ieee.es
Instituto Español de Estudios Estratégicos

Documento
Informativo

71/2012 13 noviembre de 2012

Mª José Caro Bejarano

GUÍA DE CIBERSEGURIDAD PARA LA NUEVA ETAPA ESTADOUNIDENSE

Visitar la WEB Recibir BOLETÍN ELECTRÓNICO

GUÍA DE CIBERSEGURIDAD PARA LA NUEVA ETAPA ESTADOUNIDENSE

Resumen:

En la campaña presidencial estadounidense, el Centro para una Nueva Seguridad Americana editó una guía sobre seguridad nacional, para que estos asuntos estuvieran presentes en la campaña electoral. Esta guía plantea varios temas de interés para la seguridad, entre ellos, la ciberseguridad. Aunque la incógnita sobre la identidad del nuevo presidente de EE.UU. ya se resuelto, la guía sigue siendo útil para centrar las preocupaciones sobre la seguridad nacional de este país.

Abstract:

In the presidential election campaign, the Center for a New American Security, CNAS, released a guide to national security, so that these issues were present in the election campaign. This guide addresses various national security issues, including cybersecurity. Although the mystery of the identity of the new U.S. president is already solved, the guide is still useful to focus the national security concerns of this country.

Palabras clave:

Seguridad Nacional, ciberseguridad, CNAS, ciberamenazas, protección de infraestructuras críticas.

Keywords:

National security, cyber security, CNAS, ciber threats, critical infrastructure protection.

INTRODUCCIÓN

El Centro para una Nueva Seguridad Americana (Center for a New American Security - CNAS[1]) editó una guía sobre seguridad nacional para las elecciones presidenciales de EE.UU. Este centro considera que debido a los problemas económicos del país, durante la campaña de las elecciones presidenciales, los asuntos de seguridad nacional no han recibido la merecida atención por parte de los candidatos, los medios de comunicación, y por extensión, por la opinión pública estadounidense.

En esta guía se plantean varios temas de interés para el país a los que se enfrenta antes y después de la campaña electoral como son: la disminución en el presupuesto de defensa, la situación en Afganistán, los antagonismos con China, la escalada nuclear de Irán, la guerra civil en Siria, la proliferación nuclear de Corea del Norte, la situación de la Ciberseguridad, las políticas sobre Energía y la lucha contra el cambio climático.

Un grupo de expertos de este centro elaboró esta guía orientada a ayudar a los votantes estadounidenses, socios globales y otros observadores interesados a comprender mejor los temas de seguridad nacional que impactarán en sus vidas y en la nación en la próxima década e incluso, más allá, con objeto de que durante la campaña presidencial plantearan preguntas a ambos candidatos sobre los temas propuestos:

- La inversión en una defensa nacional fuerte que satisfaga las necesidades de seguridad al tiempo que se alcanza la eficiencia que permita ahorrar impuestos.
- Guiar la reducción de tropas en Afganistán y determinar el papel de EE.UU. durante 2014.
- Impedir que Irán y Corea del Norte avancen en sus programas de armas nucleares.
- Conducir la guerra civil en Siria y sus repercusiones en la región.
- Gestionar la relación con China y ampliar el compromiso de EE.UU. en Asia-Pacífico.
- Desarrollar medios efectivos para abordar los desafíos a la ciberseguridad nacional.
- Establecer políticas que aumenten la seguridad energética nacional al tiempo que se lucha contra el cambio climático.

Esta guía examina cada uno de estos desafíos mediante la definición del tema, la proporción de información y análisis, descripción de los principales puntos de decisión para el presidente y para elevar cuestiones para los candidatos. Aunque ya han pasado las elecciones y se ha resuelto la incógnita de la identidad del próximo presidente, la guía es

[1] Se puede consultar la web http://www.cnas.org/

igualmente útil para plantear las necesidades de seguridad nacional más imperiosas en ese país.

LA CUESTIÓN DE LA CIBERSEGURIDAD

Centrándonos en la cuestión de la ciberseguridad, esta guía reclama al presidente el mantenimiento de un ciberespacio abierto, seguro y resiliente (es decir, con capacidad de resistencia y recuperación ante problemas o ataques) en colaboración con empresas privadas y gobiernos de otros países. EE.UU. tiene más de 242 millones de usuarios en Internet, por ello la red de redes es vital en el crecimiento económico y la innovación, contribuye a la comunicación global y forma parte de la vida cotidiana. No obstante, el acceso a estas tecnologías de la información se ve amenazado por una variedad de amenazas, que también afectan a los intereses económicos y de seguridad nacionales. Estas amenazas incluyen la ciberguerra por parte de actores estatales y no estatales, el ciberespionaje que roba secretos nacionales y propiedad intelectual de compañías privadas, la ciberdelincuencia que cuesta miles de millones de dólares cada día y la llamada ciberagitación referida a aquellos con objetivos políticos o ideológicos. Los decisores políticos reconocen la amenaza, pero aún no han alcanzado un consenso sobre el equilibrio entre privacidad y seguridad, la regulación gubernamental y las iniciativas del sector privado, y las restricciones en Internet frente a la libertad que ha producido beneficios económicos y sociales sin precedentes. Este debate sobre cómo y cuándo utilizar ciberarmas de tipo ofensivo está en sus inicios y aún no se comprende bien el alcance y escalada de un ciberconflicto.

ANTECEDENTES

Ciberatacantes con una amplia variedad de motivaciones lanzan sus ataques contra infraestructuras críticas como redes eléctricas, plantas nucleares, instituciones financieras y plantas de tratamiento de aguas. Según el general Keith Alexander, que dirige la Agencia de Seguridad Nacional y el U.S. Cyber Command, el número de ataques sobre infraestructuras críticas aumentaron 17 veces entre 2009 y 2011. Estos ataques procedían de bandas criminales, hackers y otras naciones. Como ejemplo de ello, las noticias de septiembre de 2012 revelaron que hackers iraníes habían lanzado con éxito un ataque masivo de denegación de servicio distribuido contra las páginas web del Banco de América y la compañía JPMorgan Chase & Co.

Además el ritmo de los ataques se está acelerando. Según un informe del gobierno de 2011, los hackers extranjeros, tanto individuales como de gobiernos, aumentan el robo de secretos

militares, datos sensibles, propiedad intelectual, y tecnologías propietarias cuyo desarrollo cuesta millones de dólares y cientos de millones en beneficios potenciales.

La ciberdelincuencia también crece. Aunque es difícil establecer estimaciones concretas de su coste, la empresa de seguridad Symantec estima que la ciberdelincuencia o cibercrimen cuesta a las empresas unos 114 mil millones cada año y hasta 274 mil millones si se incluyen los costes del tiempo de recuperación.

Los llamados "Hacktivistas" o ciberactivistas políticos o ideológicos roban información confidencial y la usan para avanzar en sus propias agendas políticas o ideológicas. En 2010 el grupo Wikileaks publicó miles de cables sensibles de la diplomacia de EE.UU., lo que creó algunas tensiones con sus aliados.

NECESIDADES PÚBLICAS EN MANOS PRIVADAS

El gobierno de EE.UU. no puede abordar estas ciberamenazas sin comprometer activamente al sector privado, ya que la industria privada es propietaria y opera la mayoría de las redes cibernéticas y las infraestructuras críticas del país. Las empresas privadas de la base industrial de defensa desempeñan un papel crítico, puesto que controlan las redes que alojan información sensible sobre las capacidades militares. El sector privado es también la fuente primordial de innovaciones tecnológicas para prevenir y responder a las ciberamenazas.

CIBERARMAS

EE.UU. continua con el desarrollo de armas cibernéticas ofensivas y, según los medios de comunicación, ha utilizado estas armas contra el programa nuclear Iraní. Como respuesta a los ciberataques, el gobierno de EE.UU. ha aclarado que se reserva el derecho a responder a un ciberataque con medidas diplomáticas, económicas, militares o cibernéticas. El debate sobre cuándo y cómo usar las ciberarmas y cómo evitar que los ciberconflictos escalen hacia una guerra a gran escala permanece bajo secreto y parece estar en sus primeras fases de estudio.

LEGISLACIÓN FALLIDA

En agosto de 2012, el proyecto de ley presentado por los dos partidos para abordar las amenazas a la ciberseguridad fracasó en el Senado. El proyecto de ley fracasó ampliamente porque los grupos empresariales se opusieron a proporcionar voluntariamente estándares

de ciberseguridad. La administración Obama estaba desarrollando un Decreto para alcanzar algunos de los objetivos de esa legislación.

Sin embargo, todas las disposiciones de la fallida ley no se pueden instituir mediante Decreto. Por ejemplo, un Decreto no puede proporcionar responsabilidad civil a las empresas que compartan información sensible con el gobierno, y tampoco puede eximir de los requisitos de servicio estándar en la contratación cibernética.

PUNTOS DE DECISIÓN

En esta próxima etapa presidencial se deben abordar un amplio abanico de ciberamenazas:
• trabajar con países aliados o de ideas afines y con el sector privado para incrementar la ciberseguridad al tiempo que se promociona la libertad en Internet.
• trabajar con el Congreso para aprobar la legislación de protección de infraestructuras criticas y facilitar la compartición de información sobre ciberamenazas mientras se calman las preocupaciones de los abogados privados y la comunidad empresarial.
• Elegir cuándo y cómo usar las ciberarmas, en tanto que se estudian los precedentes que estas decisiones sentarán para otros países.
• Formar a personal en ciberseguridad y animar el desarrollo de hardware, software y redes que sean menos vulnerables a los ciberataques.

Mª José Caro Bejarano
Analista del IEEE