en el nivel de la infraestructura. Además, puede ser valioso desarrollar normas antes del dispositivo, como en el nivel de chipset.

[1] Oficina del Secretario de Prensa de la Casa Blanca. *Orden ejecutiva 13800, Fortalecimiento de la ciberseguridad de las redes federales y la infraestructura crítica*. 16 de mayo de 2017. https://www.federalregister.gov/documents/2017/05/16/ 2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

La **educación y la concienciación van a la zaga**. La nación necesita una ciudadanía digital informada. Los individuos y las empresas deben entender cómo sus decisiones afectan a las redes, a los sistemas y a los demás.

Las normas internacionales poco claras complican los desafíos. Gran parte de la amenaza procede del extranjero, por lo que las investigaciones y los juicios internacionales son fundamentales. Es necesaria la cooperación mundial en materia de normas técnicas, seguridad de los dispositivos, atribución, flujos de tráfico y normas y defensas compartidas.

Se necesita un nuevo modelo de confianza. El Protocolo de Control de Transmisión/Protocolo de Internet, el Protocolo de Pasarela de Fronteras, el Sistema de Nombres de Dominio y muchos otros protocolos en los que se basa Internet no se diseñaron teniendo en cuenta la seguridad como preocupación principal. A medida que las redes se vuelven más abiertas e interconectadas, este modelo de confianza ya no puede ser la única base de la seguridad de Internet. [2] Definir cómo se puede construir una mayor confianza en Internet debería ser un punto clave del esfuerzo de Moonshot de ciberseguridad que se describe a continuación.

PRINCIPALES RECOMENDACIONES

El sector privado debe actuar. Hacer frente a los ataques automatizados y distribuidos requiere una vigilancia en todo el ecosistema de Internet, incluidos los proveedores de servicios de red o ISP, los fabricantes de dispositivos, los desarrolladores de software, la nube, los proveedores de aplicaciones y de alojamiento y otras entidades, todos los cuales conforman la infraestructura de Internet. El NSTAC recomienda las siguientes acciones a corto plazo:

- **Acelerar la adopción de directrices de seguridad**. El sector de las comunicaciones debería colaborar con el Departamento de Seguridad Nacional (DHS), como agencia específica del sector de las comunicaciones, y con la Administración Nacional de Telecomunicaciones e Información (NTIA) para identificar las prácticas de seguridad comunes pertinentes para las redes de comunicaciones con el fin de protegerlas contra las redes de bots y los ataques DDoS en los organismos de normalización nacionales y mundiales (por ejemplo*, las* mejores prácticas comunes (BCP) 38) e identificar los obstáculos para su adopción y/o los incentivos para promoverla. Las redes no pueden limitarse a los grandes proveedores de servicios de Internet (ISP), ya que muchas prácticas deberían ser desplegadas por cualquier entidad que gestione una red de acceso público, incluidas las empresas.

- **Desarrollar directrices de seguridad para dispositivos IoT.** El Departamento de Comercio (DOC), a través de la NTIA y el Instituto Nacional de Estándares y Tecnología (NIST), debería trabajar con los fabricantes de dispositivos para facilitar el desarrollo de una línea de base de prácticas de seguridad de sentido común recomendadas y coherentes con el riesgo asociado a un dispositivo. El DOC también debería revisar el papel y la viabilidad de la certificación voluntaria de dispositivos y de las pruebas independientes para garantizar la seguridad de los mismos.

- **Seguir innovando en torno a las soluciones basadas en la infraestructura.** Los gobiernos y la industria no pueden depender únicamente de la adopción coherente de normas para asegurar el IoT. Los ISP, los proveedores de servicios inalámbricos, los fabricantes de routers, los proveedores de soluciones de seguridad y otros están desarrollando servicios para gestionar la seguridad de la IO. Estas soluciones pueden emplearse en diferentes capas de la red, desde el interior del hogar (por ejemplo*,* Ethernet, Wi-Fi) hasta incluir; la seguridad a largo plazo

[2] Consejo de Fiabilidad e Interoperabilidad de la Seguridad de las Comunicaciones (CSRIC) V: Grupo de Trabajo 10, Legacy Risk Reductions (2017) (Informe sobre las reducciones del riesgo heredado), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

Evolución o infraestructura de red inalámbrica de quinta generación; el núcleo de la red de conmutación de etiquetas multiprotocolo; y en la capa de aplicación o en la nube. [3] Estas capacidades son emergentes y el sector privado debería seguir invirtiendo en estas tecnologías. El Gobierno de EE.UU. debería ayudar a impulsar estas capacidades incorporándolas a los requisitos de contratación federal y concienciando sobre su aplicación para la seguridad del IoT.

- **Promover los controles de seguridad de las empresas para mejorar la seguridad de los dispositivos IoT.** El NIST debería desarrollar casos de uso basados en el Marco de Ciberseguridad del NIST para que las empresas incorporen la IO a la gestión de riesgos. Muchos dispositivos de IoT tendrán una doble función en las redes de los consumidores y de las empresas. Las empresas y el gobierno pueden promover normas de seguridad de IoT para los dispositivos en los acuerdos de compra.

- **Promover la garantía del software.** La industria del software debería trabajar con el DHS para promover prácticas comunes para la garantía del software. El conocimiento de las mejores prácticas proporcionaría a los compradores visibilidad sobre cómo sus proveedores incorporan la seguridad y les ayudaría a tomar mejores decisiones de compra.

El Gobierno debe actuar. El gobierno debe responder a la creciente amenaza de las botnets en tres áreas fundamentales. El NSTAC recomienda que el gobierno (1) tome mayores medidas para apoyar a las fuerzas de seguridad; (2) promueva la adopción de normas de seguridad y mejores prácticas; y (3) desarrolle una estrategia de ciberseguridad internacional efectiva.

- **Aplicación de la ley**

    - **Apoyar la colaboración público-privada y los desmantelamientos.** El gobierno, incluido el Departamento de Justicia (DOJ), debería aumentar los esfuerzos de desmantelamiento que han mitigado con éxito el impacto de las redes de bots. El Gobierno de Estados Unidos debería aumentar los incentivos, especialmente dentro del Departamento de Justicia, para que la prevención de la ciberdelincuencia y la desarticulación de las redes de bots sean una prioridad. Las implicaciones de las botnets para la seguridad nacional justifican tanto la prevención como la persecución. El Departamento de Justicia puede necesitar recursos adicionales para aumentar estos esfuerzos, que también dependen de la colaboración con el sector privado y con posibles socios internacionales.

- **Fomento de la adopción de normas y buenas prácticas de seguridad**

    - **Promover normas flexibles mediante incentivos y eliminar los obstáculos para su adopción.** La NTIA, el NIST y otros organismos deberían convocar a las partes interesadas y promover la coordinación entre sectores para desarrollar normas comunes y promover prácticas coherentes en el gobierno y en las infraestructuras críticas. El gobierno debería identificar las lagunas y los incentivos para motivar a la industria a adoptar normas y prácticas. Algunas industrias, si se retrasan, pueden necesitar más incentivos, sobre todo cuando se trata de mitigar los riesgos de los dispositivos actualmente existentes. Las empresas más pequeñas también pueden carecer de los mismos recursos y acceso a la experiencia cibernética que las entidades más grandes. Por último, el mercado de los seguros puede impulsar

[3] Cisco ofrece un ejemplo de marco para la seguridad del IoT en cada capa de la red en https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

mejora, ya que los suscriptores examinan a las empresas en función de la madurez de sus prácticas de gestión de los riesgos de seguridad y ofrecen primas más bajas a las empresas que se encuentran más arriba en la escala de madurez.

- **Intentar armonizar los requisitos de seguridad a nivel federal, estatal e internacional.** Las normas, prácticas y reglamentos en materia de ciberseguridad se abordan a menudo de forma fragmentada y algo ineficaz. A nivel nacional, algunos estados establecen requisitos de seguridad específicos para cada estado. A nivel internacional, la Unión Europea, Japón, China y varios otros países están estudiando el desarrollo de programas de certificación y pruebas de dispositivos IoT. El Gobierno de EE.UU. debe abogar por unas normas de seguridad de IoT interoperables y coherentes en el extranjero y a nivel nacional entre los estados para fomentar un enfoque unificado.

- **Mejorar la ciberseguridad del gobierno.** El Gobierno de Estados Unidos debe dar ejemplo mejorando la seguridad de las redes federales. La modernización de la tecnología de la información (TI) es un componente clave para mejorar la ciberseguridad federal. El gobierno debe utilizar sus esfuerzos en curso para modernizar la TI federal para impulsar la adopción de nuevas tecnologías y soluciones de seguridad en el sector privado.

- **Ciberseguridad internacional**

  - **Desarrollar una estrategia global de participación de Estados Unidos en materia de normas**. Estados Unidos ha recurrido tradicionalmente a la colaboración con la industria privada para potenciar los esfuerzos del gobierno en los foros internacionales de normalización. Sin embargo, en los últimos años las entidades extranjeras han aumentado rápidamente su presencia en la elaboración de normas internacionales. El Gobierno de Estados Unidos debería colaborar con el sector privado para garantizar su representación en los principales foros que influyen en el desarrollo de las normas tecnológicas que pueden dar lugar a problemas de seguridad nacional en el futuro.

  - **Desarrollar una estrategia eficaz de ciberseguridad internacional centrada en aumentar el coste para los atacantes.** El gobierno debe priorizar el desarrollo de una estrategia integral de ciberseguridad internacional que aproveche las herramientas diplomáticas tradicionales y el apoyo a la aplicación de la ley a nivel mundial con el objetivo de aumentar los costes para los ciberatacantes. Muchos ataques DDoS son internacionales, y el gobierno debe implementar una estrategia global para hacer frente a las amenazas. La naturaleza persistente de los ciberataques significa que incluso las entidades con las mejores prácticas pueden ser explotadas. La nación debe aumentar el coste para los atacantes y, al mismo tiempo, adoptar normas, prácticas y nuevas soluciones tecnológicas innovadoras para dificultar los ataques.

- **La nación necesita un Moonshot de ciberseguridad.** Un futuro esfuerzo del NSTAC debería analizar el concepto de lanzar un Moonshot de ciberseguridad en dos fases. En la primera fase se examinarían otros modelos de Moonshot que han tenido éxito, incluso fuera del ámbito de la ciberseguridad, para identificar principios coherentes que puedan aplicarse al reto de la ciberseguridad. Como punto de partida, esto incluiría el estudio de modelos que presenten al menos las siguientes características:

  - Llamada a la acción nacional;
  - Centrarse en una meta final, estableciendo un objetivo específico o un estado final para una fecha determinada; y
  - Un proceso multipartito dirigido por el gobierno.

En la segunda fase del estudio*, el* NSTAC trataría de aclarar las consideraciones clave de ciberseguridad relacionadas con los principios identificados del Moonshot (Llamada a la Acción, Enfoque del Objetivo Final y Proceso Multiparticipativo), recurriendo a expertos en ciberseguridad para definir un objetivo final y subelementos, y ampliando el material que el NSTAC revisó durante la preparación de este Informe. [4]

[4] Un ejemplo fue la sesión informativa sobre los modelos de referencia de memoria unificada que ofreció Steve Wallach. Micron Technology, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 7 de septiembre de 2017.

1.0 INTRODUCCIÓN

Cada vez es más preocupante la posibilidad de que los actores maliciosos utilicen las redes de bots para facilitar los ataques de denegación de servicio distribuido (DDoS) a gran escala que podrían interrumpir las infraestructuras críticas de Estados Unidos. Los atacantes se aprovechan de vulnerabilidades fundamentales de Internet, como el Sistema de Nombres de Dominio (DNS), el Protocolo de Tiempo de Red (NTP), el Protocolo Simple de Descubrimiento de Servicios, el Protocolo Generador de Caracteres (CharGen) y otros protocolos, para aumentar drásticamente el tamaño y la escala de los ataques. [5] Además, aunque las redes de bots no son nuevas, los dispositivos del Internet de las Cosas (IoT) agravan el riesgo, ya que conectan a un número cada vez mayor de personas, dispositivos y redes. El ataque de la red de bots Mirai en 2016 fue la primera red de bots basada en el IoT con un impacto significativo, pero se espera que estos ataques aumenten. [6] Estos factores han provocado un rápido aumento del tamaño y la escala de los ataques DDoS. Por ejemplo, según una fuente, el tamaño de los ataques oscilaba en torno a los 100 Gigabits por segundo (Gbps) hasta mediados de 2012, después de lo cual el tamaño comenzó a aumentar drásticamente. La misma fuente estimó que el tamaño máximo de los ataques en 2016 fue de aproximadamente 800 Gbps, un aumento de ocho veces en los últimos 4 años. [7] Este informe ofrece recomendaciones para reducir el impacto potencial de las redes de bots y los ataques DDoS y la amenaza que suponen para las infraestructuras críticas del país.

1.1 Ámbito de aplicación e imputación

En mayo de 2017, la Oficina Ejecutiva del Presidente (EOP) solicitó que el Comité Asesor de Telecomunicaciones de Seguridad Nacional del Presidente (NSTAC) examinara cómo el sector privado y el gobierno pueden colaborar para mejorar la resiliencia del ecosistema de Internet y las comunicaciones. [8] La EOP, en apoyo de la Orden Ejecutiva (EO) 13800, *Fortalecimiento de la Ciberseguridad de las Redes Federales y la Infraestructura Crítica*, encargó al NSTAC que identificara formas de fomentar la colaboración para reducir las amenazas de los ataques automatizados y distribuidos (como las botnets). Además, el EOP pidió al NSTAC que considerara qué reglas de compromiso permitirán los esfuerzos de cooperación para proteger la postura de ciberseguridad de la nación. En junio de 2017, el NSTAC formó el comité de Resiliencia de Internet y Comunicaciones (ICR) para abordar las peticiones del EOP. [9] EOP declaró que las conclusiones del NSTAC servirían de base para un informe preliminar que publicarían el Departamento de Comercio (DOC) y el Departamento de Seguridad Nacional (DHS) en enero de 2018.

Los ataques DDoS y botnet son cada vez más preocupantes. En 2014, el NSTAC observó que "en 2020 habrá decenas de miles de millones de dispositivos en uso. Ahora es el momento de influir en el diseño de esos dispositivos y en los protocolos que rigen su uso; una vez desplegados, la nueva política

[5] Arbor Networks Worldwide Infrastructure Security Report, Volumen XII, disponible en https://www.arbornetworks.com/insight-into-the-global-threat-landscape

[6] Véase Computer Weekly, "Global Hacker Botnet Tops 6 Million Hijacked Devices", 27 de septiembre de 2017 http://www.computerweekly.com/news/450427023/Global-hacker-botnet-tops-6-million-hijacked-devices

[7] Arbor Networks Worldwide Infrastructure Security Report Volume XII, disponible en https://www.arbornetworks.com/insight-into-the-global-threat-landscape

[8] Oficina del Secretario de Prensa de la Casa Blanca. *Orden ejecutiva 13800, Fortalecimiento de la ciberseguridad de las redes federales y la infraestructura crítica*. 11 de mayo de 2017. https://www.federalregister.gov/documents/2017/05/16/ 2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

[9] Un informe del Subcomité ICR se debe presentar en octubre de 2017. El DHS y el DOC publicarán un informe preliminar en enero de 2018 y un informe final en mayo de 2018.

El objetivo del NSTAC es ayudar a la Administración a profundizar en la cooperación gubernamental y privada.

Este *Informe del NSTAC al Presidente sobre la resistencia de Internet y las comunicaciones* ("Informe") presenta el trabajo del NSTAC y sus recomendaciones. Proporciona a la EOP una hoja de ruta procesable para hacer frente a las amenazas que suponen las redes de bots y otros ataques distribuidos y automatizados contra nuestra infraestructura de Internet, los servicios en línea y los usuarios finales. Este Informe examina las amenazas y las soluciones, desde los remedios a corto plazo hasta el desarrollo de la arquitectura de Internet a largo plazo. El Informe está organizado de la siguiente manera:

- La sección 1 explica el alcance y los objetivos.
- La sección 2 describe el ecosistema global de Internet y cómo los ataques distribuidos amenazan la seguridad de un mundo cada vez más conectado.
- La sección 3 identifica los retos y los esfuerzos de mitigación en cada segmento del ecosistema: redes, consumidores/borde/dispositivos, empresa y software/aplicaciones/sistemas operativos (SO).
- La sección 4 ofrece recomendaciones a corto y largo plazo, así como un estudio Moonshot de seguimiento para abordar de forma holística los retos de la ciberseguridad en general, incluidos los ataques automatizados y distribuidos.
- La sección 5 identifica las oportunidades para que el gobierno utilice las herramientas únicas de que dispone y colabore con el sector privado.

1.2 Acérquese a

El NSTAC utilizó varios métodos para recabar información, entre ellos sesiones informativas de expertos en la materia, la realización de revisiones de políticas y el examen de informes sobre amenazas a la ciberseguridad, artículos y mejores prácticas para combatir estas amenazas. Entre otras cosas, el NSTAC:

- Recibió más de dos docenas de sesiones informativas de expertos de la industria, el mundo académico y el sector público, como se refleja en el Apéndice A;
- Se han revisado las políticas de ciberseguridad del sector privado y del Gobierno Federal, las normativas, los informes y las mejores prácticas, como el Marco de Ciberseguridad del Instituto Nacional de Normas y Tecnología (NIST);
- Se han revisado las mejores prácticas e investigaciones en materia de ciberseguridad de la industria.

[10] Comité Asesor de Telecomunicaciones de Seguridad Nacional del Presidente (NSTAC). *Informe del NSTAC al Presidente sobre el Internet de las cosas*. November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf. Apéndice E, E-5.

- Se examinaron estudios y comentarios sobre ciberseguridad en el NIST y la Administración Nacional de Telecomunicaciones e Información (NTIA).

El NSTAC examinó los puntos débiles de la seguridad del ecosistema e identificó áreas para mejorar la seguridad en los niveles de red, dispositivo y usuario. En este informe, el NSTAC recomienda medidas para crear un ecosistema de Internet más seguro, centrándose en las asociaciones entre el gobierno y la industria para hacer frente a las actividades maliciosas.

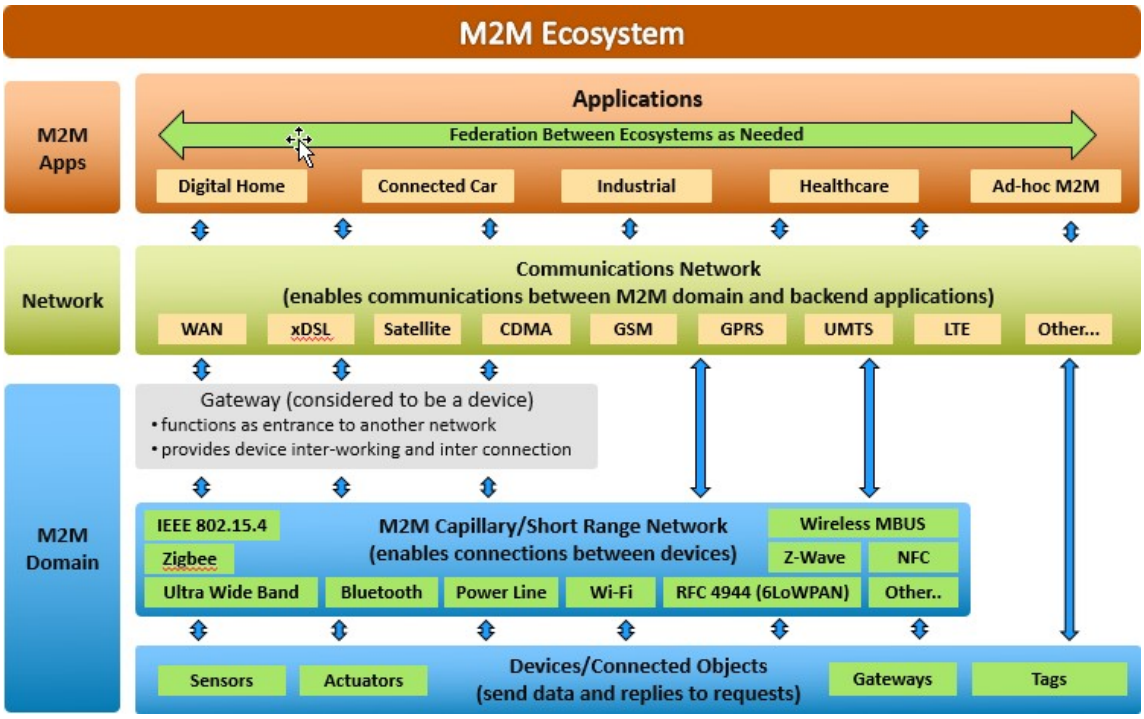
2.0 LA NATURALEZA GLOBAL DEL ECOSISTEMA FACILITA LOS ATAQUES DISTRIBUIDOS Y AUTOMATIZADOS

El ecosistema de Internet es diverso y difuso, y cada parte desempeña un papel en la seguridad. El ecosistema sigue creciendo con la proliferación de dispositivos que conectan a Internet artículos de uso cotidiano como coches y termostatos, soportan sistemas de control industrial y supervisan infraestructuras críticas. Un actor malicioso que controle un dispositivo infectado genera múltiples riesgos. En primer lugar, el dispositivo podría ser utilizado en un ataque de denegación de servicio a otro dispositivo. En segundo lugar, el software bot de un dispositivo podría utilizarse para robar información del dispositivo o rastrearlo. Por ejemplo, el software de bots en el software de navegación del coche de un congresista podría rastrear los movimientos del vehículo. En tercer lugar, el software bot en un dispositivo podría utilizarse para generar un evento de denegación de servicio (DoS) en el propio dispositivo. En cuarto lugar, el bot podría manipular los datos o provocar un comportamiento incorrecto del dispositivo, poniendo así en peligro la seguridad de los usuarios o corrompiendo los datos del dispositivo e influyendo en los resultados para los consumidores de datos. A medida que los dispositivos IoT proliferan y cumplen funciones cada vez más delicadas, como la conducción autónoma y los controles industriales, la incapacitación de los dispositivos IoT puede tener impactos significativos y peligrosos en el mundo real.

2.1 El ecosistema mundial de Internet y las comunicaciones es diverso y evoluciona

Los usuarios finales, los proveedores de servicios de Internet (PSI), los operadores de redes, los fabricantes y los desarrolladores de software conforman el ecosistema global de Internet. Los gobiernos y los sistemas internacionales también desempeñan un papel. Las capas que soportan el IoT máquina a máquina (M2M) y que componen el ecosistema se ilustran en la figura 1 de la página siguiente.

Figura 1. El ecosistema M2M



Fuente: Presentación de AT&T sobre el Informe del NSTAC al Presidente sobre el Internet de las cosas. 19 de noviembre de 2014.

Aunque algunos sostienen que los ISP están en la mejor posición para mitigar los ataques de botnets, el IoT está formado por dispositivos, redes de transporte, aplicaciones y las empresas y usuarios que los despliegan. Cada segmento se enfrenta a amenazas y requiere atención.

Figura 2. Panorama de las amenazas

Fuente: Brian Rexroad. AT&T. Sesión informativa para el subcomité ICR del NSTAC. 20 de julio de 2017.

Los expertos prevén una migración hacia los servicios gestionados de IoT a medida que las empresas ofrezcan soluciones integrales. [11] A medida que proliferan los dispositivos IoT, proporcionan una nueva escala para las redes de bots.

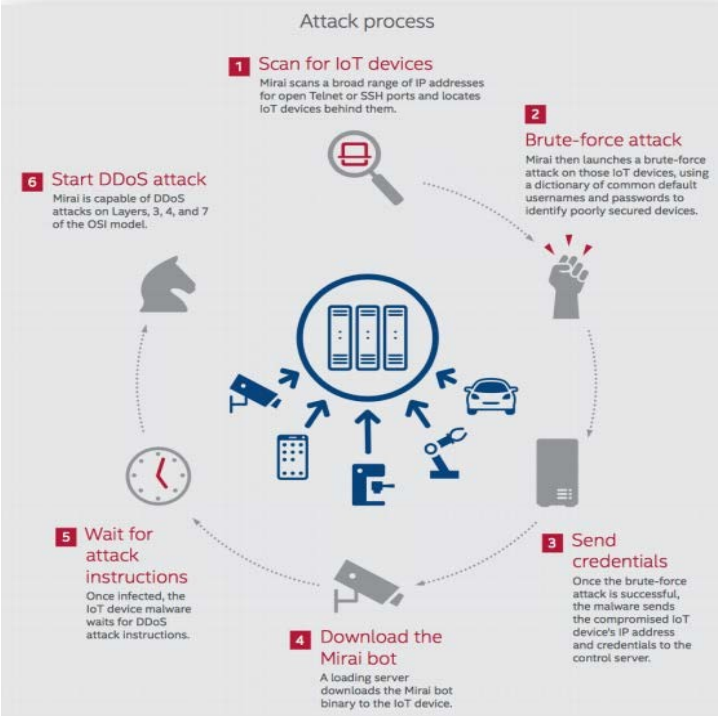
[11] Kevin Walsh. Palo Alto Networks, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 18 de julio de 2017.

2.2 Las redes de bots y los ataques distribuidos automatizados evolucionan

Las redes de bots se diseñaron originalmente para un uso positivo y posteriormente se reutilizaron para acciones hostiles. Un bot es "un programa que se instala en un sistema para que éste realice automáticamente (o de forma semiautomática) una tarea o conjunto de tareas, normalmente bajo el mando y control de un administrador remoto (también conocido como bot master o bot herder)".[12] Estos programas pueden ejecutar código no proporcionado por el proveedor ni autorizado por su propietario. La mayoría de los bots pueden apoyar actividades maliciosas como el spam, el phishing, el fraude por clic y el DDoS.

Una botnet es "una red de dispositivos informáticos de usuario final conectados a Internet infectados con malware bot y controlados de forma remota por terceros con fines nefastos".[13] Un ataque de botnet se produce cuando una red de ordenadores, IoT u otros dispositivos habilitados para el protocolo de Internet (IP) son requisados para ejecutar código no autorizado en apoyo de actividades maliciosas como el spam, el phishing, el fraude de clics y el DDoS. La figura 3 muestra cómo se producen los ataques de botnets.

Figura 3. Cómo se producen los ataques de botnets



Fuente: McAfee, https://www.mcafee.com/us/resources/misc/infographic-threats-report-mar-2017.pdf

Los bots se distribuyen generalmente a través de sitios web infectados o enlaces a sitios web maliciosos incrustados en correos electrónicos de phishing. Los usuarios pueden instalar bots inadvertidamente basándose en correos electrónicos engañosos, instrucciones web o a través de vulnerabilidades del navegador/OS. Los bots también pueden desplegarse sin que el usuario final realice ninguna acción. Por ejemplo, en la red de bots Mirai se infectaron varios dispositivos sin que el usuario

[12] Comisión Federal de Comunicaciones (FCC). CSRIC. III, *Código de Conducta Anti-Bot de Estados Unidos (ABC) para los proveedores de servicios de Internet*. Marzo de 2012. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

[13] Ibid.

interacción. Las contraseñas predeterminadas para la gestión de dispositivos o las puertas traseras instaladas por el proveedor pueden verse comprometidas, permitiendo el acceso y el control no autorizados de un dispositivo. Los bots también se distribuyen a través de esquemas de phishing, spam y otras amenazas a la seguridad. Un aspecto clave de las campañas de las redes de bots es la naturaleza persistente de los ataques que buscan explotar cualquier debilidad disponible para obtener acceso. Los bots pueden actualizar los parches de seguridad y el software antivirus de una máquina para garantizar un funcionamiento estable y la exclusión de otros bots. Cuando la gente habla de botnets, suele pensar en ataques DDoS. [14]Pero las redes de bots pueden facilitar el robo de datos, la distribución de contenido ilegal, el robo de procesamiento, el spam por correo electrónico, el fraude por clic, y otros ataques. [15]

Los **ataques de botnets están aumentando en tamaño y sofisticación con el auge del IoT**. Algunas redes de bots utilizan la inteligencia artificial (IA), la criptografía cuántica o la computación neuromórfica para crear virus más inteligentes que se adaptan a la velocidad de Internet. [16]El mayor ataque registrado fue de 800 Gbps, y aproximadamente un tercio de los ataques alcanzan picos de más de 100 Gbps. [17]Los ISP aumentaron drásticamente la protección DDoS tras los ataques DDoS a instituciones financieras en 2012-13,[18]pero los ataques DoS han aumentado de tamaño, y los atacantes han cambiado de táctica. Por ejemplo, los atacantes se dirigen a los dominios con el mayor registro DNS para amplificar la eficacia de su ataque.
Además, a medida que los dispositivos se vuelvan más autónomos e incluyan una sofisticada IA, las implicaciones de los delitos cibernéticos a través de la IO darán lugar a nuevos y graves riesgos que deben anticiparse y planificarse a corto plazo.

La **mitigación aumenta la prevención**. Los ciberataques se producirán. [19]Según la Dirección de Ciencia y Tecnología del DHS, el 70% de los ataques informáticos utilizan credenciales perdidas, robadas o débiles, y el 60% del malware utiliza la escalada de privilegios o credenciales robadas. [20]En lugar de prevenir los ataques de redes de bots, los expertos han pasado a construir redes más resistentes y a mitigar los efectos de los ataques. Las mejores prácticas para mitigar los ataques se centran en la educación del usuario y de la empresa sobre la higiene de la red y la gestión de la vulnerabilidad. Esto incluye la autenticación fuerte, la desactivación de funciones no deseadas y la actualización de servicios. Otras herramientas de mitigación son el análisis de la red y de los datos, los proxies inversos, los cortafuegos de aplicaciones y de red y los equilibradores de carga, y la reconfiguración/seguridad de los routers de Internet. La mitigación de ataques DDoS a gran escala funciona mejor cuando se complementa con servicios de centro de datos/borde. El análisis de datos, las señales, las medidas sistémicas, la detección de anomalías, la detección de datos y los activadores son útiles para mitigar los ataques de botnets. Es importante revisar las características y dependencias conjuntas para identificar comportamientos similares y asignarlos a los actores. [21]

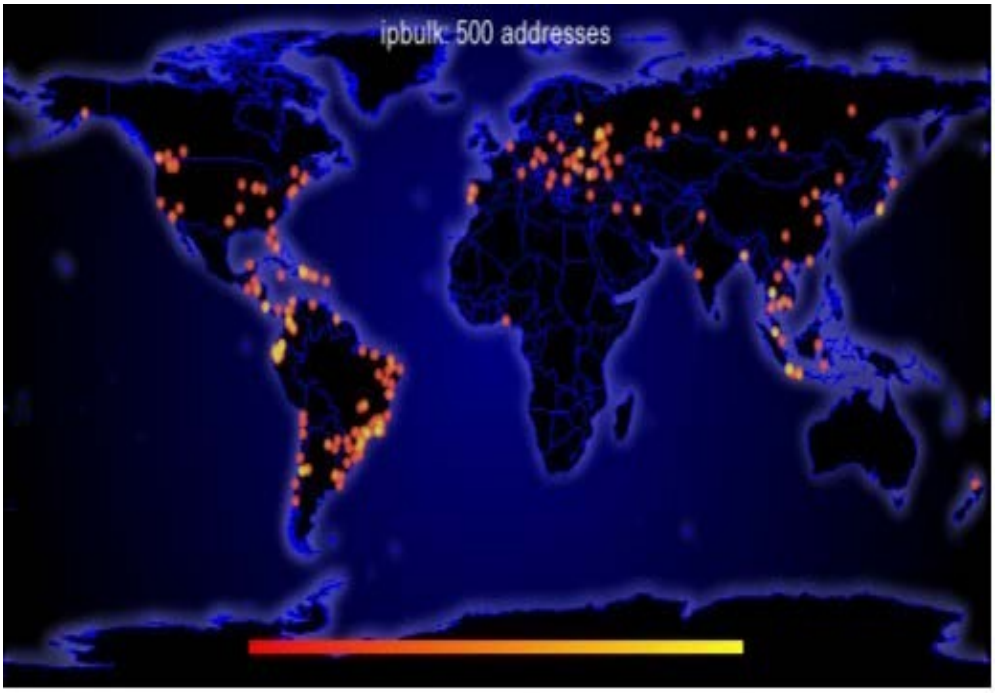
[14] Kim Zetter. "Léxico Hacker: ¿Qué son los ataques DoS y DDoS?" *Wired.* 6 de enero de 2016. https://www.wired.com/2016/01/hacker-lexicon-que-son-dos-y-ddos-ataques/.
[15] NTIA. Consejo de Coordinación del Sector de las Comunicaciones. *Libro blanco técnico del sector*. 17 de julio de 2017. https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.
[16] Anthony Scriffignano. Dun & Bradstreet, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 15 de agosto de 2017.
[17] Arrabelle Hallawell. Arbor Networks, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 3 de agosto de 2017.
[18] Bill O'Hern. AT&T, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 20 de julio de 2017.
[19] Anthony Scriffignano. Dun & Bradstreet, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 15 de agosto de 2017.
[20] Ann Cox. DHS. *Sesión informativa para el Subcomité ICR del NSTAC*. 1 de agosto de 2017.
[21] Anthony Scriffignano. Dun & Bradstreet, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 15 de agosto de 2017.

2.3 Las redes de bots y los ataques distribuidos automatizados son globales, lo que complica la respuesta

Los dispositivos infectados, los objetivos, los malos actores y las víctimas están distribuidos por todo el mundo. Los malos actores incluyen estados nacionales, grupos criminales organizados, hacktivistas e individuos. El estado de derecho tiene poco impacto, y la capacidad de los delincuentes para cubrir sus huellas complica la atribución. Los actores maliciosos suelen estar motivados por el beneficio económico o la capacidad de causar una interrupción de los servicios. [22] Existen objetivos en la industria de la salud, el mundo académico y el sector público; las víctimas en Estados Unidos son más propensas a pagar un rescate. [23]

Más del 80% del tráfico de botnets se origina en el extranjero y la mayor parte del tráfico está diseñado para parecer legítimo. China es el país con más botnets, con cerca de 1,4 millones. India es el segundo país, con menos de un millón, y Rusia es el tercero, con menos de 600.000.[24] En el primer trimestre de 2017, China y Corea del Sur "siguieron encabezando la lista de países atacantes... La mayoría de los ataques (50,8%) se originaron en China, seguida de Corea del Sur (10,8%)" y Estados Unidos, con un 7,2%.[25] La mayoría de los resolvedores de DNS abiertos utilizados en los ataques están fuera de Estados Unidos. [26]

Figura 4. Ubicación de los resolvedores de DNS



Fuente: Bill O'Hern. AT&T. Sesión informativa para el Subcomité de Resiliencia de Internet y Comunicaciones (ICR) del NSTAC. 20 de julio de 2017

[22] Ibid.

[23] Raj Samani. McAfee, Reino Unido. *Sesión informativa para el subcomité ICR del NSTAC*. 15 de agosto de 2017.

[24] Proyecto Spamhaus. *Los peores países del mundo en materia de botnets*. 18 de agosto de 2017. https://www.spamhaus.org/statistics/botnet-cc/.

[25] Incapsula. *Global DDoS Threat Landscape*. 2017. https://www.incapsula.com/ddos-report/ddos-report-q1- 2017.html.

[26] Bill O'Hern. AT&T, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 20 de julio de 2017.

En octubre de 2016, la red de bots Mirai lanzó un DDoS contra el proveedor de DNS Dyn. El ataque interrumpió algunos de los mayores sitios web del mundo. Mirai se aprovecha de la débil seguridad de muchos dispositivos IoT, escaneando continuamente los dispositivos IoT accesibles a través de Internet que solo están protegidos por la configuración predeterminada de fábrica y contienen nombres de usuario y contraseñas codificados. Mirai infecta los dispositivos con malware y los obliga a informar a un servidor de control central, convirtiéndolos en bots que pueden utilizarse en ataques DDoS. [27]Un número relativamente pequeño de fabricantes y sus proveedores posteriores son conocidos por desarrollar dispositivos IoT vulnerables.

La industria trabaja internamente y con las fuerzas de seguridad para cerrar los hosts de botnets, pero la colaboración es un reto cuando se produce a través de las fronteras políticas. El Gobierno de EE.UU. dispone de autoridades y herramientas que podrían permitirle tomar medidas afirmativas (tanto ofensivas como defensivas) contra las redes de bots, pero el uso de dichas herramientas plantea cuestiones políticas. Hay cuestiones complejas en torno a la "defensa activa" y a las operaciones cibernéticas ofensivas, incluyendo lo que debe llevarse a cabo, cómo mejorar la previsibilidad de los efectos (ya que una de las razones clave para la restricción es la falta de previsibilidad/precisión de los impactos), y quién debe participar. Estas cuestiones requieren un debate y una planificación conjuntos entre el Gobierno de Estados Unidos, los socios extranjeros y la industria. "Defensa activa" significa cosas diferentes en distintos contextos, y es necesario seguir debatiendo.

3.0 CADA PARTE DEL ECOSISTEMA DEBE ABORDAR LA SEGURIDAD

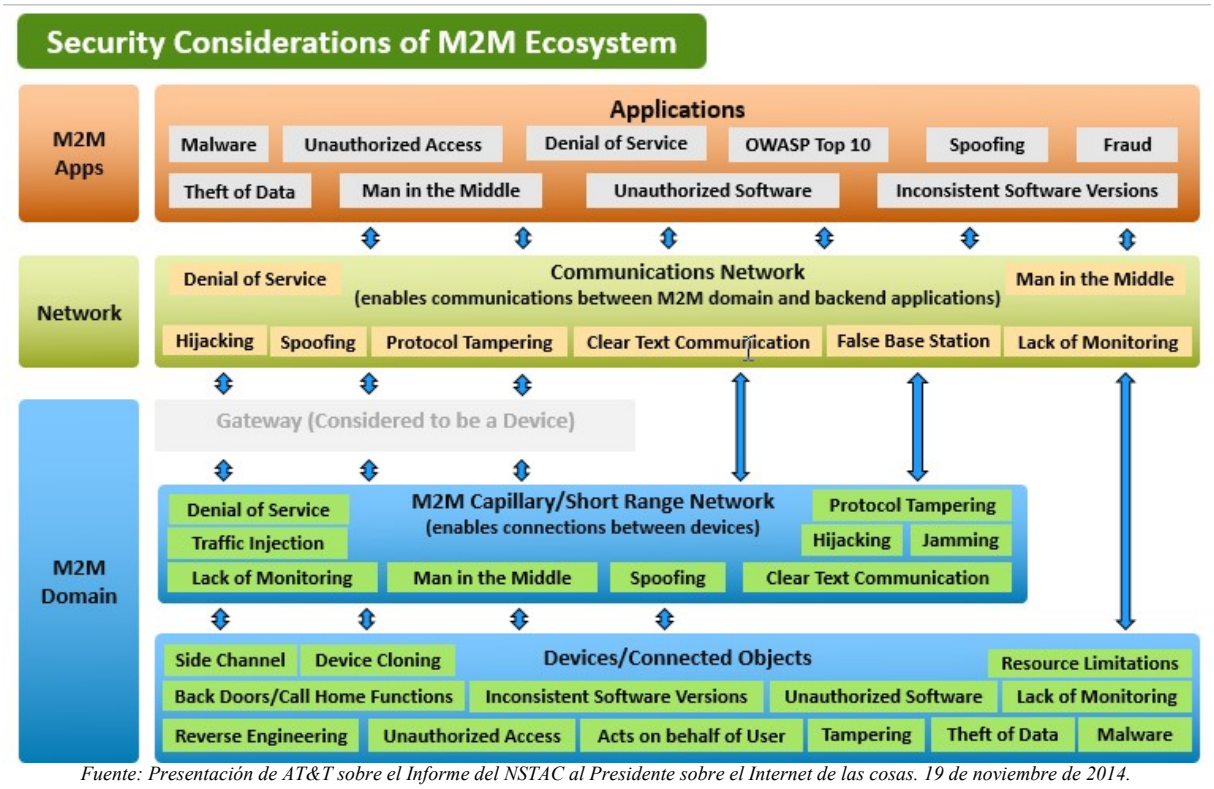
A efectos de este informe, el NSTAC dividió el ecosistema en capas:

- Red (3.1)
- Consumidores/Escala/Dispositivo (3.2)
- Empresa (3,3)
- Aplicaciones/Software/OS (3.4)
- Gobierno (3,5)
- Internacional (3,6)

La ciberseguridad exige una acción agresiva en cada parte del ecosistema.

[27] Symantec. *Mirai: Lo que hay que saber sobre la botnet que está detrás de los grandes ataques DDoS recientes*. 27 de octubre de 2016. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent- major-ddos-attacks.

Figura 5. Consideraciones de seguridad del ecosistema M2M



Fuente: Presentación de AT&T sobre el Informe del NSTAC al Presidente sobre el Internet de las cosas. 19 de noviembre de 2014.

PRINCIPALES RESULTADOS RELEVANTES PARA CADA CAPA DEL ECOSISTEMA

Varios pasos ayudarán a proteger el ecosistema de Internet de los ataques distribuidos y automatizados. Los diferentes actores deben contribuir -individual y colectivamente- a crear una mejor seguridad. Este Informe se centra en los actores clave y en su papel para reforzar la seguridad de Internet.

Capa de red. Los proveedores de servicios de red cuentan con una serie de prácticas comunes para mitigar los ataques distribuidos. Estas prácticas incluyen las Prácticas Comunes DDoS de los Proveedores de Servicios de Red; el Código de Conducta Anti-Botnet (ABC) para los ISP, y el BCP del Foro Técnico de Ingeniería de Internet (IETF), y los métodos del Consejo de Seguridad, Fiabilidad e Interoperabilidad de las Comunicaciones (CSRIC) de la Comisión Federal de Comunicaciones (FCC). El sector de las comunicaciones desarrolló prácticas en el CSRIC28 de la FCC sobre muchas cuestiones, como las mejores prácticas de DDoS, la mitigación de botnets y la aplicación del *Marco* del NIST *para mejorar la ciberseguridad de las infraestructuras críticas*. Muchos proveedores han implementado estas prácticas, sin embargo, otros ISP nacionales e internacionales, y los que operan redes

[28] El CSRIC y su organización predecesora, el Consejo de Fiabilidad e Interoperabilidad de la Red (NRIC), abordaron por primera vez las mejores prácticas de ciberseguridad en el NRIC VI de 2002 a 2004. Véase https://www.fcc.gov/about- fcc/advisory-committees/communications-security-reliability-and-interoperability-4.

capacidades[29] también deben adoptarlas para reducir el impacto de los ataques distribuidos. [30] Las recomendaciones del informe del CSRIC incluyen el bloqueo del tráfico con destino y origen en determinados puertos de Internet, la mejora de la inteligencia de la red y la visibilidad de los flujos de tráfico, el filtrado del tráfico entre proveedores de servicios de Internet en tránsito en caso de ataque a gran escala y la aplicación del aprendizaje automático en la detección de botnets.

Los proveedores de servicios de red también pueden ayudar a proteger los dispositivos IoT que están conectados a sus redes; por ejemplo, los operadores inalámbricos pueden ofrecer servicios para ayudar a gestionar la seguridad de los dispositivos IoT conectados a las redes Long Term Evolution o de quinta generación (5G) en asociación con una variedad de otros actores del ecosistema. Por ejemplo, AT&T, IBM, Nokia, Palo Alto Networks, Symantec y Trustonic formaron recientemente una Alianza de Ciberseguridad del IoT, que pretende impulsar la colaboración de las empresas miembros para desarrollar soluciones de varios niveles a los retos de ciberseguridad del IoT. Los proveedores de redes están desarrollando actualmente capacidades en la capa de red aprovechando el análisis de grandes datos y el aprendizaje automático para detectar y mitigar los ataques basados en el IoT, y es probable que sigan introduciendo nuevas capacidades y servicios para ayudar a gestionar mejor los dispositivos del IoT.

Capa de dispositivos/borde. La seguridad de los dispositivos debe mejorar, ya que el armamento de los mismos y su posible uso en ataques DDoS sigue siendo un problema importante. Aunque hay muchas actividades privadas en marcha, el gobierno debería convocar a las partes interesadas para impulsar la adopción de normas y mejores prácticas. El sector privado debería liderar el desarrollo de normas, y el gobierno puede convocar a expertos para demostrar cómo se pueden aplicar dichas normas a través de casos de uso. A medida que surjan las mejores prácticas, el ecosistema puede considerar certificaciones de dispositivos voluntarias e impulsadas por la industria que también incluyan el apoyo del fabricante para el ciclo de vida del producto. El NSTAC recomendó anteriormente que "se debería considerar la posibilidad de establecer un Underwriters Lab (UL) para la certificación de políticas de seguridad específicas"[31] El NSTAC apoya la conclusión de que sería útil alguna forma de certificación impulsada por la industria para los dispositivos de IoT, basada en normas internacionales.

Hasta cierto punto, este esfuerzo ya está en marcha. UL está desarrollando un programa de certificación de dispositivos y otras organizaciones, como el Laboratorio Independiente de Pruebas de Ciberseguridad32 (CITL), están probando dispositivos. Consumer Reports ha empezado a colaborar con entidades, como el CITL, para tener en cuenta la seguridad en las revisiones de los dispositivos, lo que puede aumentar la concienciación de los consumidores. Además, el gobierno ha iniciado procesos, como el trabajo de la NTIA sobre la capacidad de actualización de los dispositivos IoT y los esfuerzos del NIST en materia de sistemas ciberfísicos. El gobierno y la industria pueden impulsar la adopción exigiendo que los dispositivos cumplan los criterios para su despliegue en entornos de propiedad. Un marco para

[29] Mientras que las prácticas comunes como la BCP 38/84 se discuten ampliamente en relación con los ISP, la tecnología anti-spoofing es necesaria para ser desplegada por cualquier persona que opere su propio espacio de direcciones IP, incluyendo las empresas y otras entidades que proporcionan parte de su propia funcionalidad de red.

[30] Véase Matt Tooley, NCTA - The Internet & Television Association, Communications Sector Coordinating Council, *Libro blanco técnico de la industria sobre botnets y amenazas automatizadas*.

[31] NSTAC. *Informe del NSTAC al Presidente sobre el Internet de las cosas*. 9 de noviembre de 2014. https://www.dhs.gov/sites/default/files/publications/2012-05-15-NSTAC-Cloud-Computing.pdf, Apéndice E, E-5. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

[32] Cyber Independent Testing Lab (CITL). http://cyber-itl.org/.

El despliegue de dispositivos, desarrollado a través de la colaboración público-privada, debería recomendar procesos para la gestión de riesgos y confirmar que las necesidades difieren según la funcionalidad y el contexto. El gobierno debería tomar como modelo el exitoso *marco* del NIST *para mejorar la ciberseguridad de las infraestructuras críticas33*. Se están introduciendo continuamente nuevos servicios para ayudar a gestionar y asegurar los dispositivos de la IO. Los ISP, los proveedores de servicios inalámbricos, los fabricantes de routers, los proveedores de soluciones de seguridad y otros están desarrollando servicios para gestionar la seguridad de los dispositivos IoT. Como se ha señalado anteriormente, los operadores inalámbricos también están colaborando con diversas entidades para sacar al mercado soluciones que ayuden a gestionar la seguridad del IoT. Empresas de antivirus y seguridad como McAfee y Symantec también ofrecen servicios de seguridad para el hogar. [34]Cisco está promoviendo estándares en el IETF, como el estándar MUD (Manufacturer Usage Description) que permite que los dispositivos se autoidentifiquen en el hogar y puede permitir que los routers y las redes apliquen una política de seguridad contra el dispositivo. Se trata de capacidades aún incipientes y podrían complementar los estándares de seguridad en los dispositivos.

Empresas. Las empresas deben planificar y gestionar los dispositivos conectados durante su adquisición, uso y fin de vida. Estas organizaciones tienen muchos usuarios que pueden ser vulnerables a explotaciones poco sofisticadas, pero también pueden beneficiarse enormemente de la educación sobre seguridad. Las empresas también deben adoptar las mejores prácticas para garantizar la redundancia y resistencia de las redes, los datos (como las copias de seguridad para protegerse del ransomware), las ofertas de servicios en la nube y el DNS. Las empresas desempeñan un papel clave en la gestión de su entorno adoptando y exigiendo medidas de seguridad a sus proveedores, y este enfoque puede impulsar mejores normas de seguridad del IoT en todo el ecosistema de Internet.

Aplicaciones/software/OS (véase *la sección 3.4*). El ecosistema requiere un mayor uso de prácticas seguras de desarrollo y gestión de software. Como explica el NIST, "hay muchos enfoques, con distintos niveles de madurez, que resultan muy prometedores para reducir el número de vulnerabilidades en el software". [35]Sin embargo, el uso de las prácticas de desarrollo y gestión de software seguro es desigual, especialmente entre los proveedores de tecnología más pequeños o no tradicionales con menos recursos y menos experiencia. La industria y el gobierno deben promover las mejores prácticas, apoyar a los desarrolladores en las empresas de nueva creación y destacar la comunicación efectiva entre los ingenieros de software y los expertos en seguridad.

3.1 Redes

HALLAZGOS

Las redes desempeñan un papel integral en la defensa contra las redes de bots y los ataques DDoS. Los proveedores de redes adoptan diversas medidas, pero se puede hacer más para hacer frente a las redes de bots y los ataques DDoS.
Uno de los principales retos es fomentar la adopción de las mejores prácticas existentes. El NSTAC identificó las siguientes técnicas empleadas y los retos a los que se enfrenta la industria, y elaboró recomendaciones para resolver estos problemas.

[33] Instituto Nacional de Normas y Tecnología (NIST). *Marco para mejorar la ciberseguridad de las infraestructuras críticas*. 12 de febrero de 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cyb ersecurity-framework-021214.pdf.
[34] Por ejemplo, véase la plataforma doméstica segura de McAfee https://securehomeplatform.mcafee.com
[35] Publicación del NIST ITL. Enero de 2017. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=922589.

Actividades actuales

Los operadores de redes mitigan diariamente miles de amenazas, botnets y ataques DDoS, utilizando herramientas en evolución y enormes recursos para proporcionar a sus clientes y otros usuarios finales una conectividad segura. Por ejemplo, los proveedores implementan normas para evitar la suplantación de identidad, bloquean los vectores de ataque y detectan y mitigan los ataques que se dirigen a un servicio de red o lo afectan. Los proveedores de servicios ayudan a identificar las direcciones IP de origen, filtran/bloquean los correos electrónicos que coinciden con las firmas de las listas negras y filtran/bloquean el tráfico destinado a sitios de phishing. Algunas de las técnicas de seguridad de la red empleadas por los ISP son:

- **Mejor práctica común (BCP)38.** Los principales operadores aplican BCP38 en al menos una parte de sus redes. BCP38 es una práctica del IETF inventada para evitar la suplantación de direcciones IP e impide que los usuarios finales inicien el tráfico con una dirección de origen falsificada. La implementación de BCP38 aumenta la probabilidad de que el tráfico de las redes de bots sea bloqueado porque se originó con una dirección de origen falsificada, o que sea rastreable para que el operador pueda abordar una brecha de seguridad una vez identificada. La mayoría de los grandes ISP incorporan BCP38, y un número creciente de pequeños ISP están empezando a adoptarlo también.

- Bloqueo de **puertos/filtrado/límite de velocidad.** Muchos operadores aplican el bloqueo de puertos, el filtrado y la limitación de velocidad. Estas técnicas se utilizan ampliamente en los servicios de seguridad gestionados para empresas y clientes gubernamentales. Los proveedores de servicios también bloquean ciertos puertos en sus redes troncales que se sabe que contribuyen a los riesgos de seguridad. Aunque hoy en día se bloquean algunos puertos, el cálculo del riesgo de bloquear o bloquear el tráfico en la red de una empresa es diferente al de hacerlo en la Internet pública. A los ISP les preocupan los falsos positivos con respecto al bloqueo en toda la Internet, y es posible que los modelos de bloqueo o filtrado más agresivos no se amplíen. El NSTAC reconoce que puede haber una oportunidad para mejorar estos esfuerzos, pero requeriría una asociación con el gobierno para desarrollar un marco político que apoye a los ISP que toman acciones más agresivas para bloquear y filtrar contenidos. Los ISP son necesariamente conservadores en estas cuestiones, dado el potencial de falsos positivos y el incierto entorno normativo, especialmente teniendo en cuenta la normativa de neutralidad de la red de la FCC. Además, muchos sitios de mando y control aprovechan medios de comunicación legítimos que pueden provocar daños colaterales. Los proveedores de servicios de Internet ya bloquean los puertos que se utilizan ampliamente en los eventos de seguridad. AT&T, por ejemplo, intenta aislar la amenaza y minimizar el daño a la red bloqueando ciertos puertos que transfieren tráfico malicioso o perturbador, como los puertos 25, 135, 139, 445 y 1900.[36] Otros proveedores toman medidas similares. Los proveedores también limitan el tráfico de ciertos protocolos que tienen un uso nominal o limitado, o que normalmente consumen pequeñas cantidades de ancho de banda (por ejemplo, CharGen o NTP), lo que permite el uso normal de dichos protocolos, pero ayuda a mitigar su uso en los ataques DDoS. Cualquier esfuerzo por ampliar estas actividades más allá de los ejemplos anteriores que están siendo claramente aprovechados en los ciberataques requeriría la colaboración con el gobierno para garantizar que se establezca un marco político que apoye estas actividades.

[36] Véase AT&T. *Prácticas de red*. 24 de abril de 2017. https://www.att.com/gen/public-affairs?pid=20879; Xfinity. *Lista de puertos bloqueados de Comcast*. 2017. https://www.xfinity.com/support/internet/list-of-blocked-ports/. CenturyLink http://www.centurylink.com/aboutus/legal/internet-service-disclosure/full-version.html

- Marco de **Ciberseguridad del NIST**. La industria está fomentando el uso del *Marco* del NIST *para mejorar la ciberseguridad de las infraestructuras críticas*, aplicando el marco en cada área funcional básica identificada por el NIST:

  - *Identificar*: identificación de activos críticos, intercambio de información.

  - *Detectar*: muestreo de paquetes, análisis de firmas, análisis heurístico/de comportamiento.

  - *Proteger*: listas de control de acceso, vigilancia, agujeros negros/sumergibles, "depuradores" DDoS, especificación de flujo del Protocolo de Pasarela Fronteriza (BGP), redes de distribución de contenidos, anycast, software antivirus para usuarios finales, servicios de seguridad gestionados para clientes.

  - *Responder y recuperarse*: mitigar el tráfico de ataques, trabajar con los proveedores de servicios de Internet para filtrar y notificar a los clientes. Los ISP bloquean los puertos que se aprovechan en los ataques en curso (por ejemplo, el puerto 445).

- **ABC para los ISP.** La industria anima a adoptar el Código de Conducta Anti-Bot de Estados Unidos para Proveedores de Servicios de Internet desarrollado por el Grupo de Trabajo 7 del CSRIC III. El ABC es un conjunto de prácticas voluntarias que "abordan la amenaza de los bots y botnets en las redes residenciales de banda ancha a través de la participación voluntaria". Hace hincapié en diez principios clave: participación voluntaria; neutralidad tecnológica; neutralidad de enfoque; respeto a la privacidad; cumplimiento legal; responsabilidad compartida; sostenibilidad; intercambio de información; eficacia; y comunicación efectiva con los consumidores. El cumplimiento del ABC requiere la educación del usuario final, la detección de botnets, la notificación al usuario final de una posible infección de botnets, la reparación de botnets y la colaboración de los proveedores de servicios de Internet. Entre los posibles obstáculos a la aplicación se encuentran: las limitaciones tecnológicas (las soluciones actuales pueden ser insuficientes para acabar con las amenazas de las redes de bots o tener consecuencias imprevistas); los obstáculos para los consumidores y el mercado (las soluciones pueden ser consideradas por los clientes como ineficaces o indeseables, como el aumento de los costes para los consumidores); los obstáculos operativos (afectan a la misión principal y a los recursos de la organización); los obstáculos financieros (dificultad para cuantificar los costes/beneficios asociados a las recomendaciones específicas); y los obstáculos legales, normativos o políticos (leyes o políticas que desalientan la colaboración y el intercambio de información).

- **Gestión del tráfico**. Los ISP y los operadores de red invierten mucho en capacidades para gestionar el tráfico. Algunos ejemplos son el bloqueo de puertos, el aprendizaje automático y la IA para ayudar a detectar bots, el filtrado de agujeros negros de destino y el sinkholing de direcciones IP maliciosas.

- **Notificación al consumidor**. Los ISP dedican un tiempo y unos recursos considerables a realizar notificaciones a los consumidores sobre las infecciones, lo que constituye un componente clave de los principios ABC. Sobre la base de los datos agregados proporcionados de forma voluntaria y confidencial al Grupo de Trabajo de Mensajería, Malware y Antiabuso Móvil (M3AAWG), los ISP informantes notificaron entre el 98,41% y el 99,13% de los clientes infectados por bots en 2012 y entre el 94% y el 99,82% de los clientes infectados por bots en 2013. Sin embargo, como se describe a continuación, la utilidad de la educación de los consumidores es limitada, y el impacto de estos esfuerzos en la reducción de la proliferación de malware y botnets es incierto.

- **Colaboración de la industria**. La industria colabora y comparte las mejores prácticas. Por ejemplo, la industria - liderada por el IETF - está explorando soluciones de colaboración

como la señalización de amenazas abiertas DDoS. Los participantes colaboran para identificar los ataques a sus servidores y comparten información para desarrollar respuestas a las amenazas antes de que se produzca un ataque contra otras redes. El intercambio de telemetría en tiempo real entre plataformas de mitigación de DDoS facilita la mitigación de DDoS y la actualización del estado de la red. El reciente informe del Grupo de Trabajo CSRIC V de la FCC sobre el intercambio de información ofrece una visión detallada del intercambio de información en el sector de las comunicaciones. Hay otros esfuerzos en marcha, entre ellos un proyecto piloto entre los principales operadores para cooperar e interrumpir el flujo de tráfico durante un ataque DDoS a gran escala en sus principales puntos de interconexión.

- **Intercambio de información. El sector** participa en el intercambio de información, como se indica en un reciente informe del Grupo de Trabajo 5 del CSRIC V de la FCC. [37] El sector comparte información con compañeros de confianza y socios comerciales; agencias gubernamentales bajo contrato; cuerpos de seguridad; compañeros de la industria como parte del proceso de política y planificación del sector; y, agencias gubernamentales como el Centro de Coordinación Nacional del DHS y el Centro Nacional de Integración de Ciberseguridad y Comunicaciones (NCCIC). [38] El DHS también gestiona la Red Internacional de Vigilancia y Alerta en colaboración con el Departamento de Estado para compartir información a nivel internacional.

- **Redes definidas por software/reparto de redes/virtualización.** Los desarrollos arquitectónicos, como la 5G, la transición a las redes totalmente IP y la aparición de las redes definidas por software (SDN) y la virtualización promoverán la seguridad. La SDN es una arquitectura emergente que desvincula las funciones de control y reenvío de la red, permitiendo que el control de la red sea directamente programable. Esta arquitectura, combinada con interfaces abiertas y fácilmente programables, facilita la combinación de soluciones de distintos proveedores y el desarrollo de nuevas capacidades. Aunque cualquier nuevo enfoque tiene el potencial de verse comprometido, la SDN ayudará a los operadores a responder a las amenazas gracias a la visión centralizada de la red por parte del operador. La fragmentación de la red permitirá a los operadores de redes 5G proporcionar redes como servicio. Con la fragmentación de la red, una sola capa física puede dividirse en múltiples redes virtuales, lo que permite a los operadores ofrecer diferentes servicios a distintos clientes. Los servicios incluyen filtrado, enrutamiento, limitaciones de protocolo y limitación de velocidad. Los operadores pueden personalizar la seguridad de los segmentos de red para responder de forma dinámica. La virtualización de la red incluye seguridad integrada, como aislamiento y multitenencia, segmentación, cortafuegos de distribución e inserción y encadenamiento de servicios. [39]

- **Servicios de seguridad gestionados/seguridad del consumidor.** Muchos ISP ofrecen servicios de seguridad gestionada, como los servicios de defensa contra DDoS, a los clientes empresariales consumidores para ayudarles a gestionar los riesgos de seguridad. En el lado del consumidor, los ISP ofrecen notificaciones de posibles infecciones, servicio antivirus gratuito proporcionado junto con el servicio de banda ancha residencial, soporte técnico para ayudar a la reparación, entre otras capacidades. A nivel empresarial, los ISP ofrecen servicios de seguridad y de supervisión y gestión de la red a los sectores privado y público.

[37] FCC CSRIC V, Informe final del grupo de trabajo 5, *Intercambio de información,* 15 de marzo de 2017. https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf.
[38] Ibid, página 6.
[39] Bill O'Hern. AT&T, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 20 de julio de 2017.

Desafíos

Estas soluciones existentes plantean varios problemas:

- **Marco legal para la gestión de redes.** Muchas técnicas para la Internet pública o el espacio de los consumidores implican soluciones como el bloqueo, el black holing o el sinkholing de direcciones IP, el bloqueo de puertos aprovechados para el tráfico malicioso, la notificación a los clientes usuarios finales de posibles infecciones y el despliegue de prácticas comunes anti-spoofing de direcciones IP, como la BCP 38/84. Uno de los retos de estos enfoques es la posibilidad de que se produzcan falsos positivos y consecuencias no deseadas. Para solucionar eficazmente estos problemas sería necesario que los proveedores de servicios de Internet adoptaran medidas más agresivas de supervisión e inspección del tráfico, lo que plantea problemas de política. Por ejemplo, aunque había una excepción de seguridad en las anteriores normas de neutralidad de la red de la FCC, la expectativa general de que los ISP no interfieran en el flujo de tráfico aumenta los riesgos relacionados con algunas actividades.

- **Encriptación**. Los ISP pierden visibilidad a medida que se encripta más tráfico. Hoy en día, la mayor parte del tráfico en Internet está cifrado. Y para los operadores de redes de bots es muy sencillo cifrar el tráfico de las mismas. Un experto predijo que a finales de 2016, más de dos tercios del tráfico de Internet estarían cifrados. [40] Aunque los ISP pueden tener cierta visibilidad de los datos de flujo de red, como la dirección IP de origen y destino, es poco probable que los ISP tengan una amplia visibilidad de la carga útil que puede ser necesaria para un bloqueo agresivo.

- **Protocolo de Internet versión 6 (IPv6).** Los operadores que utilizan redes con IPv6 necesitan herramientas de seguridad, detección y supervisión. Debido a los desafíos de seguridad únicos que introduce IPv6, el ecosistema debe madurar el soporte de seguridad para IPv6, mejorar las herramientas de detección y descubrimiento de activos para identificar los dispositivos IPv6 falsos y garantizar que la supervisión de la red sea compatible con los activos de la red IP Versión 4 e IPv6.

- **Escalabilidad.** Persisten las dudas sobre si las soluciones funcionarán a gran escala. En las empresas, los ISP supervisan los rangos de direcciones IP correspondientes a sus clientes empresariales para identificar, detectar y frustrar los ciberataques. No está claro si las soluciones más granulares para el conjunto de Internet serán escalables, ya que las grandes redes transportan enormes cantidades de tráfico en un día determinado. [41]

- **Transportistas de tamaño pequeño/mediano**. Hay que distinguir entre las organizaciones grandes y las pequeñas y su capacidad para aplicar el BCP38 u otras medidas de seguridad. Las pequeñas empresas pueden necesitar financiación del servicio universal para una seguridad eficaz. Las empresas que venden servicios de Internet con poco margen y carecen de modelos de ingresos para cubrir las inversiones en seguridad se enfrentan a importantes retos. El NSTAC recomienda que el gobierno vuelva a examinar la cuestión de los incentivos para la implantación, en particular para las compañías pequeñas y medianas, donde incluso una inversión marginal puede requerir incentivos para dichas entidades.

- **Notificaciones a los consumidores**. Muchos ISP tienen programas de notificación, pero se desconoce la eficacia general de estos programas. Incluso cuando los consumidores reciben una notificación de

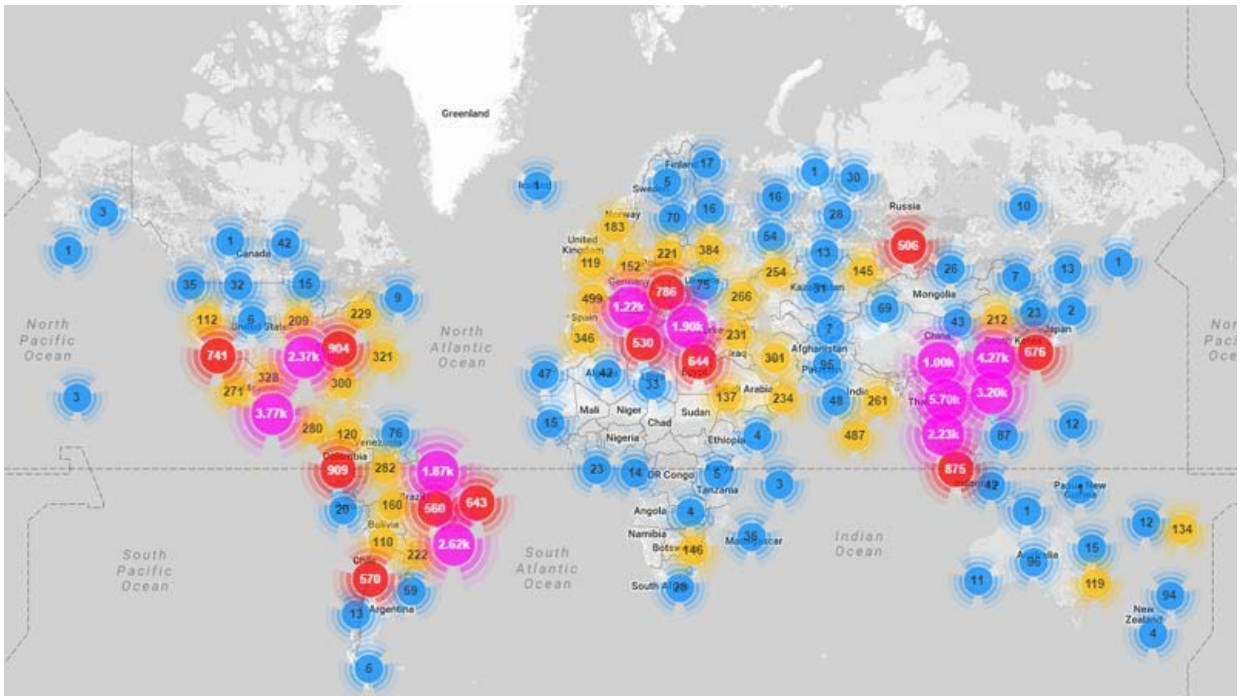
[40] Sandvine. *Fenómenos globales de Internet: Tráfico de Internet encriptado*. 2016. https://www.sandvine.com/reso urces/global-internet-phenomena/spotlight/internet-traffic-encryption.html.

[41] Bill O'Hern. AT&T, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 20 de julio de 2017. Por ejemplo, más de 168 petabytes viajan diariamente por la red de AT&T.

de seguridad, muchos carecen de los conocimientos necesarios para limpiar sus sistemas. También hay una alta tasa de reinfección, porque los consumidores suelen repetir el comportamiento que corrompió su dispositivo en primer lugar.

- **Internacional**. Los ataques de botnets contra Estados Unidos se originan en gran medida en el extranjero. Por ejemplo, el siguiente mapa muestra las fuentes de tráfico de un ataque de la red de bots Mirai el 17 de agosto de 2016, que fueron predominantemente fuera de Estados Unidos.

Figura 6. Fuentes de tráfico para un ataque de la red de bots Mirai 17 de agosto de 2016



Fuente: Brian Rexroad. AT&T. Sesión informativa para el subcomité ICR del NSTAC. 20 de julio de 2017.

Otros temas

El NSTAC abordó otras cuestiones relativas a la seguridad de los ISP, como el despliegue de las extensiones de seguridad del DNS (DNSSEC) y el enrutamiento seguro entre dominios. Es posible que DNSSEC no sea una solución viable, ya que fue útil al principio pero a medida que la red evolucionó DNSSEC no se implementó de forma óptima, lo que disminuyó su eficacia. Los ISP se enfrentan a ataques de amplificación, y señalan que varios marcos de seguridad se basan en la infraestructura y la validación de claves. El control de admisión a la red y la protección de acceso ayudan a imponer la validación antes de acceder a la red. El principal problema es la confianza y la reputación, ya que cada paquete en la red conlleva un grado de riesgo.

El NSTAC también revisó los problemas del Sistema de Señalización 7 (SS7). [42] Aunque el SS7 recibió una atención considerable, el SS7 en sí no es el problema. La cuestión es más bien la interconexión y el acceso inadecuado. (Véase CSRIC V, WG10 (marzo de 2017) y el informe del 3 de mayo de 2017 sobre SS7/2FA). El sector sigue luchando contra los operadores deshonestos que son cómplices de comportamientos delictivos,

[42] Travis Russell. Oracle. *Sesión informativa para el subcomité ICR del NSTAC.* 11 de agosto de 2017.

vender identificadores de red y autenticación a los malos actores. La industria está trabajando para mejorar la investigación de los socios de interconexión (o itinerancia) y mejorar la higiene de la red.

Otra cuestión es la seguridad del enrutamiento BGP. Esto incluye la preocupación por las entidades que publican rutas falsas en Internet que pueden ser explotadas para enrutar el tráfico y permitir a las entidades controlar el tráfico o realizar otro tipo de vigilancia. Hasta la fecha, la solución a este problema se ha centrado en el desarrollo de una Infraestructura de Clave Pública de Recursos (RPKI) que permita a los ISP y a otras entidades validar las rutas. El Centro Nacional de Excelencia en Ciberseguridad (NCCoE) del NIST ha puesto en marcha recientemente un proyecto piloto de enrutamiento seguro entre dominios para explorar varias cuestiones en torno al desarrollo de la RPKI, en el que participan numerosos ISP.

RECOMENDACIONES PARA LOS PROVEEDORES DE SERVICIOS DE RED

- **Compartir información sobre las amenazas. La** colaboración de los ISP debe incluir el intercambio de información sobre detección, notificación y métodos de mitigación planificados o utilizados en la red.

- **Aumentar el análisis del tráfico.** Muchos ISP realizan análisis, pero deberían incorporarse a servicios de seguridad gestionados más robustos para ayudar a las empresas a gestionar posibles ataques DDoS.

- **Adaptar y aplicar el aprendizaje automático para la detección de anomalías.**

- **Garantizar que los operadores de red puedan filtrar el tráfico malicioso.**

- **Fomentar el desarrollo de prácticas que permitan mitigar el tráfico DDoS lo más cerca posible de la fuente para evitar que transite por las redes.**

- **Ampliar el uso de BCP38/84 más allá de los ISP para incluir a las empresas.**

- **Continuar con la aplicación del bloqueo de puertos, la limitación de la velocidad y el filtrado cuando sea necesario.**

- **Continuar participando en los esfuerzos de la industria para aumentar la seguridad de BGP.**

3.2 Consumidores/Esquema/Dispositivos

HALLAZGOS

Los puntos débiles en el borde de las redes, en los dispositivos que se conectan a ellas y en los usuarios que compran y utilizan los dispositivos impulsan la inseguridad. El NSTAC tuvo en cuenta en su investigación tanto a los consumidores como a los dispositivos de borde.

Los consumidores desempeñan un papel fundamental. El error humano puede socavar la inversión de la industria en soluciones técnicas y de software. Muchos ataques siguen desplegando eficazmente métodos de baja tecnología, como el phishing, y los malos actores se aprovechan de la escasa higiene cibernética para lanzar ataques de redes de bots. El 70% de los hackeos utilizan credenciales perdidas, robadas o débiles; el 60% de todo el malware utiliza la escalada de privilegios o

credenciales robadas. [43] Las recomendaciones del CSRIC de la FCC hacían hincapié en la importancia de educar a los usuarios finales sobre las medidas de protección, como contraseñas seguras, software antivirus, cortafuegos y aceptación de actualizaciones. [44] El gobierno tiene recursos para educar a los consumidores, sin embargo, los mensajes pueden perderse en la gran cantidad de páginas de consejos, avisos de la Oficina Federal de Investigación (FBI) y otras comunicaciones que existen.

Los usuarios pueden ignorar la seguridad a la hora de tomar decisiones de compra y pueden no instalar o configurar los dispositivos adecuadamente. Los usuarios finales pueden no cambiar las contraseñas o utilizar las herramientas de seguridad disponibles y pueden ignorar las actualizaciones disponibles. Además, es posible que los usuarios no borren los datos personales o la configuración de los dispositivos cuando los sustituyen. Los usuarios pueden no tener suficiente información, pero también pueden ignorar la información disponible. Una encuesta realizada por el Pew Research Center reveló que el 28% de
Los propietarios de teléfonos inteligentes estadounidenses no aseguraron el acceso a su dispositivo con un simple número de identificación personal de cuatro dígitos u otra característica de seguridad. [45] Aunque la mayoría de los usuarios de teléfonos inteligentes afirman que actualizan las aplicaciones o el sistema operativo de sus dispositivos, aproximadamente el 40 por ciento dijo que retrasaba las actualizaciones hasta que era conveniente. [46] El estudio reveló que el 14% de los usuarios de teléfonos inteligentes nunca ha actualizado el sistema operativo de su dispositivo y el 10% nunca ha actualizado sus aplicaciones. [47] La falta de higiene no es exclusiva de los usuarios comerciales: los usuarios de la administración pública también deben mejorar la ciberhigiene. Las agencias pueden estar limitadas por la escasez de recursos, y el gobierno debe tener en cuenta los costes de sus futuras necesidades de seguridad. La OE 13800 subraya adecuadamente la rendición de cuentas y la responsabilidad de los jefes de los organismos. [48]

Los dispositivos son críticos. Muchos dispositivos se desarrollan con pocas capacidades de seguridad, ya que algunos proveedores no prestan la debida atención a las cuestiones de seguridad. El ataque de la red de bots Mirai explotó más de un millón de cámaras con contraseñas y credenciales débiles. [49] Los dispositivos pueden tener contraseñas por defecto inalterables, lo que los hace fácilmente explotables, o pueden ser incapaces de soportar actualizaciones, lo que hace más difícil llevar a cabo la gestión de parches en caso de una vulnerabilidad de seguridad. La Comisión Federal de Comercio (FTC) señaló que la seguridad de los dispositivos variará, pero está surgiendo un cierto consenso sobre las características sensatas. [50] Con unas expectativas de 28.000 millones de

[43] Ann Cox. DHS. *Sesión informativa para el Subcomité ICR del NSTAC*. 2 de agosto de 2017.

[44] FCC. CSRIC II, Grupo de Trabajo 2A: Informe final. *Cyber Security Best Practices*. en 91. Marzo de 2011. https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

[45] Kenneth Olmstead y Aaron Smith. "Los estadounidenses y la ciberseguridad". *Informe del Centro de Investigación Pew*. en 19. 26 de enero de 2017. http://assets.pewresearch.org/wpcontent/uploads/sites/14/2017/01/26102016/ Americans-and-Cyber-Security-final.pdf.

[46] Ibid. en 20.

[47] Ibid.

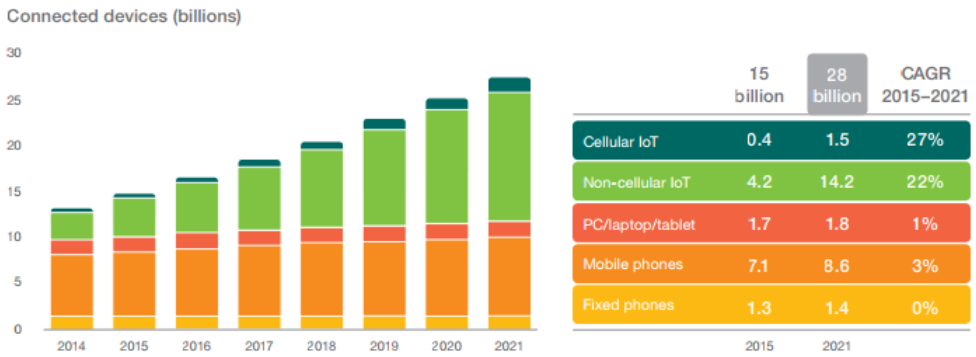
[48] Oficina del Secretario de Prensa de la Casa Blanca. *Orden ejecutiva 13800, Fortalecimiento de la ciberseguridad de las redes federales y la infraestructura crítica*. 16 de mayo de 2017. https://www.federalregister.gov/documents/2017/05/16/ 2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

[49] Lorenzo Franceschi-Bicchierai, *How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet.* 29 de septiembre de 2016. https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected- cameras-ddos-botnet-brian-krebs.

[50] Thomas B. Pahl. FTC. Empezar *con la seguridad - y seguir con ella*. 28 de julio de 2017. https://www.ftc.gov/news- events/blogs/business-blog/2017/07/start-security-stick-it ("Cuando se trata de la seguridad de los datos, lo que es razonable dependerá del tamaño y la naturaleza de su negocio y del tipo de datos que maneja"); Internet de
Cosas: Privacidad y seguridad en un mundo conectado. FTC. n.130. Enero de 2015. https://www.ftc.gov/system/ files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet- things-privacy/150127iotrpt.pdf ("Puede haber otras medidas adecuadas, como las medidas de seguridad que un

conexiones para 2021, y el 73% del tráfico mundial de Internet es [móvil51] , las redes o las personas por sí solas no podrán proporcionar seguridad a todos estos dispositivos.

Figura 7. Crecimiento de los dispositivos conectados



Fuente: Informe de movilidad de Ericsson (junio de 2016)[52]

La militarización de los dispositivos del IoT supone un reto importante. Los dispositivos mal protegidos y siempre encendidos, comprometidos por redes de bots, podrían tener consecuencias catastróficas. Los proveedores de IoT y sus usuarios finales a veces son apáticos al daño que pueden causar los dispositivos vulnerables, y pueden tener pocos incentivos para invertir en seguridad más allá de lo necesario para garantizar el funcionamiento del dispositivo.

La IO debe admitir actualizaciones y un sistema de autenticación y validación. [53 Los] nuevos protocolos maliciosos pueden derrotar a los modelos de seguridad anticuados, por lo que es necesario actualizar la seguridad más antigua. Los proveedores de servicios de red pueden ayudar a gestionar los dispositivos no seguros de la red, pero hay factores que complican la situación. Por ejemplo, aproximadamente el 70% del tráfico de Internet a nivel mundial está cifrado, y se espera que esta cifra aumente. [54]Para aumentar la complejidad, muchos dispositivos de los consumidores no son direccionables públicamente y operan detrás de routers domésticos y sistemas de traducción de direcciones de red que no son gestionados por los ISP. Los usuarios suelen tener varios routers. Algunas empresas, como los ISP y los proveedores de soluciones de seguridad, están experimentando con servicios de gestión de la seguridad, pero el potencial del mercado es incierto.

La seguridad no se limita a la capa de los dispositivos. No podemos confiar únicamente en la construcción de la seguridad en los dispositivos para abordar la seguridad. Por ejemplo, los proveedores de redes pueden realizar análisis del tráfico que atraviesa sus redes y aplicar el aprendizaje automático para ayudar a identificar y mitigar las amenazas a

La empresa debería aplicarlos en función de los riesgos que presenta el acceso no autorizado al dispositivo y de la sensibilidad de la información recogida").

[51] Informe de movilidad de Ericsson. *En el pulso de la sociedad en red*. Junio de 2016. https://www.ericsson.com/res/ docs/2016/ericsson-mobility-report-2016.pdf; Cisco. *Índice de redes visuales de Cisco: Previsión y metodología, 2016-2021.* Libro blanco. 7 de junio de 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/ visual-networking-index-vni/complete-white-paper-c11-481360.html.

[52] Informe de movilidad de Ericsson. *En el pulso de la sociedad en red*. Junio de 2016. https://www.ericsson.com/res/docs /2016/ericsson-mobility-report-2016.pdf.

[53] Raj Samani. McAfee, Reino Unido. *Sesión informativa para el subcomité ICR del NSTAC.* 15 de agosto de 2017.

[54] Véase Sandvine. *Fenómenos globales de Internet: Tráfico de Internet encriptado*. 2016. https://www.sandvine.com/reso urces/global-internet-phenomena/spotlight/internet-traffic-encryption.html.

algunos dispositivos IoT. También ha habido propuestas como el estándar MUD de Cisco, que se está introduciendo en el IETF. El MUD permitiría a los dispositivos autoidentificarse y ser colocados por los routers y otros equipos de red en distintas clases de servicio aplicando límites de tarifa y listas blancas para gestionar la seguridad. Además, empresas como McAfee están empezando a ofrecer servicios de gestión de la seguridad de los dispositivos domésticos. Estos esfuerzos están en sus inicios, pero pueden mejorar la seguridad a medida que el mercado evoluciona.

La **cadena de suministro también es importante**. Los operadores están mejorando las defensas, pero no pueden hacerlo solos. Los fabricantes de chips y los proveedores de plataformas deben aumentar sus esfuerzos y el ecosistema debe promover las nuevas mejoras de seguridad "atornilladas" a las redes domésticas. La industria y el gobierno deben centrarse en el marketing de seguridad, reconocer las responsabilidades compartidas y fomentar el trabajo en equipo.

El NSTAC reconoce que existen diversas opiniones sobre el papel del gobierno en la seguridad de la IO. Sin embargo, está claro que hay que centrarse en mitigar estas vulnerabilidades.

Actividades actuales

Se están desarrollando numerosas innovaciones para abordar la capa del usuario final y del dispositivo. Los fabricantes de chips y los proveedores de plataformas están incorporando seguridad adicional a los dispositivos IoT poco sofisticados. [55] Como explicó la Consumer Technology Association (CTA):

- El Instituto de Investigación Colaborativa de Intel para la Computación Segura ha desarrollado un marco de seguridad TrustLite para mejorar la seguridad de los pequeños dispositivos IoT. [56]
- Los Field Programmable Gate Arrays o Systems on a Chip de Altera utilizan la aceleración criptográfica por hardware y las actualizaciones de software remotas protegidas por AES.
- Los productos IoT de Analog Devices utilizan aceleración de hardware criptográfico, arranque seguro y protección de lectura de la memoria en el circuito.
- Apple, Qualcomm, Samsung Electronics y otros utilizan chips con TrustZone de ARMS.
- Las plataformas de IoT de IBM, Microsoft, Intel, NXP, Panasonic y Samsung llevan incorporada la seguridad o una guía de seguridad para los implementadores.

Los dispositivos de monitorización de red (NMD) de consumo y los routers inteligentes son cada vez más frecuentes. Los NMD de consumo contienen especificaciones que incluyen el modo de red privada virtual (VPN), protección contra ataques DoS, bloqueo de accesos no autorizados y escaneo de virus y malware. Los routers inteligentes vienen ahora con características similares. La industria está diseñando hardware capaz de proporcionar actualizaciones de seguridad "atornilladas" a las redes domésticas de los consumidores.

La industria ofrece varias herramientas a los clientes para ayudar a proteger los dispositivos. Entre ellas se encuentran el suministro de herramientas antivirus a los consumidores para ayudar a detectar virus y limpiar las máquinas; el análisis de amenazas de un

[55] Mike Bergman. Asociación de Tecnología de Consumo. *Sesión informativa para el subcomité ICR del NSTAC*. 3 de agosto de 2017.
[56] Koeberl, Patrick, et, al. "TrustLite: A Security Architecture for Tiny Embedded Devices". http://www.icri-sc.org/fileadmin/user_upload/Group_TRUST/PubsPDF/trustlite.pdf

perspectiva de la red; notificar a los usuarios finales y proporcionar herramientas de autorremediación y opciones de atención de pago; y proporcionar un servicio de mitigación de DDoS para los clientes suscritos.

Existen directrices voluntarias y mejores prácticas para mitigar las vulnerabilidades de los dispositivos y aumentar la concienciación de los consumidores, y la industria también está aprovechando estos esfuerzos.

- La Asociación de Móviles del Grupo (GSMA), por ejemplo, ha elaborado orientaciones para el desarrollo de productos y servicios seguros de IoT, incluso para los fabricantes de dispositivos de punto final de IoT. [57]

- La CTA está desarrollando buenas prácticas para mejorar la seguridad de los dispositivos conectados en el hogar. [58]

La industria está trabajando con el gobierno para proporcionar recursos para la seguridad de la IO en la etapa del usuario final. Por ejemplo, los miembros de la industria están colaborando con la NTIA en un proceso de múltiples partes interesadas para desarrollar un léxico común para la mejora de la IO. Como parte de ese proceso, los grupos de trabajo han identificado orientaciones sobre el tema de más de 30 organizaciones estadounidenses e internacionales,[59] características para asegurar las actualizaciones por aire, y orientaciones para comunicar sobre la capacidad de actualización del IoT a los consumidores.

RECOMENDACIONES PARA LOS CONSUMIDORES/BORDE/DISPOSITIVOS

- **Establecer y promover directrices consensuadas de seguridad de los dispositivos**. Los dispositivos deben ser reforzados con prácticas básicas de ciber higiene, incluyendo la capacidad de recibir actualizaciones y parches. Varios esfuerzos gubernamentales buscan aumentar la higiene de la ciberseguridad, pero se necesita más. [60] El gobierno y la industria deben determinar si es necesario desarrollar expectativas mínimas de seguridad. Los fabricantes de dispositivos, en particular los de kits de desarrollo de dispositivos IoT, deben garantizar que se incluyan buenas herramientas y que se utilicen configuraciones seguras por defecto, parches automáticos y la capacidad de recuperarse de las infecciones de malware. [61]

- **Promover los servicios de gestión del hogar**. El gobierno debería apoyar la inversión de la industria en servicios de gestión del hogar, que supervisarían las operaciones de los dispositivos conectados dentro del hogar. Esta capacidad podría ofrecerse en los routers o como un dispositivo independiente dentro del hogar.

- **Promover la concienciación/educación de los consumidores**. La industria debe seguir educando a los usuarios, incluso sobre la importancia de completar las actualizaciones. El gobierno debe ampliar y

[57] Véase GSMA IoT Security Guidelines. https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/.
[58] Asociación de Tecnología de Consumo. *Resumen del proyecto: Securing Connected Devices for Consumers in the Home*. CTA-CEB33. 7 de julio de 2017. https://standards.cta.tech/apps/group_public/project/details.php?project_id=429.
[59] Véase NTIA. *Catalog of Existing IoT Security Standards (Draft Version 0.01), NTIA Multistakeholder Process on IoT Security Upgradability and Patching, Existing Standards, Tools, and Initiatives Working Group*. Julio de 2017. https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.
[60] Arabella Hallawell. Arbor Networks, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 3 de agosto de 2017.
[61] Véase el borrador del NIST. Publicación especial 800-193. *Directrices de resiliencia del firmware de la plataforma.* Mayo de 2017. https://csrc.nist.gov/csrc/media/publications/sp/800-193/draft/documents/sp800-193-draft.pdf

coordinar sus mensajes. Hay campañas existentes, como STOP.THINK.CONNECT, que pueden utilizarse para este fin.

- **Apoyar un mayor intercambio de información**. El gobierno debe fomentar el intercambio de información entre los fabricantes de dispositivos, incluidos los puertos seguros y la protección de la responsabilidad.

3.3 Empresa

HALLAZGOS

Los usuarios y sistemas de las empresas desempeñan un papel fundamental. Las empresas -compañías con cientos de miles de dispositivos, organismos gubernamentales cuyos integrantes dependen de la conectividad, pequeñas empresas que despliegan sensores industriales y traen su propio dispositivo (BYOD)- se ven afectadas por las redes de bots de dos maneras. En primer lugar, las empresas son objeto de ataques de botnets. En segundo lugar, las empresas tienen concentraciones de dispositivos IoT que podrían ser aprovechados como parte de una red de bots global si se dejan vulnerables.

Durante años, los adversarios han utilizado los ataques DDoS con redes de bots para interrumpir las operaciones de las empresas. Las empresas pueden ser el objetivo de ataques DDoS debido a que los estados nacionales tienen como objetivo la infraestructura de los Estados Unidos, los hacktivistas tratan de hacer una declaración, los delincuentes distraen de los ataques más insidiosos, u otras empresas que tratan de interrumpir la competencia. A medida que la TI, las infraestructuras físicas y la continuidad del negocio de las empresas dependen de los dispositivos habilitados para IP, las empresas se vuelven más susceptibles a la inhabilitación a largo plazo o permanente de sus operaciones; lo que algunos llaman "destrucción del servicio". Incluso si las empresas no son ellas mismas el objetivo de las redes de bots, sus dispositivos vulnerables pueden servir de puerta de entrada para la penetración en sus redes, el robo de datos de gran valor e incluso la destrucción de las infraestructuras operativas y de TI desde dentro. Los propios dispositivos IoT de una empresa pueden ser utilizados para lanzar un ataque DoS contra la propia empresa debido a la proliferación de dispositivos conectados en casi todas las redes empresariales.

El gran número de dispositivos dificulta el seguimiento de los mismos por parte de las organizaciones, aumentando el riesgo de robo y dejando los dispositivos vulnerables a los ataques. Las empresas de todos los tamaños deben gestionar más puntos de interacción en sus redes, incluidas las VPN, para facilitar el acceso fuera de las instalaciones. Este aumento de la conectividad expone a las empresas a amenazas adicionales, incluidas las procedentes de dispositivos cuya seguridad puede no ser sofisticada. La necesidad de aprovisionar, supervisar, actualizar y gestionar el final de la vida útil de los dispositivos puede suponer un reto mayor del que pueden asumir los departamentos de TI de las empresas.

La amenaza de las redes de bots para las empresas va más allá de los ataques a los dispositivos. Un reto importante es la protección contra los ataques a los recursos compartidos que la empresa utiliza para llevar a cabo sus actividades. Dado que los servicios de las empresas abarcan su red de TI interna, las ofertas en la nube y los recursos compartidos, deben protegerse contra un incidente que afecte al negocio en uno de esos servicios. Por ejemplo, la presencia en Internet de muchas empresas se desconectó cuando sus servicios DNS se interrumpieron durante el ataque Mirai a Dyn en octubre de 2016.

Las empresas pueden desempeñar un papel importante en la mitigación de las amenazas de botnets. Los despliegues de IoT de las empresas dentro de las redes internas deberían ser más manejables con la aplicación de tecnologías de seguridad apropiadas que estén en consonancia con los riesgos identificados. Para reducir el riesgo de la empresa, estas capacidades de seguridad deben ofrecerse de forma coherente en toda la cadena de valor del IoT para permitir la

visibilidad y automatización necesarias para que las empresas eviten que las ciberamenazas se dirijan a los elementos conectados, y protejan las redes y los entornos de los controladores de los ataques iniciados por los dispositivos. Estas capacidades deben estar integradas de forma nativa, con altos niveles de automatización en todas las funciones para identificar rápidamente los ataques avanzados y garantizar que los controles de seguridad preventivos puedan aplicarse en todos los entornos en tiempo casi real. En el contexto de los despliegues del IoT, la prevención de las ciberamenazas en toda la cadena de valor del IoT de la empresa requiere como mínimo (1) la seguridad de los puntos finales; (2) la seguridad de las redes locales; (3) la seguridad dentro de las redes de los proveedores de servicios asociados; y (4) la seguridad de los entornos de la nube y de los controladores de host de IoT.

Como ejemplo, el Cuerpo de Marines adopta un enfoque agresivo de la gestión empresarial. [62] El Cuerpo de Marines rastrea cada dispositivo que intenta conectarse a su red, y se asegura de que el dispositivo esté totalmente parcheado y cumpla con los protocolos de seguridad antes de conectarse. El Cuerpo de Marines mantiene una política estricta para los dispositivos personales. Cuando se permite el BYOD, los dispositivos se colocan en contenedores virtuales para proteger los datos del dispositivo y la red gubernamental. Los Marines también se aseguran de que los usuarios tengan los privilegios mínimos para llevar a cabo sus responsabilidades, utilizan la autenticación de dos factores y auditan a los usuarios para cada creación, modificación y eliminación de archivos.
Aunque este enfoque es más agresivo de lo que pueden hacer la mayoría de las empresas, muestra los pasos que podrían tomarse como parte de un programa para proteger a las empresas de las redes de bots y otras amenazas. [63]

Una de las conclusiones del NSTAC es que los dispositivos IoT tienen una amplia gama de características y capacidades. Dentro de un entorno empresarial, algunos activos de IoT de alto valor que tienen capacidades de procesamiento avanzadas, como los automóviles, pueden conllevar un grado de riesgo de ciberseguridad que hace viable el despliegue de una solución de seguridad de punto final dedicada. Sin embargo, muchos otros dispositivos IoT de la empresa carecen de potencia de cálculo individual y, en su lugar, dependen de las funciones de mando y control de los hosts controladores para el cumplimiento de la seguridad. Además, un gran porcentaje de plataformas y controladores de IoT empresariales dependen de la conectividad en la nube, que puede estar alojada en centros de datos internos, nubes públicas o entornos de proveedores de servicios. Una seguridad coherente y bien integrada en todas estas plataformas y controladores, independientemente de su ubicación, es fundamental para evitar el compromiso y la ejecución de actividades de mando y control no autorizadas que podrían aprovechar grandes franjas de dispositivos IoT empresariales para ataques automatizados y distribuidos.

Las innovaciones prometedoras están preparadas para ayudar a las empresas: La SDN y la virtualización de las funciones de red (NFV), así como otros enfoques, perfeccionarán la arquitectura y la organización de los sistemas y permitirán adoptar medidas de seguridad creativas. La SDN ofrecerá varias ventajas a la seguridad de las empresas:

- Control centralizado: ofrece un punto de vista de seguridad mejorado;
- Gestión: la gestión de la seguridad mejora con la visibilidad total de la red;
- Aplicaciones: Las aplicaciones SDN proporcionan funciones nativas de control de la seguridad;
- Recogida de datos: la recogida y el análisis nativos ofrecen una respuesta mejorada.

[62] Ray Letteer. Cuerpo de Marines de los Estados Unidos. *Sesión informativa para el subcomité ICR del NSTAC*. 29 de agosto de 2017.
[63] Ibid.

- Eficiencia: La SDN permite un reencaminamiento y cambios de infraestructura más inmediatos (Dynamic Enforcement). [64]

La NFV también es prometedora. El Instituto Europeo de Normas de Telecomunicación65 explica que la NFV en la 5G soportará la fragmentación de la red, que consiste en la creación de múltiples instancias lógicas de red (es decir, cortes) en la misma red, que pueden aprovecharse para desplegar y gestionar cortes de red de forma automatizada y flexible. Los principios de diseño nativo de la nube maximizan el uso eficiente de los recursos de la empresa a través de una multiplexación más fina en la infraestructura.
La gestión de servicios de extremo a extremo, es decir, la habilitación de diferentes ofertas de servicios para diferentes clientes, permite a los clientes seleccionar los componentes básicos del servicio de red que mejor se adapte a sus necesidades. La computación de borde, con sistemas altamente distribuidos, permite que las funciones de red se ejecuten en los servidores más cercanos al dispositivo del usuario final, es decir, en el "borde" de la arquitectura de red. Se espera que la nubificación de la red de acceso radioeléctrico proporcione a los operadores una capacidad sin precedentes en términos de flexibilidad, agilidad, gestión de recursos/servicios y orquestación. Los servicios multisitio/dominio, incluido el soporte de la Infraestructura como Servicio, la NFV como Servicio y la composición del Servicio de Red en diferentes dominios administrativos es fundamental en la transición a la 5G. Gestión de licencias NFV, la estandarización de los mecanismos de gestión de licencias subyacentes evitaría agravar la complejidad de las licencias. Estas innovaciones promueven la seguridad, la fiabilidad y la escalabilidad en la seguridad empresarial.

Las empresas deben establecer algunos objetivos claros para hacer frente a estos riesgos, entre ellos los siguientes

Mitigar el riesgo de los ataques de botnets tradicionales contra las redes de las empresas. Las empresas deben explorar todos los métodos disponibles para mitigar el riesgo de ataques de botnets tradicionales dirigidos a sus redes. Esto incluye trabajar con los proveedores de servicios de Internet para implantar defensas a nivel de red, como el bloqueo de puertos, el enrutamiento del flujo de tráfico y la lucha contra la suplantación de identidad y otras metodologías de atribución antes de los ataques DoS. Muchas empresas recurren a sus proveedores de red para que les proporcionen controles o funcionalidades como parte de los servicios de seguridad gestionados que pueden restringir la comunicación de los dispositivos con dominios ajenos a los controladores autorizados y habilitar soluciones de seguridad avanzadas como cortafuegos basados en aplicaciones con el apoyo de grandes cantidades de inteligencia dinámica sobre amenazas.

Asegúrese de que los dispositivos tienen seguridad integrada en el momento de la compra y durante su ciclo de vida. Las empresas pueden tomar varias medidas para garantizar que los dispositivos conectados funcionen de forma segura en sus redes. Estos pasos incluyen considerar la seguridad de los dispositivos en el momento de la compra; hacer a los proveedores potenciales una serie de preguntas sobre cómo los proveedores aseguran los dispositivos, incluyendo cómo autenticar a un dispositivo y cómo parchear o actualizar un dispositivo; y potencialmente hacer que los dispositivos sean probados por una organización independiente. Muchas empresas tienen un importante poder adquisitivo y pueden impulsar una mejor seguridad general durante las fases de diseño y producción del ciclo de vida del desarrollo de los dispositivos.

Tras la implantación, las empresas deben conocer y emplear todos los métodos disponibles para evitar que los dispositivos sean reclutados (o utilizados para atacar sus propias redes). A la hora de asegurar los dispositivos en sus redes, las consideraciones más importantes para las empresas son: la detección (la capacidad de

[64] Bill O'Hern. AT&T, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 20 de julio de 2017.
[65] Grupo de Especialización de la Industria NFV del ETSI. *Perspectivas de los operadores de red sobre las prioridades de la NFV para la 5G*. 21 de febrero de 2017. https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf

detectar todos los dispositivos conectados en tiempo real), la segmentación (la capacidad de segmentar o "amurallar" los puntos finales de otras partes de sus redes, y la automatización (la capacidad de que las soluciones seleccionadas funcionen de forma automatizada), que son fundamentales para lograr la escala a medida que el número de dispositivos conectados aumenta exponencialmente. Existen diversas opciones que ofrecen estas características, como herramientas que permiten a las empresas una autenticación sólida de los dispositivos; herramientas que permiten elaborar perfiles de comportamiento de los dispositivos (la capacidad de detectar comportamientos anormales de los dispositivos que podrían indicar un peligro); y técnicas de escaneo que permiten a las empresas buscar vulnerabilidades y malware de forma más activa, para no interrumpir el funcionamiento de los dispositivos. Las empresas deben estar atentas a los nuevos enfoques y herramientas que les ayudarán a proteger los dispositivos de sus redes, incluidas las plataformas de orquestación y gestión de eventos e información de seguridad que permiten analizar y compartir información contextual en tiempo real.

RECOMENDACIONES PARA LAS EMPRESAS

Motivar y habilitar la seguridad empresarial es difícil, en parte debido a la diversidad de entornos y necesidades de las empresas. El NSTAC ha identificado varios pasos que deberían darse:

- **Considere las recomendaciones aplicables anteriormente para los dispositivos de consumo como herramientas para mejorar la postura de seguridad en los entornos empresariales, especialmente para el BYOD.**

- **Mejorar el conocimiento de las mejores prácticas.** El DHS y otros organismos deberían colaborar con los sectores verticales de la industria, representados por grupos industriales (y, en el caso de las empresas consideradas "infraestructuras críticas", por sus Consejos de Coordinación Sectorial) para garantizar el conocimiento de las mejores prácticas para mitigar los efectos de los ataques de botnets y para asegurar los dispositivos conectados. En la medida de lo posible, el DHS y la industria deberían proporcionar guías de prácticas específicas del sector. Además, el DHS debería aprovechar el trabajo que se está realizando en el NCCoE.

- **Considerar incentivos para promover la adopción de normas.** Las agencias federales y el Congreso deberían considerar la posibilidad de utilizar fondos federales para incentivar la adopción de las recomendaciones de este informe en los proyectos financiados por el gobierno federal y para las empresas que implementan los proyectos. Estos incentivos sólo serían aplicables en los casos en los que no existan ya requisitos de seguridad de los dispositivos dirigidos o supervisados por el Gobierno federal (como en el caso de los dispositivos médicos).

- **Implantar servicios de seguridad gestionados.** Las empresas de todos los tamaños y tipos deberían considerar la posibilidad de implantar servicios de seguridad gestionados. Todas las organizaciones deben evaluar su postura de seguridad y considerar cuidadosamente si deben desplegar algún tipo de enfoque de seguridad gestionada. Además, las capacidades de supervisión deben abordar todos los tipos de dispositivos conectados. Los servicios como la mitigación de DDoS en caso de ataques facilitados por botnets son útiles, ya que las empresas van a ser cada vez más responsables de la seguridad.

- **Abordar la seguridad de la empresa.** Las empresas deben aprovechar el aislamiento de la red, la microsegmentación y las técnicas de filtrado para asegurar y restringir el acceso a Internet. Otras opciones que pueden ayudar a la seguridad de la empresa son:

    - *Conocimiento de los dominios:* Las empresas deben rastrear y bloquear el tráfico de los dominios que albergan amenazas. Las empresas también deben tomar medidas para proteger sus dominios. Atacantes

suelen dirigirse a los dominios con la mayor entrada DNS para amplificar la eficacia de su ataque.

- *Implantar controles compensatorios cuando sea necesario.* No todas las organizaciones podrán desplegar los protocolos prescritos. Como explica el NIST, en un entorno industrial, "puede haber situaciones en las que el [sistema de control industrial o ICS] no pueda soportar controles de seguridad o mejoras de control, o en las que la organización determine que no es aconsejable implementarlos a través del ICS. En tal situación, la organización proporciona una justificación que describe cómo los controles compensatorios proporcionan una capacidad de seguridad equivalente o un nivel de protección para el ICS, y por qué los controles de seguridad de línea de base relacionados no podrían ser empleados. "[66]Ejemplos de estos controles incluyen la detección en tiempo real consciente de la red, la autenticación y la autorización, la gestión de la vulnerabilidad, el perfil de comportamiento, la segmentación y la mitigación. [67] Los controles de compensación no resolverán el problema de las redes de bots globales, pero son un paso importante para proteger a las empresas.

- *Aprovechar la nube.* Los proveedores de servicios en la nube establecidos han aumentado su postura de seguridad y pueden ofrecer a las empresas importantes ventajas de seguridad. Las empresas -privadas y gubernamentales- deberían explorar los proveedores de la nube y la seguridad que pueden ofrecer.

- *Utilizar el aprovisionamiento dinámico.* Se trata de una parte importante de la virtualización y segmentación de la red, que permite a las empresas agilizar y controlar mejor el modo en que los dispositivos y los usuarios están autorizados a estar en un sistema. El aprovisionamiento dinámico automatiza los procesos de TI y refuerza los requisitos de seguridad, además de permitir una respuesta más rápida a los problemas de seguridad.

- *Redundancia.* Todas las empresas deberían considerar la redundancia para el DNS y todos los servicios de Internet críticos para el negocio.

- **Consideremos el mercado de los seguros. El mercado de los seguros** puede impulsar la mejora, ya que los suscriptores examinan a las empresas en función de la madurez de sus prácticas de gestión de los riesgos de seguridad y ofrecen primas más bajas a las empresas que se encuentran más arriba en la escala de madurez.

3.4 Aplicaciones/Software/OS

HALLAZGOS

El software de las aplicaciones y los sistemas operativos desempeña un papel fundamental a la hora de hacer frente a las redes de bots, que se intensifica a medida que el software se integra en más sistemas y dispositivos.
Además, a medida que el software ha proliferado, muchas empresas tecnológicas no tradicionales se han convertido en proveedores. Aunque se ha producido una mejora significativa y un intercambio de software seguro

[66] Boletín del NIST ITL. *Adaptación de los controles de seguridad para los sistemas de control industrial*. Noviembre de 2015. http://csrc.nist.gov/publications/nistbul/itlbul2015_11.pdf.
[67] Wallace Sann. ForeScout. *Sesión informativa para el subcomité ICR del NSTAC*. 22 de agosto de 2017.

Los procesos de desarrollo y gestión, los proveedores de software no tradicionales, las empresas de nueva creación y otros pueden no conocer o no tener recursos para aplicar los procesos. Además, en el contexto de la IO, el riesgo de las vulnerabilidades del software puede ser elevado; los coches conectados podrían chocar y las tostadoras inteligentes podrían provocar un incendio. [68]

Desafío de las redes de bots Relevancia para las aplicaciones/software/OS

Las aplicaciones, el software y los sistemas operativos son fundamentales porque son la clave de la seguridad de los puntos finales y de la seguridad de los servicios o recursos que aprovechan los puntos finales. Múltiples desarrolladores proporcionan software integrado en los dispositivos, aplicaciones y servicios; esta diversidad es integral para la innovación, pero presenta un desafío para la seguridad. Las partes interesadas se encuentran en diferentes niveles de madurez en el desarrollo y la gestión del software. Mientras que el desarrollo de software es clave para limitar el número y la gravedad de las vulnerabilidades en el software desde el principio, la gestión es clave para garantizar que las vulnerabilidades que se descubran puedan ser abordadas.

Es impracticable o imposible desarrollar software sin vulnerabilidades. Aunque se está avanzando en los métodos formales de verificación para piezas pequeñas y altamente críticas de sistemas vitales, el uso de tales métodos a escala o para sistemas ciberfísicos complejos sigue siendo un reto a medio y largo plazo. [69]En cambio, la aplicación de las mejores prácticas, directrices y herramientas de desarrollo y gestión de software seguro puede aumentar la seguridad de base.

Sin embargo, a pesar de la disponibilidad de prácticas, directrices y herramientas de los vendedores, la concienciación y la aplicación por parte de los vendedores y los clientes se retrasa considerablemente. En primer lugar, no todo el software es desarrollado o gestionado por proveedores a gran escala, y las prácticas de desarrollo seguro no pueden aplicarse necesariamente de forma fácil o coherente en entornos de desarrollo más pequeños. En segundo lugar, el código fuente abierto va en aumento; a menudo es mantenido por voluntarios que pueden no tener requisitos o procesos para el desarrollo seguro, una responsabilidad clara o financiación para responder a los problemas de seguridad. En tercer lugar, los usuarios pueden interrumpir la implementación, y muchos luchan por aplicar parches o mitigaciones de seguridad en productos, servicios o dispositivos en los contextos del consumidor y la empresa.

Se están realizando esfuerzos para hacer frente a la amenaza

Los proveedores de software empezaron a trabajar para mejorar la seguridad del código, es decir, el desarrollo del software, hace más de 15 años. Esta área de práctica, a menudo denominada aseguramiento del software, anima a los desarrolladores a crear un software más seguro y a abordar los requisitos de cumplimiento de la seguridad. Muchos grandes proveedores han desarrollado programas, formación y herramientas para el desarrollo, la implementación y el perfeccionamiento del código. Por ejemplo, el uso del ciclo de vida de desarrollo de seguridad (SDL) garantiza que el software se diseñe, desarrolle e implante teniendo en cuenta la seguridad durante todo su ciclo de vida. [70] Los proveedores han colaborado a través de organizaciones sin ánimo de lucro como el Software Assurance Forum

[68] Charlie Mitchell. Dentro de la ciberseguridad. *El fundador de Black Hat ve la responsabilidad del software como el principal desafío de la política de ciberseguridad.* 26 de julio de 2017. https://insidecybersecurity.com/daily-news/black-hat-founder-sees-software-liability-major-cybersecurity-policy-challenge.

[69] Kevin Hartnett. WIRED. *Computer Scientists Close in on Perfect, Hack-Proof Code.* 23 de septiembre de 2016. https://www.wired.com/2016/09/computer-scientists-close-perfect-hack-proof-code/.

[70] Microsoft. ¿Qué es el ciclo de vida del desarrollo de la seguridad? https://www.microsoft.com/en-us/sdl/default.aspx.

para la Excelencia en el Código (SAFECode) para promulgar prácticas para la garantía del software. [71] Los proveedores han contribuido al desarrollo de la Organización Internacional de Normalización (ISO)/Comisión Electrotécnica Internacional (IEC) 27034, una norma internacional basada en procesos para especificar, diseñar/seleccionar e implementar controles de seguridad de la información.

Los proveedores de software han estado trabajando para mejorar la gestión del software desarrollando, implementando y promoviendo políticas, procesos y programas de divulgación coordinada de vulnerabilidades (CVD). La divulgación y gestión de vulnerabilidades implica la comunicación con terceros que las encuentran; la validación y clasificación de las vulnerabilidades; el desarrollo de una actualización para mitigar la vulnerabilidad (por ejemplo, un "parche"); y la aplicación de actualizaciones o mitigaciones a los sistemas que están en funcionamiento. Al igual que con las herramientas para mejorar el aseguramiento del código, los proveedores de tecnología han invertido en las mejores prácticas para la divulgación y el manejo de las vulnerabilidades. Existen dos normas ISO, la ISO/IEC 29147 y la ISO/IEC 30111, que describen los procesos para recibir información sobre vulnerabilidades de terceros, comunicarse con ellos sobre los problemas notificados, e investigar, clasificar y resolver las vulnerabilidades.

Algunos proveedores de tecnología han invertido en la promoción de la CVD, y el Gobierno de Estados Unidos también ha aumentado sus esfuerzos en este ámbito. [72]Numerosos proveedores de software han participado en el proceso de múltiples partes interesadas de la NTIA en torno a la divulgación y gestión de vulnerabilidades para aumentar la adopción de las mejores prácticas existentes, mejorar la respuesta a los complicados desafíos de divulgación que implican a múltiples partes y ayudar a las industrias de seguridad crítica a entender mejor cómo adoptar la CVD. [73]Basándose en el esfuerzo de la NTIA, la Administración de Alimentos y Medicamentos publicó unas directrices que animaban a los fabricantes de dispositivos médicos a adoptar la CVD, haciendo referencia a las normas ISO/IEC 29147 e ISO/IEC 30111,[74]y la Administración Nacional de Seguridad en el Transporte por Carretera publicó unas directrices que animaban a los fabricantes de automóviles a disponer de un método y una política para recibir los informes de vulnerabilidad de los investigadores de seguridad. [75]Además, el Departamento de Defensa (DoD) y la Administración de Servicios Generales han creado programas CVD y/o programas de recompensas por errores, lo que permite la coordinación con los investigadores. [76]Recientemente, el Departamento de Justicia (DOJ) publicó un marco para ayudar a las organizaciones a crear un programa voluntario coordinado de divulgación de cibervulnerabilidades.
El Congreso también está estudiando la cuestión. Aunque puede que no sea apropiado para todas las organizaciones, el CVD podría ayudar a resolver los problemas de gestión del software.

[71] SafeCode. https://safecode.org/about-safecode/.
[72] I Am the Cavalry. *DOT Gov Coordinated Disclosure Timeline.* https://www.iamthecavalry.org/wp-content/uploads/2016/12/IATC_Gov-Coordinated-Disclosure-Timeline_v1.0.jpg.
[73] NTIA. Proceso de múltiples partes interesadas: Vulnerabilidades de la ciberseguridad. 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.
[74] Departamento de Salud y Servicios Humanos (HHS). "Postmarket Management of Cybersecurity in Medical Devices-Guidance for Industry and Food and Drug Administration Staff". 28 de diciembre de 2016. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022. pdf.
[75] Administración Nacional de Seguridad Vial (NHTSA). "Mejores prácticas de ciberseguridad para vehículos modernos". Octubre de 2016. https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.
[76] DOD. "El DOD anuncia la política de divulgación de vulnerabilidades digitales y el lanzamiento de "Hack the Army"". *Comunicado de prensa*. 21 de noviembre de 2016. https://www.defense.gov/News/News-Releases/News-Release- View/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/; https://hackerone.com/deptofdefense; GSA. Vulnerability Disclosure Policy. https://18f.gsa.gov/vulnerability- disclosure-policy/.

RECOMENDACIONES PARA LOS DESARROLLADORES DE SOFTWARE

Los esfuerzos por mejorar el aseguramiento del software y gestionar y responder a las vulnerabilidades notificadas o descubiertas de otro modo han mejorado de forma demostrable la ciberseguridad, pero el trabajo para crear una combinación de incentivos y desincentivos podría ayudar. Para ello, el NSTAC recomienda las siguientes consideraciones:

En primer lugar, las políticas centradas en el aseguramiento del software y la gestión de la vulnerabilidad - independientemente del mecanismo de aplicación- deben aprovechar las normas internacionales, incluidas la IEC/ISO 27034, la ISO/IEC 29147 y la ISO/IEC 30111. Deben centrarse en los procesos utilizados para desarrollar y arreglar el software (es decir, cómo se construye el software para reducir el número de vulnerabilidades y cómo se parchean o mitigan las vulnerabilidades) en lugar de la presencia de vulnerabilidades.

En segundo lugar, ni los gobiernos ni las empresas han aprovechado eficazmente las fuerzas del mercado para impulsar el desarrollo de un software más seguro porque aún no está claro qué norma deben cumplir las fuerzas del mercado. El NSTAC recomienda que el Gobierno de Estados Unidos fomente la concienciación sobre el papel que la seguridad del software y las compras de tecnología tienen en el riesgo operativo. El gobierno también debería hacer hincapié en las mejores prácticas y normas existentes, permitiendo a los compradores de tecnologías de la información y la comunicación (TIC) mantener conversaciones con sus proveedores sobre el desarrollo de productos y servicios tecnológicos y las prácticas de gestión de la seguridad.

El NSTAC recomienda específicamente lo siguiente:

- **El gobierno y las instituciones educativas deben esforzarse por hacer que la seguridad forme parte del plan de estudios de Informática dentro de la iniciativa de Ciencia, Tecnología, Ingeniería y Matemáticas.**

- **La comunidad de desarrollo de software debería proporcionar directrices sobre los procesos de DevSecOps.**

- **La industria debería considerar programas razonables y prudentes de divulgación coordinada de vulnerabilidades.** Estos podrían incluir programas de CVD gestionados por la organización o programas subcontratados si las organizaciones no tienen la capacidad de gestionarlos internamente.

- **La industria debe dar a los desarrolladores las herramientas para codificar de forma segura.** Mejorar las herramientas de desarrollo de código para mejorar la trazabilidad y la seguridad.

- **Compartir las mejores prácticas para hacer frente a las vulnerabilidades.** La NTIA ha revisado esta cuestión[77] y la industria puede apoyar las recomendaciones derivadas de ese proceso de múltiples partes interesadas, así como otras orientaciones. [78]

[77] NTIA. Proceso de múltiples partes interesadas: Vulnerabilidades de la ciberseguridad. 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

[78] DOJ. "Marco para un programa de divulgación de vulnerabilidades para sistemas en línea". Julio de 2017. https://www.justice.gov/criminal-ccips/page/file/983996/download.

- **El gobierno debería considerar la protección de la responsabilidad de quienes abordan públicamente las vulnerabilidades.** Es posible que la nación necesite un cambio de paradigma en su forma de abordar estos retos.

- **El gobierno y la industria deberían colaborar en una campaña para promover el aseguramiento del software, es decir, validar el software para limitar las vulnerabilidades de seguridad.** Esto puede requerir la promoción de mejores prácticas o directrices para dar ejemplo a los desarrolladores de software.

- **Considerar cuidadosamente cómo asegurar el desarrollo del código abierto.** El esfuerzo colectivo de la industria para dotar de fondos a los elementos críticos de la infraestructura global de la información a través de la Iniciativa de Infraestructura Central ayudará a resolver algunos problemas, sin embargo, el NSTAC cree que es necesario un mayor esfuerzo.

- **El gobierno y la industria deben aumentar la comprensión de los usuarios de tecnología sobre la importancia de la aplicación de parches a tiempo.** Esto puede hacerse incorporando estos componentes a los programas existentes de concienciación sobre la seguridad.

3.5 Gobierno

HALLAZGOS

El gobierno desempeña un papel clave en la resistencia de Internet y las comunicaciones. Es un comprador y gestor de dispositivos conectados; es un regulador o convocante en la configuración de la política; y ejerce un poder soberano para perseguir a los delincuentes, defender a la Nación y negociar con otros países. Cada función es diferente, presenta diferentes retos y ofrece diferentes oportunidades.

Como gestor y comprador, el gobierno se enfrenta a muchos de los mismos retos de las redes de bots que otros usuarios empresariales. El número de usuarios de dispositivos conectados en la administración pública dificulta la gestión de los mismos. El gobierno tiene la responsabilidad añadida de proteger la información gubernamental sensible, así como los datos de los ciudadanos, lo que convierte al gobierno en un objetivo de alto valor. Además, las entidades gubernamentales de Estados Unidos gestionan varios bloques de IP vulnerables. [79]Se enfrenta a otros retos en el entorno normativo y de política de adquisiciones, que restringe la flexibilidad y exige que las decisiones de adquisición se tomen con mucha antelación y estén sujetas a la supervisión y a las restricciones externas.

El gobierno tiene oportunidades únicas para mejorar la seguridad. Como gestor, el gobierno puede tomar medidas para mejorar las prácticas de gestión del uso del móvil, utilizando cualquier número de servicios de gestión de dispositivos existentes y aumentando la concienciación sobre la importancia de emplear prácticas básicas de ciber higiene. Como comprador de tecnología, el gobierno puede exigir dispositivos más seguros. Las normas gubernamentales suelen conducir a la adopción de esas normas por parte del sector privado, evitando el desarrollo de prácticas diferentes y potencialmente competitivas. El senador Mark Warner presentó un proyecto de ley, la *Ley de Mejora de la Ciberseguridad del Internet de las Cosas (IoT) de 2017*, que propone mejorar la seguridad del IoT mediante el establecimiento de requisitos mínimos para los dispositivos del IoT

[79] Ann Cox. DHS. *Sesión informativa para el Subcomité ICR del NSTAC*. 1 de agosto de 2017.

adquiridos por el Gobierno Federal. [80] Sin embargo, una legislación como la *Ley de Ciberseguridad de la IO* podría tener consecuencias no deseadas si no se aborda con cuidado. El proyecto actual, si se promulga, podría exponer a los contratistas del gobierno a la responsabilidad debido a los onerosos requisitos de certificación, fomentar la "piratería" de los dispositivos del gobierno, y limitar la capacidad de los contratistas para gestionar adecuadamente las revelaciones de vulnerabilidad. La mejor manera de garantizar la ciberseguridad es a través de soluciones flexibles e impulsadas por el mercado que reflejen el liderazgo y la innovación del sector privado y que se desarrollen mediante la colaboración entre la industria y el gobierno. [81]

Como regulador o convocante, el gobierno puede dar forma a la política y a las normas, al tiempo que promueve la innovación. En Estados Unidos, la política cibernética hace hincapié en el gobierno como convocante. El gobierno debe seguir reuniendo a las partes interesadas para desarrollar las mejores prácticas con las partes interesadas de una selección diversa de la industria y en todo el ecosistema de las comunicaciones y las TIC. Es imperativo que el gobierno cierre la brecha de conocimiento entre las industrias sofisticadas y las no sofisticadas. A nivel internacional, el gobierno puede facilitar la colaboración a mayor escala, animando a otros países a compartir información y adoptar las mejores prácticas adecuadas para mitigar las redes de bots. Estos esfuerzos podrían reducir notablemente el número y la magnitud de estos ataques, ya que muchos se originan en el extranjero.

El gobierno desempeña un papel importante a la hora de garantizar la financiación de la investigación sobre ciberseguridad y mitigación de ataques, cuyos beneficios no pueden exagerarse. Además del gasto directo, el gobierno debe seguir buscando oportunidades para comprometerse con el público para mejorar la seguridad. Este año, la FTC organizó un concurso de premios para crear soluciones para "protegerse de las vulnerabilidades de seguridad en el software que se encuentra en los dispositivos IoT en sus hogares. "[82] El ganador -un desarrollador de software de New Hampshire- desarrolló una aplicación móvil que puede ayudar a los usuarios a determinar si sus dispositivos están desactualizados o sus redes son inseguras. [83]

El gobierno también tiene un papel único en la seguridad pública y debe trabajar con el NIST y otros para aumentar la seguridad de los sistemas de seguridad pública. Las acciones de aplicación de la FTC contra los fabricantes que emplean medidas de seguridad lamentablemente inadecuadas ponen a la industria sobre aviso de la necesidad de implementar la seguridad básica y representar con veracidad la seguridad de sus dispositivos a los consumidores. [84]

Como nación soberana, el gobierno tiene poderes y deberes únicos para proteger a los ciudadanos, hacer cumplir la ley y defender al país de amenazas externas, incluidas las redes de bots. A través de estos poderes,

[80] Mark Warner. "Senadores presentan una legislación bipartidista para mejorar la ciberseguridad de los dispositivos del "Internet de las cosas" (IoT)". *Comunicado de prensa*. 1 de agosto de 2017. https://www.warner.senate.gov/public/index.cfm/pressreleases?ID= 06A5E941-FBC3-4A63-B9B4-523E18DADB36.

[81] Mike Bergman. Asociación de Tecnología de Consumo. *Sesión informativa para el subcomité ICR del NSTAC*. 3 de agosto de 2017.

[82] FTC. Desafío del inspector del hogar de IoT. 2017. https://www.ftc.gov/iot-home-inspector-challenge.

[83] FTC. "La FTC anuncia el ganador de su concurso de seguridad para dispositivos domésticos del Internet de las Cosas". *Comunicado de prensa*. 26 de julio de 2017. https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things- home-device-security.

[84] FTC. "La FTC aprueba la orden final de resolución de cargos contra TRENDnet. Inc." *Comunicado de prensa*. 7 de febrero de 2014. https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against- trendnet-inc; https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home- routers-cloud-services-put.

el gobierno puede detener o disuadir algunas actividades maliciosas. Algunos ejemplos de herramientas eficaces son el bloqueo de registros de dominio, el bloqueo de IP y las investigaciones criminales y el desmantelamiento de botnets.

Las asociaciones público-privadas con las fuerzas del orden han sido eficaces, y Estados Unidos debería buscar oportunidades para ampliar estos esfuerzos. Las fuerzas de seguridad, los equipos de respuesta a emergencias informáticas y otros organismos suelen recurrir al sector privado para obtener información sobre amenazas y datos de los proveedores de telecomunicaciones, antivirus y el sector financiero. La inteligencia es esencial para identificar a los individuos con la motivación, la intención y el respaldo para llevar a cabo ciberataques, y estas asociaciones ayudan a los gobiernos y a los proveedores de servicios de Internet a nivel mundial a identificar y remediar las amenazas. El NSTAC recomienda que el gobierno aumente la colaboración con el sector privado, en particular con respecto a las investigaciones. Estas asociaciones público-privadas han florecido en el Reino Unido, y las empresas de seguridad estadounidenses y otras están dispuestas a cooperar con el gobierno para apoyar las investigaciones pendientes y futuras. [85]

El Departamento de Justicia, en coordinación con el FBI, otros organismos policiales y entidades privadas, ha conseguido desmantelar redes de bots. El primer desmantelamiento con éxito se produjo en abril de 2011, cuando el gobierno detuvo "Coreflood", un ataque que afectaba a más de 378.000 dispositivos. [86] Desde entonces, ha habido otras victorias, como el reciente desmantelamiento de dos mercados negros en línea, AlphaBay y Hansa, con la cooperación de gobiernos extranjeros. [87]

Ejemplos de grandes retiros de botnets88

- 2011: DNS Changer89
- 2011: Coreflood (378.000 dispositivos)
- 2013: Citadel (2 millones de dispositivos)
- 2014: GameOver Zeus (de 500.000 a 1 millón de dispositivos)
- 2016: Avalance (500.000 dispositivos)
- 2017: Kelihos/Waldec (100.000 dispositivos)

Al reducir las barreras normativas que limitan la participación de la industria, el gobierno podría hacer frente de manera más eficiente incluso a los ataques más sofisticados de las redes de bots.

El gobierno puede mejorar los desmantelamientos de botnets eliminando las barreras que limitan la participación de la industria. Los desmantelamientos de botnets requieren tiempo, dinero y recursos, y pocas empresas tienen el incentivo de emprender las acciones legales necesarias para intentar un desmantelamiento de botnets. [90] Para la industria, los desmantelamientos de botnets suelen implicar asumir el control de la infraestructura, redirigir

[85] Raj Samani. McAfee, Reino Unido. *Sesión informativa para el subcomité ICR del NSTAC*. 15 de agosto de 2017.
[86] DOJ. "El Departamento de Justicia toma medidas para desactivar una botnet internacional". 13 de abril de 2011. https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.
[87] DOJ. "AlphaBay, el mayor 'mercado oscuro' online, cierra". 20 de julio de 2017. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.
[88] Leonard Bailey. DOJ. *Sesión informativa para el subcomité ICR del NSTAC*. 10 de agosto de 2017.
[89] http://www.dcwg.org/dns-changer/
[90] Ibid.

comunicaciones, y mitigar los daños. Estas actividades suelen requerir la autorización del usuario final o una orden judicial, una orden de restricción temporal o un requerimiento civil. [91] Esto es un reto cuando los ataques maliciosos se originan fuera de la propia red de un ISP. Por lo tanto, los gobiernos - junto con el apoyo de la industria - están mejor posicionados para dirigir las actividades de desmantelamiento de botnets.

Otra cuestión que puede frenar las reducciones es la medición del éxito para los fiscales. En el contexto de la actividad delictiva en el mundo físico, los objetivos del gobierno y las estructuras de incentivos reflejan un enfoque en la identificación y el enjuiciamiento de los acusados. Estos objetivos y estructuras de incentivos tradicionales pueden no estar totalmente optimizados para el mundo virtual, que permite a los ciberdelincuentes tener un mayor anonimato y, por lo tanto, frustra significativamente los esfuerzos para identificarlos y perseguirlos como acusados. Sin embargo, también hay otras formas en las que los fiscales pueden desbaratar y disuadir la delincuencia -incluidos los ataques de botnets con malware- en el mundo virtual. Sin dejar de buscar y perseguir a los acusados de delitos, lo que sigue siendo fundamental, los fiscales también pueden verse incentivados a centrarse más ampliamente en la prevención del delito y la seguridad nacional.
Los fiscales pueden ayudar a prevenir la proliferación y el impacto negativo de las redes de bots. Pueden desbaratar y desmantelar las operaciones de las redes de bots, incluso cuando no hay ningún acusado potencial.

La interrupción y el desmantelamiento de las redes de bots puede tener efectos positivos significativos. Por ejemplo, los esfuerzos de la colaboración público-privada para cortar los vínculos entre los ordenadores infectados y la infraestructura de Citadel, una de las mayores redes de bots documentadas, hicieron que cesara el 90% de la actividad de la red de bots. [92] Del mismo modo, la toma de posesión por parte del gobierno de Coreflood, que utilizaba software malicioso para desviar información personal y financiera de usuarios desprevenidos, permitió a las víctimas eliminar el software malicioso de sus máquinas y evitó una mayor pérdida de privacidad y daños a la seguridad financiera de los usuarios. En nueve días, el número de balizas procedentes de ordenadores infectados que se enviaban a los servidores disminuyó considerablemente. [93]

Sin embargo, muchas botnets no son desarticuladas por el gobierno - o hay un retraso en su desarticulación - ya que, en consonancia con su estructura de incentivos, muchos fiscales están más centrados en identificar y procesar a un acusado penal. [94] Con arreglo a las directrices actuales, los fiscales federales sólo se ven alentados a iniciar el enjuiciamiento cuando creen que la conducta de la persona constituye un delito federal y que las pruebas admisibles serán suficientes para obtener y mantener una condena. Este enfoque en el enjuiciamiento limita la interrupción y el desmantelamiento de las redes de bots por parte del gobierno porque, en gran parte, no hay una persona o personas fácilmente identificables para enjuiciar, incluso cuando los delitos están en curso.

El gobierno ha aumentado eficazmente su atención a la prevención en otros contextos; el Departamento de Justicia ha orientado efectivamente más recursos y energía hacia la prevención en el contexto de la lucha contra el terrorismo. Las lecciones aprendidas de estos éxitos pueden ser aplicables cuando el gobierno considere cómo evolucionar las estructuras de incentivos relacionados con la ciberdelincuencia de una manera que no esté exclusivamente ligada a

[91] Véase la Ley de Fraude y Abuso Informático (CFAA) (18 U.S.C. § 1030); la Ley de Escuchas Telefónicas (18 U.S.C. § 2511); las Leyes de Registro de Plagio/Trap and Trace (18 U.S.C. §§ 3121 *et seq.*).

[92] Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 247 (2014).

[93] Memorándum suplementario del Gobierno en apoyo de la medida cautelar, pág. 4, Figura 1 en *Estados Unidos v. John Doe*, No. 3:11-cv-561 (VLB) (D. Conn. Filed Apr. 11, 2011).

[94] Los presupuestos anuales y las medidas de rendimiento de la Oficina del Fiscal de los Estados Unidos (USAO) están directamente vinculados al número de condenas.

En cambio, fomenta la coordinación entre los organismos federales y con el sector privado para desbaratar y desmantelar las redes de bots. Por ejemplo, aunque el FBI tiene la importante función de investigar los ciberdelitos, su autoridad para actuar no está exenta de limitaciones. El FBI debe cooperar, coordinar y buscar la aprobación de los fiscales federales para emplear ciertas herramientas de investigación, y la autorización suele retenerse a menos que exista una probabilidad de condena, lo que limita el potencial del gobierno para prevenir la ciberdelincuencia y proteger contra los riesgos de seguridad nacional. La reorientación de las estructuras de recursos e incentivos también permitiría al gobierno aprovechar y asociarse con el sector privado en la prevención de la ciberdelincuencia de forma más regular y productiva para proteger mejor a las víctimas de las redes de bots y aumentar los costes de las operaciones de las redes de bots para los delincuentes. El aumento de los costes de las operaciones delictivas tiene un efecto positivo en cascada; al reducir el número de delincuentes que pueden permitirse participar en la delincuencia en línea también se reduce el "ruido" en el ecosistema, lo que permite a las entidades tanto del sector público como del privado identificar con mayor eficacia las amenazas persistentes avanzadas más sigilosas.

El NSTAC recomienda las siguientes acciones para mejorar los esfuerzos de retirada:

- **Las políticas del DOJ deberían apoyar más la intervención gubernamental. El DOJ puede necesitar recursos adicionales para aumentar estos esfuerzos, que también dependen de la colaboración con el sector privado y con posibles socios internacionales.**

- **Las implicaciones de las redes de bots para la seguridad nacional justifican que el Departamento de Justicia se centre en la prevención y la interrupción de los ataques de redes de bots, y no en su persecución**.

- **El presupuesto para la ciberdelincuencia a nivel federal debería reflejar la importancia de la prevención y no debería estar vinculado a la persecución y las condenas.** [95]

El gobierno también debe asegurarse de que la legislación existente no limita el intercambio de información de la industria o las actividades de "defensa activa" apropiadas. Leyes como la *Computer Fraud and Abuse Act*, la *Wiretap Act,* y la *Pen Register/Trap and Trace Act* pueden desanimar involuntariamente a los ISP a la hora de tomar ciertas "medidas defensivas activas" - como implementar el filtrado de entrada/salida (BCP 38 y 84), bloquear el tráfico malo reportado y neutralizar un sistema que esté atacando la red del proveedor - debido a preocupaciones de responsabilidad legal. [96] Las protecciones legales en caso de error son limitadas, y las empresas se enfrentan a posibles críticas por los errores cometidos. El gobierno debería buscar formas de limitar los riesgos de responsabilidad a los proveedores que de buena fe emplean medidas defensivas activas. La *Ley de Intercambio de Información sobre Ciberseguridad* (CISA) de 2015 autoriza la supervisión de la información de un sistema de información con fines de ciberseguridad y proporciona protecciones de responsabilidad para tales actividades y otras medidas defensivas. [97] Leyes como la CISA permiten a la industria proteger sus redes y apoyar los esfuerzos de toma de decisiones del gobierno. Si se espera más del sector privado, deberían considerarse protecciones adicionales. La mejora de la ciberseguridad requerirá una asociación mutuamente beneficiosa entre la industria y el gobierno.

[95] Richard Boscovich. Microsoft. *Sesión informativa para el subcomité ICR del NSTAC*. 16 de agosto de 2017.
[96] Ley de fraude y abuso informático (CFAA) (18 U.S.C. § 1030); Ley de escuchas telefónicas (18 U.S.C. § 2511); Leyes de registro/trampa y rastreo (18 U.S.C. §§ 3121 *et seq.*); Leonard Bailey. DOJ. *Sesión informativa para el Subcomité ICR del NSTAC*. 10 de agosto de 2017.
[97] Ley de Intercambio de Información sobre Ciberseguridad de 2015, Pub. L. No. 114-113, 129 Stat. 2242 (2015).

RECOMENDACIONES

Se están realizando esfuerzos para mejorar la rendición de cuentas de las agencias, tal y como refleja el Presidente en la OE 13800.[98] El gobierno debe basarse en estos esfuerzos, predicando con el ejemplo. Además, el gobierno debe emplear enérgicamente sus herramientas de aplicación de la ley, eliminando al mismo tiempo los obstáculos a la acción privada.

- **Dar ejemplo aprovechando con sensatez las capacidades en las adquisiciones**. El gobierno debería invertir en aumentar la seguridad de las redes federales. Los esfuerzos actuales, como el despliegue de Diagnóstico y Mitigación Continuos para las agencias civiles y Cumplir para Conectar para el DoD, ambos basados en las mejores prácticas del NIST, permiten a las agencias detectar, inventariar y remediar todos los dispositivos de IoT y de tecnología operativa, así como los puntos finales basados en Windows, en las redes federales. El liderazgo en este ámbito podría servir de ejemplo para la industria privada.

- **Emplear las normas y orientaciones del NIST para la Ley Federal de Gestión de la Seguridad de la Información y la Gestión de la TI**. El NIST, en colaboración con el sector privado, está mejorando continuamente las mejores prácticas de ciberseguridad. Esto incluye los esfuerzos para mejorar su marco, actualizar las capacidades criptográficas (en particular la criptografía resistente al quantum), y explorar las capacidades de seguridad de la IA y el IoT. El NIST también está trabajando para mejorar la arquitectura de Internet, incluida la seguridad del dominio y de BGP. El gobierno debería estar entre los primeros en implementar estos estándares.

- **Aumentar los desmantelamientos de botnets por parte de las fuerzas de seguridad**. El gobierno debería aprovechar los recientes éxitos en el desmantelamiento de botnets para demostrar la eficacia de la prevención. Entre otras cosas, el gobierno debería considerar:

  - Garantizar que las estructuras de incentivos reflejen la importancia de la prevención en lugar de estar significativamente vinculadas al enjuiciamiento y las condenas;

  - Racionalización de los procesos de aplicación de la ley para el desmantelamiento de redes de bots, incluido el uso de directrices de sentencia definitivas;

  - Apoyar la colaboración entre el sector público y el privado en materia de retirada de fondos; y

  - Modernizar sus métodos de recopilación de ciberinteligencia permitiendo que un analista se centre en un objetivo durante un periodo más largo, convirtiéndose así en un experto y más capaz de combatir un ataque específico. Al mismo tiempo que se estudia la forma de mejorar la retirada de botnets, es imperativo que el gobierno actúe con transparencia.

- **Evitar la duplicación**. El gobierno debería consolidar y coordinar los esfuerzos para reforzar la ciberseguridad de la nación de forma más eficiente. Por ejemplo, ha habido varios esfuerzos superpuestos para mejorar la seguridad de la cadena de suministro de una variedad de agencias, incluyendo el NIST, el DHS y la FCC. También se han solapado los esfuerzos para la seguridad de la IO, incluso en el DHS, el NIST y la NTIA, así como en múltiples agencias que supervisan los diversos verticales de la IO (como

[98] Oficina del Secretario de Prensa de la Casa Blanca. *Orden Ejecutiva 13800, Fortalecimiento de la ciberseguridad de las redes federales y la infraestructura crítica*. 16 de mayo de 2017. https://www.federalregister.gov/documents/2017/05/16/ 2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

vehículos, ciudades inteligentes, etc.). Son cuestiones importantes que se beneficiarían de un enfoque coordinado.

- **Mantener un papel de convocatoria y promoción**. El gobierno está especialmente preparado para convocar a la industria a fin de aplicar los marcos existentes a nuevas áreas como la IO y desarrollar las mejores prácticas para las tecnologías en evolución. Deben fomentarse los procesos de múltiples partes interesadas, como los del NIST y la NTIA, y promover su asesoramiento práctico. Aunque el gobierno no debe emitir mandatos, puede animar a las entidades a adoptar estas normas ofreciendo incentivos. Al mismo tiempo, el gobierno debe revisar las normas que surjan de estos procesos para identificar y cubrir cualquier laguna que pueda afectar a la IO.

- **Aumentar las protecciones para los proveedores de servicios de Internet que adopten medidas de defensa**. Los estatutos existentes suelen desalentar el uso de medidas de defensa activas por parte de la industria. Por lo tanto, el gobierno debería buscar formas de limitar la responsabilidad legal de los proveedores que tratan de proteger sus sistemas de los ataques de botnets.

- **Financiar la investigación en ciberseguridad y el desarrollo de normas.** Es imprescindible financiar la investigación y el desarrollo. El gobierno debe apoyar financieramente estos esfuerzos, incluyendo la investigación de las mediciones de la ruta de referencia, la topología a nivel de router, la topología a nivel de instalación, el rendimiento y las mejores prácticas de higiene de seguridad. La investigación de nuevas tecnologías -en particular la tecnología cuántica- es necesaria a medida que las amenazas evolucionan y el cifrado se vuelve menos eficaz.

- **Promover normas y directrices de consenso voluntario. Las** asociaciones público-privadas y las directrices voluntarias son más eficaces que los mandatos, que se quedan rápidamente obsoletos en este entorno en constante evolución. [99]Cualquier regulación debe centrarse en la mitigación de riesgos y en la limitación de la responsabilidad que pueda surgir de los esfuerzos de la industria por compartir información y emplear medidas de defensa.

3.6 Internacional

HALLAZGOS

Ningún debate sobre los ataques distribuidos está completo sin prestar especial atención a los actores internacionales, que forman parte de cada capa del ecosistema anterior. Entre los actores internacionales y los desafíos se encuentran:

- **Empresas tecnológicas internacionales**. Los fabricantes de dispositivos y los proveedores de servicios se extienden por todo el mundo, vendiendo productos a nivel internacional. Esto incluye una amplia gama de fabricantes de equipos (como teléfonos inteligentes, electrodomésticos, automóviles, sensores industriales y dispositivos médicos) hasta proveedores de servicios móviles y de Internet a nivel mundial (operadores de redes virtuales móviles, propietarios de redes, proveedores de servicios de Internet, operadores de redes privadas, mayoristas y revendedores).

- **Cadenas de suministro globales**. El software, los conjuntos de chips y otros componentes de los dispositivos de la IO y las redes de comunicaciones globales proceden de todo el mundo.

[99] Raj Samani. McAfee, Reino Unido. *Sesión informativa para el subcomité ICR del NSTAC.* 15 de agosto de 2017.

- Entidades **de gestión de Internet**. Varias entidades participan en la gestión y las funciones básicas de la infraestructura mundial de Internet, desde los nombres de dominio hasta el encaminamiento del tráfico. La Corporación de Asignación de Nombres y Números de Internet y otras muchas participan en cuestiones de gobernanza y en las actividades cotidianas.

- **Gobiernos individuales y bloques regionales**. Cada gobierno tiene las mismas participaciones y funciones que Estados Unidos: usuario/comprador, regulador y soberano. Los distintos países tienen enfoques diferentes de la regulación y la política tecnológica. Las regiones también han colaborado, y los países europeos y asiáticos trabajan colectivamente en aspectos de la política tecnológica y de Internet, incluida la IO. Los esfuerzos nacionales y regionales alimentan los sistemas y organismos mundiales.

- **Organismos de normalización mundial y cooperativas industriales**. Decenas de organismos de normalización, desde el Instituto de Ingenieros Eléctricos y Electrónicos hasta la Alianza para las Soluciones de la Industria de las Telecomunicaciones y la ISO, dan forma a las normas y protocolos tecnológicos internacionales. Su trabajo se basa en el consenso para promover verdaderas innovaciones en las redes de comunicaciones, incluida la interoperabilidad. Se basan en la experiencia y la participación de una comunidad internacional. Los grupos de la industria también trabajan juntos; ejemplos de ello son la GSMA, la Asociación de la Industria de las Telecomunicaciones y otros. Y algunos grupos regionales, como el Registro Americano de Números de Internet, son clave para una red de comunicaciones global más amplia.

Las redes de bots son una amenaza global. Más del 80% del tráfico de botnets se origina en el extranjero. [100] Para hacer frente al desafío de las redes de bots es necesaria la cooperación internacional para desarrollar normas, y todos los países deben trabajar para asegurar sus redes y dispositivos.

El esfuerzo del Gobierno del Reino Unido es un ejemplo

Los países adoptan enfoques variados, pero los esfuerzos más prometedores incluyen verdaderas asociaciones entre el sector privado y el gobierno, libres del miedo a la responsabilidad o a la recriminación. Por ejemplo, el trabajo proactivo que se está llevando a cabo en el Reino Unido, que incluye campañas de concienciación pública, prácticas gubernamentales internas y asociaciones entre el sector público y el privado, ha dado lugar a redes más seguras. [101]

- **Campañas de concienciación pública**. El Gobierno del Reino Unido ha puesto en marcha una serie de campañas de concienciación pública destinadas a educar al público sobre prácticas más seguras. Colaboró con los grandes fabricantes de dispositivos para impulsar las cuentas con doble factor de autenticación, que disminuyen las preocupaciones de seguridad relacionadas con el robo de contraseñas. El gobierno también utiliza sus sitios web para recordar a los usuarios que actualicen su software. Por ejemplo, los declarantes de impuestos que utilizan programas informáticos obsoletos para presentar sus declaraciones reciben un aviso para que actualicen su software y no puedan presentar sus declaraciones si no lo hacen antes del siguiente periodo de presentación. El gobierno está iniciando una colaboración con el mundo académico para traducir los datos y estadísticas sobre ciberseguridad e higiene en información y gráficos

[100] Mike Bergman. Asociación de Tecnología de Consumo. *Sesión informativa para el subcomité ICR del NSTAC.* 3 de agosto de 2017 (en el que se afirma que aproximadamente el 89% de las ubicaciones de los ataques Mirai/Dyn se encontraban en un país extranjero).
[101] Ian Levy. Centro Nacional de Ciberseguridad del Reino Unido. *Sesión informativa para el subcomité ICR del NSTAC.* 9 de agosto de 2017.

que el público pueda entender. Estos importantes pasos ayudarán al público a comprender la importancia de la ciberseguridad y a tomar las medidas adecuadas para cambiar su comportamiento.

- **Prácticas gubernamentales internas**. El Reino Unido protege su huella en línea. Ha añadido la autenticación de mensajes basada en el dominio, la notificación y la conformidad a todos los dominios gubernamentales del país para evitar la suplantación de correos electrónicos. Para reducir los ataques de malware, el gobierno realiza un escaneo automático de cualquier sitio que utilice un nombre gov.uk. El gobierno también está protegiendo la marca gov.uk rastreando y eliminando agresivamente los sitios web que suplantan a gov.uk. El gobierno también está tomando medidas para gestionar mejor su empresa. Recoge datos sobre los organismos que se retrasan en las actualizaciones y los utiliza para obligar a los integradores de sistemas a mejorar o arriesgarse a que el gobierno publique esa información para consumo público. El gobierno también está tratando de no comprar software que no sea seguro o que no haya sido validado.

- **Asociaciones público-privadas**. Las asociaciones entre el Gobierno del Reino Unido y el sector privado ayudan a prevenir los ataques y a hacer más seguras las redes. Por ejemplo, el gobierno pidió a los hosts que retiraran o arreglaran el tráfico dañino, lo que dio lugar a una drástica disminución de la disponibilidad de phishing, webinject y phishing de marca gubernamental. Según la información proporcionada por el Cuartel General de Comunicaciones del Gobierno del Reino Unido (GCHQ), el gobierno logró derribar 153 almacenes de credenciales de kits de phishing, 2.570 ataques de fraude de tarifa avanzada y 23.000 retransmisiones de correo. Para proteger sus redes, el gobierno construyó una estructura de DNS recursivo a escala del sector público que incluye un servicio de filtrado. Ofrece este servicio a los ISP de forma gratuita. Según GCHQ, en julio de 2017, este servicio ha bloqueado 23.046 dominios únicos que alojan contenido malicioso. El uso del servicio de mitigación de phishing y malware del gobierno dio como resultado 79.567 ataques retirados con éxito. El gobierno también está utilizando una táctica de "nombrar y avergonzar" para animar a industrias como los bancos y los ISP a incorporar procesos seguros en sus defensas.

Otras asociaciones internacionales

En Europa, el proyecto "No More Ransom" es una colaboración entre el Centro Europeo del Cibercrimen, la policía holandesa y empresas comerciales como Amazon Web Services. [102] La iniciativa se creó para servir de repositorio único de claves de cifrado con el fin de mejorar la seguridad global. La comunidad informa a las víctimas del ransomware con el que han sido infectadas y ha eliminado colectivamente varios programas maliciosos, como Shade, Chimera y WildFire. Esta iniciativa también ofrece 50 herramientas de cifrado disponibles públicamente para las víctimas de ransomware. Esfuerzos como "No More Ransom" son pasos importantes para la comunidad internacional en la lucha contra las redes de bots.

RECOMENDACIONES PARA EL GOBIERNO

- **El gobierno de Estados Unidos debe desarrollar normas internacionales que frenen la proliferación de botnets. El** Reino Unido demuestra que los gobiernos pueden desempeñar un papel importante a la hora de modelar la seguridad y colaborar con el sector privado para que las redes -privadas y públicas - más seguro. Otros gobiernos pueden aprender de este ejemplo; sin embargo, los gobiernos

[102] Raj Samani. McAfee, Reino Unido. *Sesión informativa para el subcomité ICR del NSTAC.* 15 de agosto de 2017.

no puede actuar solo. El Gobierno de EE.UU. debe colaborar con el sector privado para trabajar en los organismos internacionales de normalización con el fin de desarrollar normas basadas en las mejores prácticas para guiar a los gobiernos y a los proveedores de servicios. La adopción generalizada de las normas proporcionará una importante defensa.

- **El Gobierno de EE.UU. debería impulsar un marco internacional para la seguridad de los dispositivos**. El desarrollo de dispositivos seguros requiere la cooperación internacional. Esto incluye la identificación de uno o varios organismos que podrían encargarse de desarrollar un marco o plataforma para compartir información sobre las características de seguridad de los dispositivos y las huellas dactilares de comportamiento y/o los requisitos de parcheo y actualización. Estas normas pueden ayudar a los fabricantes a desarrollar dispositivos más seguros y a las empresas y consumidores a gestionar mejor sus dispositivos.

- **Desarrollar la disuasión internacional contra los ataques de los Estados nación.** Los estados nación originan ahora un número significativo de ataques de botnet. Para disuadir este comportamiento será necesario que los organismos internacionales y las naciones individuales adopten una postura firme contra estas acciones. Estas acciones eliminarán una fuente importante de estos ataques y, lo que es más importante, empezarán a aumentar el coste para los atacantes.

MOONSHOT DE 4.0 CIBERSEGURIDAD

La sección anterior de este Informe (*Sección 3.0*) se centró en las recomendaciones a corto plazo relacionadas con las mejores prácticas y tecnologías existentes y conocidas que, si se aplican de forma más amplia, podrían tener un impacto tangible inmediato en la reducción de la amenaza de los ciberataques automatizados y distribuidos. Las conclusiones del Subcomité ICR del NSTAC reforzaron la recomendación anterior del NSTAC en el *Informe del NSTAC al Presidente sobre la Visión Estratégica de las Tecnologías Emergentes103* de que los retos actuales de la ciberseguridad de la nación no están limitados principalmente por el entorno tecnológico, sino por factores controlados por el ser humano, como diversos retos legales, de comportamiento y educativos que hasta ahora han limitado el despliegue de las mejores prácticas de ciberseguridad ampliamente aceptadas.

Aunque la plena aplicación de las recomendaciones de *la sección 3.0* tendría un impacto tangible en la ciberseguridad del país, estas recomendaciones colectivas siguen representando, en última instancia, soluciones incrementales que son insuficientes para abordar la totalidad de los retos de ciberseguridad más fundamentales y persistentes del país. Además, el NSTAC ha llegado a la conclusión de que el panorama tecnológico actual y emergente -que incluye avances significativos en el aprendizaje automático, la nube y la computación cuántica- proporciona la base necesaria para lograr una transformación drástica de la ciberseguridad. El NSTAC determinó que los esfuerzos carecen principalmente de una unidad nacional concertada de esfuerzo y dirección estratégica. Por ello, el NSTAC reitera su recomendación, mencionada por primera vez en el *Informe del NSTAC al Presidente sobre la Visión Estratégica de las Tecnologías Emergentes*, de que el gobierno establezca un Moonshot de ciberseguridad nacional.

[103] NSTAC. *Informe del NSTAC al Presidente sobre visiones estratégicas de las tecnologías emergentes*, https://www.dhs.gov/sites/default/files/publications/Draft%20NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20%287-10-17%29%20v3%20%281%29-%20508.pdf

Con el respaldo de la Casa Blanca, el NSTAC se compromete a poner en marcha el concepto de Moonshot de ciberseguridad para asesorar a la industria privada sobre la forma en que el gobierno podría coordinar más eficazmente un esfuerzo nacional. Basándose en el consenso del NSTAC y de la EOP, este estudio tendría una duración limitada para reflejar tanto la urgencia a corto plazo del desafío de la ciberseguridad, al tiempo que garantizaría una exhaustividad y un rigor adecuados para una iniciativa de esta magnitud. Para llevar a cabo este estudio, el NSTAC propone una doble línea de acción inicial.

Definir el proceso: Principios básicos de los modelos Moonshot

La primera fase del estudio del NSTAC revisará los modelos que han tenido éxito, independientemente de la industria o la materia, que en general reflejan los principios básicos de los esfuerzos Moonshot. El NSTAC mirará más allá del ámbito de la ciberseguridad para identificar las lecciones aprendidas de los esfuerzos de movilización nacional que han tenido éxito anteriormente. Esta primera fase de estudio se centrará en responder a la pregunta fundamental: *¿Cuáles son los principios básicos que definen los modelos Moonshot que han tenido éxito?*

Como base de partida, el NSTAC se centrará en identificar otras iniciativas que se caractericen por los principios que se enumeran a continuación. Estos elementos propuestos son sólo directrices para informar del alcance inicial del estudio y no se considerarán exhaustivos. En el momento de redactar este documento, el NSTAC ha llegado a la conclusión de que, para que una iniciativa pueda calificarse como Moonshot, debe caracterizarse como mínimo por los siguientes elementos:

- **Llamada a la acción nacional:** El gobierno, al más alto nivel, debe considerar públicamente un problema de importancia nacional y declarar su solución como una prioridad estratégica nacional.

- **Centrado en el objetivo final**: El gobierno debe enfatizar una visión estratégica orientada al ambicioso objetivo final, con un plazo definido, sin definir prescriptivamente los pasos incrementales necesarios para alcanzar ese objetivo final.

- **Proceso multipartito:** El gobierno debe catalizar el esfuerzo nacional aprovechando sus exclusivas facultades de convocatoria y creando los mecanismos de colaboración apropiados que se requieran para aprovechar formalmente la comunidad de múltiples partes interesadas, incluyendo al menos la industria privada y el mundo académico, para ejecutar el objetivo final estratégico definido.

Definir específicamente el Objetivo de Ciberseguridad

La segunda fase del estudio del NSTAC se centrará en aplicar al ámbito de la ciberseguridad las lecciones aprendidas en estos esfuerzos nacionales del Moonshot. Esta segunda fase tratará de aportar más claridad y recomendaciones sobre las consideraciones clave en materia de ciberseguridad relacionadas con los principios Moonshot identificados (Llamada a la Acción, Enfoque del Objetivo Final y Proceso Multiparticipativo), y otros aún por identificar. Por ello, en esta segunda fase del estudio, el NSTAC escuchará a diversos expertos en ciberseguridad y a otras personas para definir adecuadamente el objetivo final declarado, y los subelementos del objetivo final. Esta fase tratará de responder a la pregunta: *¿Qué es un "moonshot" con un alcance adecuado, aplicado al ámbito de la ciberseguridad?*

5.0 EL GOBIERNO DEBE COLABORAR CON LA INDUSTRIA

El gobierno debe liderar la lucha contra las amenazas de ciberseguridad para nuestro futuro digital conectado. Las amenazas provienen de los estados-nación, el crimen organizado, los hacktivistas, los terroristas y otros. El sector privado no puede hacerlo solo. El Gobierno Federal debe liderar en casa y en el extranjero, fomentando la colaboración entre sectores económicos y fronteras políticas. El NSTAC recomienda las siguientes actividades que el gobierno debe realizar para abordar la seguridad de la IO.

Proteger y ampliar las asociaciones público-privadas, que han sido la base de la ciberpolítica federal. La industria ha colaborado con el DHS en lugares como el NCCIC y el Equipo de Preparación para Emergencias Informáticas de Estados Unidos durante décadas. La industria también trabaja con el gobierno en el CSRIC, el Consejo Asesor de Tecnología y otros ámbitos, como el NIST y la NTIA.

La industria ha colaborado con el gobierno para proteger las infraestructuras críticas. En respuesta a la OE 13636, que pedía la identificación y protección de las infraestructuras críticas, ocho directores ejecutivos del sector financiero iniciaron un esfuerzo para mejorar la ciberseguridad de los servicios financieros básicos, conocido como Centro de Análisis y Resiliencia Sistémica Financiera (FSARC). El FSARC, en colaboración con el gobierno, coordina campañas contra adversarios clave, desarrolla y comparte las mejores prácticas y las lecciones aprendidas, contribuye a los casos penales en apoyo de la aplicación de la ley federal, y aprovecha el acceso y la información del gobierno de EE.UU. para identificar dónde la actividad criminal está alineada o es utilizada por actores de inteligencia extranjeros. [104]El sector privado ayudó a dar forma al Marco de Ciberseguridad del NIST y lo ha aplicado, y los sectores lo han adaptado a sus necesidades específicas. Por ejemplo, el documento final del CSRIC IV de marzo de 2015, *Cybersecurity Risk Management and Best Practices (Gestión de riesgos de ciberseguridad y mejores prácticas)*[105] proporciona orientación para ayudar a los proveedores de comunicaciones a utilizar y adoptar el Marco de Ciberseguridad del NIST. Iniciativas como esta son especialmente útiles para los proveedores más pequeños que operan con presupuestos limitados.

Estas asociaciones se basan en la confianza y deben permanecer libres de la amenaza de la regulación y la aplicación.

Considerar formas creativas de cultivar el intercambio de información sobre vulnerabilidades, incluyendo protecciones de responsabilidad y puertos seguros. Si los operadores y los fabricantes van a hablar de las vulnerabilidades de los productos y servicios, debe haber un reconocimiento de los riesgos asociados al hacerlo, y una protección para dicha actividad. Los programas de divulgación de vulnerabilidades son interesantes, pero pueden carecer de componentes clave para funcionar. En 2016, el DHS señaló que debería convocar a un grupo de socios para considerar la responsabilidad, entre otras cuestiones. [106]El Instituto de la Cámara de Estados Unidos para la Reforma Legal y otros han estado estudiando estas cuestiones, por ejemplo, en *Torts of the Future*, la Cámara señala que "[l]os fabricantes de productos conectados se enfrentan a importantes riesgos de responsabilidad derivados de

[104] Scott DePasquale. Centro de Análisis y Respuesta de Servicios Financieros. *Reunión informativa para el subcomité ICR del NSTAC.* 10 de agosto de 2017

[105] FCC, CSRIC IV, Grupo de Trabajo 4: Informe final*, Grupo de Trabajo de Gestión de Riesgos de Ciberseguridad y Mejores Prácticas*. Marzo de 2015.https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[106] Véase DHS. "Principios estratégicos para asegurar el Internet de las cosas (IoT)". Versión 1.0. 15 de noviembre de 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things- 2016-1115-FINALpdf.

ciberataques o el robo de información privada".[107] El Gobierno Federal debe considerar cómo el riesgo de litigio civil y nuestro sistema judicial litigioso pueden obstaculizar la actividad beneficiosa.

Identificar y abordar los límites legales que restringen las medidas defensivas del sector privado. Las medidas de mitigación de DDoS y otras pueden exponer a las empresas a riesgos en virtud de la legislación federal. También pueden tener consecuencias no deseadas, como el daño a terceros si hay errores de atribución. El gobierno debe identificar sus objetivos de defensa activa y el papel del sector privado. Además, el gobierno debe considerar si las protecciones y autoridades de la CISA son suficientes. La protección para compartir indicadores de ciberamenazas y medidas defensivas [108] puede no ser suficiente. Una protección adecuada de la responsabilidad de los proveedores de servicios de Internet y otros será fundamental para seguir desarrollando las medidas defensivas y el intercambio de información. El lenguaje legislativo de la protección de la responsabilidad debe actualizarse al mismo tiempo que se amplía el papel de los miembros del ecosistema.

Ajustar la forma de operar de la inteligencia estadounidense al abordar las ciberamenazas. El National Infrastructure Advisory Council (NIAC) evaluó recientemente los enfoques del Reino Unido e Israel en materia de recopilación de información. [109] El NIAC sugiere que "la coordinación efectiva a la velocidad, es impulsada por una autoridad central que puede coordinar las prioridades cibernéticas para la nación, alinear los recursos de la industria y el gobierno y proporcionar liderazgo nacional para la defensa cibernética".[110] El informe discute además los esfuerzos en el Reino Unido en la creación del Centro Nacional de Seguridad Cibernética del Reino Unido y la Oficina Cibernética Nacional de Israel. El NSTAC recomienda que el Gobierno de Estados Unidos evalúe estos modelos y determine si alguno de los conceptos que se están desarrollando en el Reino Unido e Israel puede ser útil para organizar los esfuerzos de ciberseguridad del Gobierno de Estados Unidos. El NSTAC también recomienda que Estados Unidos considere la posibilidad de modificar sus métodos de recopilación de ciberinformación permitiendo que un analista se centre exclusivamente en un objetivo durante un periodo más largo, convirtiéndose así en un experto y posiblemente más capaz de combatir un ataque específico de su objetivo.

Mejorar el intercambio de información con el sector privado. El gobierno tiene acceso a información de inteligencia; sin embargo, el proceso para compartir esa información a nivel clasificado puede ser engorroso. El NSTAC recomienda que el Presidente ordene al Gobierno Federal que lleve a cabo una revisión de los programas de información existentes para determinar si están cumpliendo los objetivos y recomendar nuevos enfoques, incluso de forma piloto, para permitir un mejor intercambio de información. El gobierno también debería reconocer que no todos los receptores de información tienen las mismas capacidades. Debería haber una gama de modelos de intercambio de información disponibles en consonancia con las capacidades de cada parte.

Eliminar el exceso de reglamentación a nivel federal, estatal y local. El sector privado está preocupado por las obligaciones reglamentarias, los mandatos técnicos y los regímenes de información que

[107] Instituto de la Cámara de los Estados Unidos para la Reforma Legal. "Torts of the Future-Addressing the Liability and Regulatory Implications of Emerging Technologies". Marzo de 2017. http://www.instituteforlegalreform.com/uploads/sites/1/_Torts_of_the_Future_Addressing_the_Liability_and_Regulatory_Implications_of_Emerging_Technologies_April_2017.pdf?pagename=uploads/sites/1/Torts_of_the_Future_Addressing_the_Liability_and_Regulatory_Implications_of_Emerging_Technologies_.pdf.

[108] Sección 104(c) de la Ley de Intercambio de Información y Cibernética de 2015, 6. U.S.C. 1504.

[109] NIAC. "Securing Cyber Assets-Addressing Urgent Cyber Threats to Critical Infrastructure". Agosto de 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

[110] Informe del NIAC al Presidente "Securing Cyber Assets", en 19 (agosto de 2017), disponible en https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf

agotan recursos valiosos y fomentan una mentalidad de cumplimiento que dará prioridad a la mentalidad de "marcar la casilla" en lugar de una innovación ágil y agresiva. En el espacio de la ciberseguridad, las amenazas, las vulnerabilidades y las respuestas se mueven exponencialmente más rápido de lo que podría hacerlo cualquier regulador. Si el gobierno quiere verdaderos socios, debe dejar claro que la colaboración y los mejores esfuerzos no van a rebotar en el sector privado en la regulación y la aplicación punitiva. El Gobierno Federal debe desalentar la actividad estatal, ya sea en mandatos técnicos, cargas de privacidad en línea u otras medidas, ya que pueden complicar y obstaculizar el desarrollo de productos y servicios.

El gobierno puede reconocer que hay, y seguirá habiendo, actividad estatal, ya sea en mandatos técnicos, cargas de privacidad en línea u otras medidas, y que algunos de estos esfuerzos pueden fragmentar y complicar el desarrollo de productos y servicios. Teniendo en cuenta esta realidad, el NSTAC recomienda que el Gobierno Federal anime a los estados, en primer lugar, a adoptar y aplicar las mejores prácticas y recomendaciones de ciberseguridad disponibles y coherentes para las propias organizaciones y sistemas administrativos de los estados y, a continuación, a promover lo mismo para el ecosistema de residentes y empresas de los estados. Se debería animar a los estados a participar en foros nacionales con las principales partes interesadas para lograr enfoques coherentes hacia la ciberseguridad. Entre ellos deberían figurar la Asociación Nacional de Gobernadores, la Asociación Nacional de Directores Estatales de Información, la Conferencia Nacional de Legislaturas Estatales y el Consejo de Coordinación de Gobiernos Estatales, Locales, Tribales y Territoriales del DHS.

Representar agresivamente la política y los intereses económicos de Estados Unidos en el extranjero. El sector global de las TIC necesita que el Gobierno de Estados Unidos lidere en el extranjero. Las regiones y los países están abordando la seguridad y la tecnología de manera divergente. Es una cuestión de seguridad nacional y de interés económico que Estados Unidos defienda enérgicamente los mercados abiertos, la neutralidad tecnológica y los procesos de normalización transparentes. Si Estados Unidos no lidera, las normas legales y los reglamentos prescriptivos de otras naciones podrían establecer puntos de referencia internacionales y frenar el crecimiento internacional de las empresas estadounidenses.

Promover el desarrollo de la mano de obra en ciberseguridad. Numerosos informes recomiendan que el gobierno aborde las deficiencias de la mano de obra cibernética que pueden paralizar nuestra capacidad de responder a las amenazas crecientes. Algunos ejemplos son el informe del NIAC (que sugiere un programa de intercambio de expertos entre el sector público y el privado, por ejemplo),[111] el informe final del CSRIC, *Cybersecurity Workforce Development Best Practices Recommendations*,[112] varios esfuerzos del DHS, incluida la creación de la National Initiative for Cybersecurity Careers and Studies[113] el National Cybersecurity Workforce Framework,[114] el Cybersecurity Workforce Development Toolkit,[115]

[111] NIAC. "Securing Cyber Assets-Addressing Urgent Cyber Threats to Critical Infrastructure". Recomendación 4. Agosto de 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17- 508.pdf.

[112] CSRIC. Informe final del WG7. "Recomendaciones de mejores prácticas para el desarrollo de la fuerza de trabajo de ciberseguridad". Marzo de 2017. https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.

[113] NICCS, https://niccs.us-cert.gov/.

[114] NICCS. NICE Cybersecurity Workforce Framework. https://niccs.us-cert.gov/workforce-development/cyber- security-workforce-framework.

[115] NICCS. "Cybersecurity Workforce Development Toolkit-Cómo construir una fuerte fuerza de trabajo de ciberseguridad". Marzo de 2017. https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development
El programa de desarrollo de la fuerza de trabajo de la ciberseguridad es una herramienta de trabajo.

y el Informe sobre la mejora de la ciberseguridad en el sector sanitario116 (junio de 2016). Además, es posible que el personal de ciberseguridad tenga que entender tanto la codificación como los idiomas extranjeros, ya que la mayoría de las redes de bots se codifican utilizando idiomas distintos del inglés. Queda mucho trabajo por hacer, pero ha surgido un consenso de que este es un área crítica para la atención del gobierno.

Tenga cuidado al utilizar el sistema de contratación pública para abordar la ciberseguridad de la IO. El gobierno debe pensar en cómo garantizar que sus productos y servicios estén debidamente protegidos. Sin embargo, el gobierno debe evitar centrarse de forma desproporcionada en los dispositivos o basarse en mandatos unilaterales para lograr esta seguridad mejorada. El NSTAC recomienda que el gobierno explore los servicios gestionados que pueden ofrecer los expertos del sector privado. Esto permitiría al gobierno aprovechar la experiencia y la escala del sector privado (proveedores de servicios de Internet, proveedores de la nube, otros que proporcionan servicios a terceros) en lugar de utilizar mandatos de seguridad de dispositivos más rudimentarios.

Desarrollar grupos de reflexión para explorar las oportunidades del Moonshot. En lugar de repetir ideas ya intentadas, como la ampliación de un nuevo protocolo de propiedad intelectual, el gobierno debería identificar nuevos enfoques. El NSTAC recomienda que el gobierno explore la creación de asociaciones y grupos de reflexión colaborativos e innovadores similares al Centro Nacional de Excelencia en Ciberseguridad del NIST, que se asocia con el sector privado, el mundo académico y otros organismos para encontrar soluciones a problemas tecnológicos. Otro enfoque a considerar es una estructura similar a la de la Agencia de Proyectos de Investigación Avanzada de Defensa, centrada en la ciberseguridad, que se beneficia de autoridades de contratación especiales y vehículos de contratación alternativos que permiten a la agencia aprovechar las oportunidades para avanzar en su misión.

6.0 CONCLUSIÓN

Se espera que las redes de bots y los ataques que facilitan no hagan más que crecer. La mitigación de este complejo problema requerirá una serie de acciones de todo el ecosistema de Internet. Aunque este informe ofrece recomendaciones para los fabricantes de dispositivos, los proveedores de servicios de red, los desarrolladores de software, las empresas y el gobierno, no son las únicas entidades que deben participar en la mitigación de la amenaza. La ciberseguridad es una responsabilidad compartida y depende de que cada parte del ecosistema desempeñe un papel. El NSTAC también espera que la gama de soluciones evolucione con el tiempo. Por lo tanto, el NSTAC no prevé que este informe o cualquier otro proceso que le suceda sea estático. Abordar este reto requerirá una colaboración y un compromiso continuos entre el sector privado y el gobierno. Por último, muchas de las recomendaciones son iterativas y no cambiarán fundamentalmente la naturaleza subyacente del problema. Por esta razón, el NSTAC recomienda que en un futuro estudio del NSTAC se investigue la posibilidad de un Moonshot de ciberseguridad que tenga como objetivo la infraestructura subyacente de Internet y recomiende mejoras a largo plazo.

[116] Grupo de trabajo sobre ciberseguridad en la industria sanitaria (Grupo de trabajo HCIC). "Informe sobre la mejora de la ciberseguridad en la industria sanitaria". Recomendación 6.4. Junio de 2017. https://www.phe.gov/Preparedness/planning/ CyberTF/Documents/report2017.pdf.

ANEXO A: MIEMBROS

MIEMBROS DEL SUBCOMITÉ

Sr. Raymond Dolan, Sonus Networks Inc. y copresidente del subcomité Sr. John Donovan, AT&T Inc. y copresidente del subcomité

Sr. Chris Boyer, AT&T Inc. y copresidente del grupo de trabajo ICR Sr. Kevin Riley, Sonus Networks Inc. y copresidente del grupo de trabajo ICR

AT&T, Sr. Inc.	Jonathan Gannon Sr. Bill O'Hern
Avaya, Inc.	Sr. Vico Loquerico
CenturyLink, Inc.	Sra. Kathryn Condello Sr. Paul Diamond Sr. John Schiel Sr. Donald Smith
Tecnologías de la Comunicación, Inc.	Sr. Milan Vlajnic
Departamento del Homeland Security	Sr. Gregory Shannon
Diógenes Group, LLC	Sr. William Gravell
Dun & Bradstreet Sr. Corporation	Gregory Mortensen Sr. Jon Rose
Equinix, Inc.	Sra. Cindy Liu
ForeScout Technologies, Inc.	Sr. Tamer Baker Sra. Katherine Gronberg
Lockheed Martin Corporation	Sr. Darrell Durst
Microsoft Corporation	Sr. Richard Boscovich Sra. Amanda Craig Deckard
McAfee, LLCSr. Patrick Flynn	Sr. Kent Landfield
Seguridad Nacional Sra. Agency	Cheri Caddy
National Telecommunications and Información Administration	Sr. Shawn Cochran Sra. Megan Doscher

	Sra. Evelyn Remaley
National Institute of Standards and Technology	Sr. Tim Polk Sr.
NCTA - The Internet & Television Association	Matt Tooley Sra.
Neustar, Inc.	Terri Claffey
Corporación Oracle	Dr. Prescott Winter Sr.
Palo Alto Networks, Inc.	Sean Morgan Sr.
Raytheon Company Unisys	Michael Daly
Corporation	Sr. Mark Cohn Sr. Tom Patterson
USTelecomm	Sr. Robert Mayer
Verizon Communications, Inc.	Sr. Kevin Kirsche Sr. Timothy Vogel

INFORMADORES - EXPERTOS EN LA MATERIA

Arbor Networks, Inc.	Sra. Arrabelle Hallawell Sr.
AT&T, Inc.	Brian Rexroad Sr. Bill O'Hern
CA Technologies, Inc.	Sr. Jaime Brown
Centro para la Democracia y la Tecnología	Sra. Michelle Richardson Sr.
Consumer Technology Association Cyber	Mike Bergman
Threat Alliance	Sr. Michael Daniel Sr.
Departamento de Defensa	Mitchell Komaroff Dra.
Departamento de Seguridad Nacional	Ann Cox
Departamento de Justicia	Sr. Leonard Bailey
Dun & Bradstreet Corporation	Dr. Anthony Scriffignano Sr.
Embajada de Japón	Daisuke Hayashi

Oficina Federal del Investigation	Sr. Tom Grasso
ForeScout Technologies, Inc.	Sr. Wallace Sann
Financial Services Analysis & Response Sr. Center	Scott DePasquale
Financial Systematic Analysis & Resilience Center	Sr. Bill Nelsen
Ministerio del Interior y Comunicación de Japón	Sr. Atsushi Goto Sr. Yasu Taniwaki
Centro Nacional Japonés de Preparación y Estrategia de la Industria para la Ciberseguridad	Sra. Kasumi Sugomoto
Agencia de Proyectos de Investigación Avanzada de	Sr. Kerry Long Sr.
Inteligencia McAfee Reino Unido	Raj Samani Sr. Steve
Micron Technology, Inc.	Wallach
Microsoft	Sr. Richard Boscovich Sr. Rob Spiger
NCTA - The Internet & Television Association	Sr. Matt Tooley
Agencia de Seguridad Nacional	Sra. Cheri Caddy
Instituto Nacional de Normas y Tecnología	Sr. Andrew Regenscheid Dr. Charles Romine
Neustar, Inc.	Sr. Barrett Lyon Sr.
Oracle	Travis Russell Sr.
Palo Alto Networks, Inc.	Kevin Walsh Sr. J.F.
Raytheon Company sn3rd	Mergen Sr. Sean
LLC	Turner
Corporación Unisys	Sr. Brent Houlahan Sr. Jack Koons
Centro Nacional de Ciberseguridad del Reino Unido	Dr. Ian Levy Dr.
Cuerpo de Marines de los Estados Unidos	Ray Letteer

USTelecom	Sr. Robert Mayer
Venable LLP	Sr. Ari Schwartz
VeriSign, Inc.	Sr. Danny McPherson Dr. Eric Osterweil

GESTIÓN DEL SUBCOMITÉ

NSTAC Federal Designado Officer	Sra. Helen Jackson
Suplente NSTAC DFO	Sra. Sandy Benevides Sra. DeShelle Cleghorn
Booz Allen Hamilton, Inc.	Sra. Ursula Arno Sr. William Hyde
Total Systems Technology Corporation	Sr. Robert Carter

APÉNDICE B: ACRÓNIMO S

5G Quinta generación
ABC Código de Conducta ABC Anti-Botnet
Inteligencia Artificial
BCP Mejores prácticas BCP comunes
Protocolo de BGP pasarela fronteriza
Protocolo BYOD Bring Your Own Device
CharGen del generador de caracteres
Ley de CISA intercambio de información sobre ciberseguridad
Instrucción de la CITL Cybersecurity Independent Testing Laboratory
CNSSI Comisión de Sistemas de Seguridad Nacional
CSRIC Seguridad, fiabilidad e interoperabilidad de las comunicaciones Asociación
de Council CTA Tecnología del Consumidor
CVD Coordinated Vulnerability Disclosure
DDoS Denegación de servicio CVD
Coordinated Vulnerability Disclosure
DDoS distribuida
DHS Departamento de Seguridad Nacional
Sistema de DNS nombres de dominio
DNSSEC Domain Name System Security Extensions DOC
Departamento de Comercio
DoD Departamento de Defensa
DOJ Departamento de Justicia
DoS Denegación de servicio
Orden EO ejecutiva
EOP Executive Office of the President ETSV
Tecnología Emergente Estratégica Vision
FBI Oficina Federal de Investigación
Comisión FCC Federal de Comunicaciones
FSARC Análisis sistémico financiero y resiliencia Comisión
Center FTC Federal de Comercio
Gbps Gigabits por segundo
Asociación GCHQ Government Communications Headquarters
GSMA del Grupo Especial de Móviles
Sistema de ICR Internet and Communications Resilience ICS
control industrial
Foro Technologies IEC International Electrotechnical
Commission IETF Técnico de Ingeniería de la ICT Información y
las Comunicaciones Technologies IEC International Electrotechnical
Commission IETF en Internet
IoT Internet de los objetos
Protocolo de IP Internet
IPv6 Protocolo de Internet versión 6
Proveedores de ISO International Organization for Standardization
ISP servicios de Internet
Tecnología de IT la información
M2M De máquina a máquina
Grupo de M3AAWG trabajo de mensajería, malware y antiabuso en móviles

MUD Fabricante Uso Descripción
Centro NCCIC Nacional de Integración de la Ciberseguridad y las Comunicaciones
NCCoE Instituto Nacional de Normas y Tecnología Centro Nacional de Excelencia en NCCoE Ciberseguridad
Virtualización de NFV funciones de red
Consejo NIAC Consultivo Nacional de Infraestructuras
Dispositivos de NIST National Institute of Standards and Technology
NISTIR NIST Glossary of Information Security Terms NMD monitorización de red
NS/EP Seguridad nacional/preparación para NS/EP emergencias
Protocolo de NSTAC National Security Telecommunications Advisory Committee
NTIA National Telecommunications and Information Administration NTP tiempo de red
Sistema operativo
RPKI Recursos Infraestructura de RPKI Clave Pública
SAFECode Foro de Garantía de Software para la Excelencia en el
Ciclo de Vida Code SDL del Desarrollo de la Seguridad
Red SDN definida por software
SS7 Sistema de señalización 7
Reino Unido
Laboratorio UL Underwriters
Estados Unidos
Red VPN privada virtual

APÉNDICE C: GLOSARIO

5G - Una futura red móvil de quinta generació, cuya especificación la Unión Internacional de Telecomunicaciones no ha definido completamente. Se espera que soporte velocidades de datos de 10 gigabits por segundo y superiores. Los despliegues comerciales de la 5G no se esperan hasta alrededor de 2020. (Diccionario de telecomunicaciones de Newton)

Inteligencia artificial - La inteligencia exhibida por las máquinas o el software. Término popularizado por Alan Turing, históricamente describe una máquina que podría engañar a la gente haciéndoles creer que es un ser humano a través del Test de Turing. Recientemente, los científicos de este campo han abandonado en gran medida este objetivo para centrarse en la singularidad de la inteligencia de las máquinas y aprender a trabajar con ellas de forma inteligente y útil. (Diccionario Telecom de Newton)

Autenticación - El proceso por el cual un usuario, fuente de información o simplemente información demuestra que es quien dice ser; el proceso de determinar la identidad de un usuario que intenta acceder a una red y/o sistema informático. (Diccionario de telecomunicaciones de Newton)

Botnet - Red de ordenadores conectados a Internet que han sido infectados por el software de mando y control de un tercero malintencionado y que pueden ser instruidos remotamente por ese tercero para realizar acciones dañinas como lanzar ataques a través de Internet. (Diccionario de telecomunicaciones de Newton)

Computación en la nube - Modelo que permite el acceso a la red bajo demanda a un conjunto compartido de capacidades/recursos configurables de tecnología de la información, (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios), que pueden ser rápidamente aprovisionados y liberados con un mínimo esfuerzo de gestión o interacción del proveedor de servicios. Permite a los usuarios acceder a servicios basados en la tecnología desde la nube de la red sin tener conocimiento, experiencia o control sobre la infraestructura tecnológica que los soporta. Tanto los datos del usuario como los servicios de seguridad esenciales pueden residir y ser gestionados dentro de la nube de red. (Instrucción del Comité de Sistemas de Seguridad Nacional (CNSSI) 4009, adaptado) (Informe del NSTAC 2016)

Infraestructura **crítica** - Sistema y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud pública nacional o la seguridad, o cualquier combinación de estos asuntos. Las infraestructuras críticas pueden ser propiedad y estar operadas tanto por el sector público como por el privado. *Ley de Protección de Infraestructuras Críticas de 2001*, 42 U.S.C. 5195c(e)] (CNSSI 4009, Adaptado)

Ciberataque - Un ataque, a través del ciberespacio, cuyo objetivo es el uso del ciberespacio por parte de una empresa para interrumpir, inutilizar, destruir o controlar maliciosamente un entorno/infraestructura informática; o destruir la integridad de los datos o robar información controlada. (CNSSI 4009)

Ciberseguridad - La capacidad de proteger o defender el uso del ciberespacio de los ciberataques. (CNSSI 4009)

Ataques de denegación de servicio - Impedir el acceso autorizado a los recursos o retrasar las operaciones de tiempo crítico. El tiempo crítico puede ser de milisegundos o de horas, dependiendo del servicio prestado. (CNSSI 4009)

Ataques de denegación de servicio distribuidos - Una técnica de denegación de servicio que utiliza numerosos hosts para realizar el ataque e impide el acceso autorizado a los recursos o retrasa las operaciones de tiempo crítico. (Glosario de términos de seguridad de la información del NIST - (NISTIR) 7298 - Revisión 2)

Cortafuegos: pieza de hardware o software, o hardware y software, que impide que personas no autorizadas accedan a un ordenador o red informática. (Diccionario de telecomunicaciones de Newton)

Internet de los objetos - El conjunto de redes de dispositivos interconectados. (Diccionario de telecomunicaciones de Newton)

Protocolo de Internet (IP) - Parte de la familia de protocolos del Protocolo de Control de Transmisión/IP que describe el software que rastrea la dirección de Internet de los nodos, encamina los mensajes salientes y reconoce los mensajes entrantes. También se utiliza en las pasarelas para conectar redes de nivel 3 de interconexión de sistemas abiertos y superiores. (Diccionario de telecomunicaciones de Newton)

Malware - Software creado y distribuido con fines maliciosos, como invadir los sistemas informáticos en forma de virus, gusanos u otros complementos y extensiones que enmascaran otras capacidades destructivas. (Diccionario Newton Telecom)

Comunicaciones de **Seguridad Nacional/Preparación para Emergencias (NS/EP)** - Servicios de telecomunicaciones que se utilizan para mantener un estado de preparación o para responder y gestionar cualquier evento o crisis (local, nacional o internacional) que cause o pueda causar lesiones o daños a la población, daños o pérdidas de bienes, o que degrade o amenace la postura NS/EP de los Estados Unidos (47 Code of Federal Regulations Chapter II, § 201.2(g)). Las comunicaciones NS/EP incluyen principalmente aquellas capacidades técnicas apoyadas por políticas y programas que permiten al Poder Ejecutivo comunicarse en todo momento y bajo cualquier circunstancia para llevar a cabo las funciones esenciales de su misión y responder a cualquier evento o crisis (local, nacional o internacional), para incluir la comunicación consigo mismo; los poderes Legislativo y Judicial; los gobiernos estatales, territoriales, tribales y locales; las entidades del sector privado; así como el público, los aliados y otras naciones. Las comunicaciones NS/EP incluyen además aquellos sistemas y capacidades a todos los niveles del gobierno y del sector privado que son necesarios para garantizar la seguridad nacional y para gestionar eficazmente los incidentes y las emergencias. (Definición del Comité Ejecutivo de Comunicaciones NS/EP basada en la Orden Ejecutiva 13618, *Asignación de funciones de comunicaciones de seguridad nacional y preparación para emergencias* [2012])

Redes - Sistema(s) de información implementado(s) con una colección de componentes interconectados, que pueden incluir routers, hubs, cableado, controladores de telecomunicaciones, centros de distribución de claves y dispositivos de control técnico. (Glosario de términos de seguridad de la información del NIST (NISTIR) 7298 - Revisión 2)

Virtualización de la red - Un medio para mejorar la eficiencia de una red y reducir los costes. Consiste en crear múltiples particiones virtuales en un único hardware. Reduce el

cantidad de hardware de red necesario y permite gestionar múltiples funciones desde una única consola. (Diccionario de telecomunicaciones de Newton)

Protocolo - Conjunto de reglas y formatos, semánticos y sintácticos, que permiten a los sistemas de información intercambiar información. (Glosario de términos de seguridad de la información del NIST - NISTIR 7298 - Revisión 2)

Red definida por **software** - Una red privada virtual. En concreto, se refiere al servicio de red definida por software de AT&T, que se introdujo en 1985 para los clientes más importantes de AT&T y que sólo proporcionaba servicios de acceso dedicado. (Diccionario de telecomunicaciones de Newton)

Amenaza - Cualquier circunstancia o evento con el potencial de impactar negativamente en las operaciones de la agencia (incluyendo su misión, funciones, imagen o reputación), los activos de la agencia o los individuos a través de un sistema de información mediante el acceso no autorizado, la destrucción, la divulgación, la modificación de la información y/o la denegación de servicio. (NIST SP 800-53, CNSSI 4009, adaptado)

APÉNDICE D: BIBLIOGRAFÍA Y

AT&T. *Prácticas de la red*. 24 de abril de 2017. https://www.att.com/gen/public-affairs?pid=20879.

Arbor Networks. *Worldwide Infrastructure Security Report,* Volume XII, disponible en https://www.arbornetworks.com/insight-into-the-global-threat-landscape

Bailey, Leonard. DOJ. *Sesión informativa para el Subcomité ICR del NSTAC*. 10 de agosto de 2017.

Bergman, Mike. CTA. Sesión informativa para *el Subcomité ICR del NSTAC*. 3 de agosto de 2017.

Boscovich, Richard. Microsoft. Sesión informativa para *el subcomité ICR del NSTAC*. 16 de agosto de

2017. Boyer, Chris. Copresidente de política pública del M3AAWG (AT&T), Nuevo *informe de métricas*

del M3AAWG Bot.
Comparte la perspectiva de los operadores de redes. 20 de octubre de 2014. https://www.m3aawg.org/blog/nuevo-m3aawg-bot-metrics-informe-participaciones-redes-operadoras%E2%80%99-perspectiva.

Burke, Samuel. CNN. *La empresa china reconoce su papel involuntario en el ciberataque.* 24 de octubre de 2016. http://money.cnn.com/2016/10/23/technology/ddos-cyber-attack-chinese- firm/index.html.

Cisco*. Índice de redes visuales de Cisco: Previsión y metodología, 2016-2021, libro blanco*. 7 de junio de 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual- networking-index-vni/complete-white-paper-c11-481360.html.

Ley de Fraude y Abuso Informático (CFAA) (18 U.S.C. § 1030); Ley de Escuchas Telefónicas (18 U.S.C. § 2511); Estatutos de Registro de Plumas/Trap and Trace (18 U.S.C. §§ 3121 *et seq.*); Leonard Bailey. *Sesión informativa para el Subcomité ICR del NSTAC*. 10 de agosto de 2017.

Computer Weekly, "Global Hacker Botnet Tops 6 Million Hijacked Devices", 27 de septiembre de 2017 http://www.computerweekly.com/news/450427023/Global-hacker-botnet-tops-6- million-hijacked-devices.

Asociación de Consumidores de Tecnología, *Resumen del proyecto: Securing Connected Devices for Consumers in the Home, CTA-CEB33,* 7 de julio de 2017. https://standards.cta.tech/apps/group_public/project/details.php?project_id=429.

Cox, Ann. DHS*. Sesión informativa para el Subcomité ICR del NSTAC.* 1 de agosto de

2017. Cyber Independent Testing Lab (CITL). http://cyber-itl.org/.

Ley de intercambio de información sobre ciberseguridad de 2015, Pub. L. No. 114-113, 129 Stat. 2242 (2015).

CSRIC. Informe final del WG7. "Recomendaciones de mejores prácticas para el desarrollo de la fuerza de trabajo de ciberseguridad". Marzo de 2017. https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.

Departamento de Defensa (DoD). "El Departamento de Defensa anuncia la política de divulgación de vulnerabilidades digitales y el lanzamiento de "Hack the Army"". *Comunicado de prensa*. 21 de noviembre de 2016. https://www.defense.gov/ News/News-Releases/News-Release-View/Article/1009956/dod-announces-digital- vulnerability-disclosure-policy-and-hack-the-army-kick-off/.

Departamento de Salud y Servicios Humanos (HHS). "Postmarket Management of Cybersecurity in Medical Devices-Guidance for Industry and Food and Drug Administration Staff". 28 de diciembre de 2016. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

Departamento de Seguridad Nacional (DHS). "Principios estratégicos para asegurar el Internet de las cosas (IoT)". Versión 1.0. 15 de noviembre de 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115- FINAL .....pdf.

DHS. Equipo de Preparación para Emergencias Informáticas de los Estados Unidos. *Build Security In.* https://www.us- cert.gov/bsi.

Departamento de Justicia (DOJ), *A Framework for a Vulnerability Disclosure Program for Online Systems* julio de 2017. https://www.justice.gov/criminal-ccips/page/file/983996/download.

DOJ. "AlphaBay, el mayor 'mercado oscuro' online, cierra". 20 de julio de 2017. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

DOJ. "El Departamento de Justicia toma medidas para desactivar una red de bots internacional". 13 de abril de 2011. https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.

Grupo de especialización industrial del ETSI NFV. *Perspectivas de los operadores de red sobre las prioridades de la NFV para la 5G.* 21 de febrero de 2017. https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf

Informe de movilidad de Ericsson. *En el pulso de la sociedad en red.* Junio de 2016. https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.

Comisión Federal de Comunicaciones (FCC), Communications Security Reliability and Interoperability Council (CSRIC) III*, U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers*, marzo de 2012. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/ CSRIC-III-WG7-Final-ReportFinal.pdf.

FCC, CSRIC II, Grupo de Trabajo 2A: Informe final*, Mejores prácticas de ciberseguridad*. Marzo de 2011. https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final- Report.pdf.

FCC, CSRIC IV, Grupo de Trabajo 4: Informe final*, Grupo de Trabajo de Gestión de Riesgos de Ciberseguridad y Mejores Prácticas*. Marzo

2015.https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815. pdf.

FCC CSRIC V, Informe Final del Grupo de Trabajo 5, *Intercambio de Información,* 15 de marzo de 2017. https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf.

FCC CSRIC. Informe final del Grupo de Trabajo 7, *Recomendaciones de mejores prácticas para el desarrollo de la fuerza de trabajo de ciberseguridad.* Marzo de 2017. https://www.fcc.gov/files/csric5-wg7- finalreport031517pdf.

FCC CSRIC V, Grupo de Trabajo 10, Reducciones del riesgo de legado (2017) (Informe sobre reducciones del riesgo de legado), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

Fitzgerald, Brian y Chris Wysopal. Veracode*. Reunión informativa para el subcomité ICR del NSTAC.* 1 de agosto de 2017.

Comisión Federal de Comercio (FTC). "Anuncia el ganador de su concurso de seguridad para dispositivos domésticos del Internet de las cosas". *Comunicado de prensa*. 26 de julio de 2017. https://www.ftc.gov/news-events/press- releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

FTC. "La FTC aprueba la orden final que resuelve los cargos contra TRENDnet. Inc." *Comunicado de prensa*. 7 de febrero de 2014. https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc; https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

FTC. Internet de los objetos: Privacy & Security in a Connected World. n.130. Enero de 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report- november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

FTC. Desafío del inspector del hogar de IoT. 2017. https://www.ftc.gov/iot-home-inspector-challenge. FTC.

Staff Report. *Internet of Things: Privacy & Security in a Connected World, FTC.* Enero 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet- things-privacy/150127iotrpt.pdf.

Franceschi-Bicchierai, Lorenzo, *How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet.* 29 de septiembre de 2016. https://motherboard.vice.com/en_us/article/ 8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs.

Universidad George Washington, Centro de Seguridad Cibernética y Nacional. *Hacia la zona gris: El sector privado y la defensa activa contra las ciberamenazas.* Octubre de 2016. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

GSA. Política de divulgación de vulnerabilidades. https://18f.gsa.gov/vulnerability-disclosure-policy/.

GSMA. Directrices de seguridad del IoT. Febrero de 2016. https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/.

Hallawell, Arrabelle. Arbor Networks, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 3 de agosto de 2017.

Hartnett, Kevin. WIRED. *Los informáticos se acercan a un código perfecto y a prueba de piratas informáticos.* 23 de septiembre de 2016. https://www.wired.com/2016/09/computer-scientists-close-perfect- hack-proof-code/.

Grupo de trabajo sobre ciberseguridad del sector sanitario. *Informe sobre la mejora de la ciberseguridad en el sector sanitario.* Junio de 2017. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

Yo soy la Caballería. *DOT Gov Coordinated Disclosure Timeline.* https://www.iamthecavalry.org/wp-content/uploads/2016/12/IATC_Gov-Coordinated-Disclosure-Timeline_v1.0.jpg.

Incapsula. *Global DDoS Threat Landscape.* https://www.incapsula.com/ddos-report/ddos-report- q1-2017.html.

Koeberl, Patrick, et, al. "TrustLite: A Security Architecture for Tiny Embedded Devices". http://www.icri-sc.org/fileadmin/user_upload/Group_TRUST/PubsPDF/trustlite.pdf

Lerner, Zach, "Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets", 28 HARV. J.L. & TECH. 237, 247 (2014).

Letteer, Ray. Cuerpo de Marines de los Estados Unidos. *Sesión informativa para el subcomité ICR del NSTAC*.

30 de agosto de 2017. Levy, Ian. Centro Nacional de Ciberseguridad del Reino Unido. *Reunión informativa para*

el Subcomité del NSTAC ICR.
9 de agosto de 2017.

McAfee. *Ataque de la red de bots Mirai IoT: Una ilustración del honeypot.* 5 de abril de 2017. https://www.youtube.com/watch?v=vnitAXYGmI0.

McAfee. Secure Home Platform Service. https://securehomeplatform.mcafee.com/. Microsoft. ¿Qué es el

ciclo de vida del desarrollo de la seguridad? https://www.microsoft.com/en-us/sdl/default.aspx.

Mitchell, Charlie. "El fundador de Black Hat considera que la responsabilidad del software es el principal reto de la política de ciberseguridad". *Inside Cybersecurity*. 26 de julio de 2017. https://insidecybersecurity.com/daily- news/black-hat-founder-sees-software-liability-major-cybersecurity-policy-challenge.

Administración Nacional de Seguridad Vial (NHTSA). "Mejores prácticas de ciberseguridad para vehículos modernos". Octubre de 2016. https://www.nhtsa.gov/staticfiles/nvs/pdf/812333 Ciberseguridad para vehículos modernos.pdf.

NIAC. "Securing Cyber Assets-Addressing Urgent Cyber Threats to Critical Infrastructure". Agosto de 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft- report-08-15-17-508.pdf.

Network Functions Virtualization-White Paper on NFV Priorities for 5G. 21 de febrero de 2017. https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf.

NICCS. NICE Cybersecurity Workforce Framework. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

NICCS. "Cybersecurity Workforce Development Toolkit-How to Build a Strong Cybersecurity Workforce". Marzo de 2017. https://niccs.us-cert.gov/sites/default/files/documents /pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf.

Instituto Nacional de Normas y Tecnología (NIST). *Marco para mejorar la ciberseguridad de las infraestructuras críticas*. 12 de febrero de 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

NIST. Publicación especial 800-193. *Directrices de resiliencia del firmware de la plataforma.* Mayo de 2017. https://csrc.nist.gov/csrc/media/publications/sp/800-193/draft/documents/sp800-193-draft.pdf

Boletín del Laboratorio de Tecnología de la Información (ITL) del NIST. *Reduciendo drásticamente las vulnerabilidades del software.* Enero de 2017. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=922589.

Boletín del NIST ITL. *Adaptación de los controles de seguridad para los sistemas de control industrial.* Noviembre de 2015. http://csrc.nist.gov/publications/nistbul/itlbul2015_11.pdf.

Administración Nacional de Telecomunicaciones e Información (NTIA). *Catalog of Existing IoT Security Standards (Draft Version 0.01),* NTIA Multistakeholder Process on IoT Security Upgradability and Patching, Existing Standards, Tools, and Initiatives Working Group. Julio de 2017. https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.

NTIA. Consejo de Coordinación del Sector de las Comunicaciones. *Libro blanco técnico del sector*. 17 de julio de 2017. https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.

NTIA. *Proceso multilateral: Vulnerabilidades de ciberseguridad*. 15 de diciembre de 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilidades.

NSTAC. *Informe del NSTAC al Presidente sobre el Internet de las Cosas*. November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

O'Hern, Bill. AT&T, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 20 de julio de 2017.

Olmstead, Kenneth y Aaron Smith. "Los estadounidenses y la ciberseguridad". *Pew Research Center Informe.* en 19. 26 de enero de 2017. http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.

Pahl, Thomas B. FTC. *Comience con la seguridad - y siga con ella*. 28 de julio de 2017. https://www.ftc.gov/news-events/blogs/business-blog/2017/07/start-security-stick-it.

SafeCode. https://safecode.org/about-safecode/.

Samani, Raj. McAfee, Reino Unido. *Sesión informativa para el subcomité ICR del NSTAC*. 15 de agosto

de 2017. Sann, Wallace. ForeScout. Sesión informativa para *el subcomité ICR del NSTAC*. 22 de agosto

de 2017. Sandvine, *Fenómenos globales de Internet: Tráfico de Internet encriptado*. 2016. https://www.sandvine.com/resources/global-internet-phenomena/spotlight/internet-traffic-encryption.html.

Schneier, Bruce. *Tenemos que salvar a Internet del Internet de las cosas*. 6 de octubre de 2016. https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html.

Scriffignano, Anthony. Dun & Bradstreet, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 15 de agosto de 2017.

Proyecto Spamhaus. *Los peores países del mundo en materia de botnets.* 18 de agosto de 2017. https://www.spamhaus.org/statistics/botnet-cc/.

Symantec. *Mirai: Lo que hay que saber sobre la botnet que está detrás de los últimos grandes ataques DDoS.* 27 de octubre de 2016. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks.

Tooley, Matt. National Cable and Television Association (NCTA), Communications Sector Coordinating Council, *Industry Technical White Paper on Botnets and Automated Threats*.

Instituto de la Cámara de los Estados Unidos para la Reforma Legal. "Torts of the Future-Addressing the Liability and Regulatory Implications of Emerging Technologies". Marzo de 2017. http://www.institutefor legalreform.com/uploads/sites/1/_Torts_of_the_Future_Addressing_the_Liability_and_Regulory_Implications_of_Emerging_Technologies_April_2017.pdf?pagename=uploads/sites/1/Torts_of_the_Future_Addressing_the_Liability_and_Regulatory_Implications_of_Emerging Tecnologías_.pdf.

Wallach, Steve. Micron Technology, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 7 de septiembre de 2017.

Walsh, Kevin. Palo Alto Networks, Inc. *Reunión informativa para el subcomité ICR del NSTAC*. 18 de julio de 2017.

Warner, Mark. "Los senadores presentan una legislación bipartidista para mejorar la ciberseguridad de los dispositivos del Internet de las cosas". *Comunicado de prensa*. 1 de agosto de 2017. https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63- B9B4-523E18DADB36.

Oficina del Secretario de Prensa de la Casa Blanca. *Orden Ejecutiva 13800, Fortalecimiento de la ciberseguridad de las redes federales y la infraestructura crítica*. 11 de mayo de 2017. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

Xfinity. *Lista de puertos bloqueados de Comcast.* https://www.xfinity.com/support/internet/list-of-blocked-ports/.

Zetter, Kim. "Léxico Hacker: ¿Qué son los ataques DoS y DDoS?" *Wired.* 16 de enero de 2016. https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/.