NOTA DE FUTURO 8/2017

13 de diciembre de 2017

Silvia Rodríguez[*]

Tendencias en Tecnología y Seguridad digital

Métodos de análisis y utilidad de las nuevas tecnologías para la prevención de amenazas

Nota de futuro: Tendencias en Tecnología y Seguridad digital

Métodos de analisis y utilidad de las nuevas tecnologías para la prevención de amenazas

Este artículo es una síntesis y traducción de: George Washington University Center for Cyber & Homeland Security (CCHS), 'Trends in Technology and Digital Security, Fall 2017 Symposium – Compendium of Proceedings', George Washington University Center for Cyber & Homeland Security (CCHS), 16 de noviembre de 2017

La seguridad nacional en una época de rápido cambio tecnológico

El cambio tecnológico es sorprendente. Hoy hay un mayor número de ingenieros y los nuevos descubrimientos tecnológicos son fácilmente incorporables. La cara oscura de esto es que hay más tecnologías de las que preocuparse. Esta acumulación de riesgos incluye oportunidades ofensivas asimétricas que incrementan el precio de los sistemas defensivos y ponen en riesgo su efectividad.

Las tecnologías más desestabilizadoras están al alcance de cualquiera. El periodo de superioridad de Estados Unidos en temas de defensa e innovación tecnológica está en decadencia. Este cambio en el entorno tecnológico es cada vez más complicado y, desde el punto de vista estadounidense, habría que centrarse en las amenazas que presentan riesgos existenciales al país.

La biología tiene características que pueden ser preocupantes. ¿Qué pasaría si el enemigo pudiera crear enfermedades? Los organismos biológicos pueden utilizarse como armas. Todo lo que se necesita es la secuencia de ADN o ARN para codificar el virus y productos químicos para convertir dicho código en algo biológico. La biología se ha transformado en informática e ingeniería. Hoy cualquiera puede comprar equipamiento y desarrollar un virus en su garaje.

El fácil acceso y habilidades necesarios representan un problema importante de inteligencia nacional. Es difícil rastrear armas biológicas y el número de actores del que preocuparse es elevado. Además, los accidentes también pueden llegar a ser catastróficos.

Ante esta situación, debemos pensar en una nueva fenomenología que pueda ayudar a revelar este tipo de actividades. Debemos mejorar la Inteligencia de Reconocimiento y Signatura (MASINT) para ser capaces de analizar las actividades químicas, biológicas, radiológicas y nucleares desde la distancia. Asimismo, Estados Unidos debe mejorar sus capacidades.

* Alumna en prácticas de la Universidad Pontificia de Comillas

Las opiniones contenidas en las notas CAP son responsabilidad de sus autores, sin que reflejen necesariamente la opinión del Centro de Análisis y Prospectiva de la Guardia Civil

La previsión de amenazas: métodos y herramientas

La misión de la Comunidad de Inteligencia consiste en evitar la sorpresa: entender las amenazas, verlas con antelación y actuar. Si nos centramos en el futuro, vemos que hay una transformación en la información digital y el *big data*. Ahora existe mayor oportunidad para recopilar, guardar y analizar más información que nunca. En términos de herramientas y equipamiento, habría que considerar al superordenador Oak Ridge, que funcionará en menos de cinco años, como el más poderoso del mundo.

En Estados Unidos, donde se entrena a la gente para ser los mejores, existe un problema con la alerta anticipada. Un área en la que claramente no se ha actuado bien en cuanto a la previsión de amenazas es la ciberseguridad, compuesta de tres ejes: inteligencia digital (recolección y análisis); infraestructura de confianza (medidas defensivas y el análisis que se aplica); y un apuntalamiento por el flujo de trabajo analítico y la habilidad de realizar operaciones más rápidas.

Los conocimientos sobre amenazas deben ser prácticos y oportunos. Deben adaptarse a nuestro entorno y aquí es cuando se falla. Adaptar la inteligencia a dicho entorno significa que hay que dar respuesta a ciertas preguntas. Para ello, debemos conocer nuestras prioridades y hacer que los analistas de ciberseguridad se centren en las amenazas más importantes. Por lo tanto, hay tres niveles en los que se debe actuar: estratégico, operativo y táctico.

Asimismo, también existe una cuestión transversal en la ciberseguridad: la biología y la seguridad de la información, que juntas presentan una situación para la que los analistas no están preparados.

Con la previsión y análisis de amenazas, las oportunidades tienen un doble filo, pues los adversarios tienen capacidades similares a las nuestras en temas de innovación y velocidad, lo que sobrepasa nuestras defensas.

En este sentido es importante separar lo conocido de lo desconocido. Los seres humanos no tienen la capacidad de predecir, algo que la tecnología cada vez tiene más capacidad de hacer. Por lo tanto, este es un área en la que quizás los seres humanos no puedan aportar demasiado. Los conocimientos desconocidos (*unknown knows*) necesitan automatizarse. Lo mismo ocurre en el ámbito de los desconocimientos desconocidos (*unknown unknows*).

¿Dónde nos lleva esto? Hay que mirar hacia dentro y descubrir cuáles son los activos digitales que necesitan protección. Volviendo al tema de la biología, lo más crítico es el genoma humano, así

como la seguridad de la información acompañada de la biología y la nanotecnología. Esto no es ficción y las lecciones del pasado están claras: hay que compartir información y no olvidar que la posibilidad de que ocurran accidentes tecnológicos es una realidad.

La Inteligencia Artificial en ciberseguridad: implicaciones éticas y tecnológicas

Tecnologías emergentes: el impacto en la fuerza laboral

Se ha explorado el impacto de las tecnologías emergentes en la fuerza laboral, incluyendo la automatización y la inteligencia artificial (IA). Se han considerado 43 posibles futuros escenarios ubicados entre 10 y 20 años en el futuro y se han reducido a cuatro categorías: el primero es un futuro de menos trabajo, hecho de forma no tradicional, donde el trabajo "sucio" lo llevarían a cabo las máquinas y los seres humanos se encargarían de la prestación de cuidados y los trabajos artesanales. En el segundo, menos gente tendría trabajo y habría más competitividad. El tercer futuro recibe el nombre de "mundo grupal", ya que la mayoría de empleos serían proyectos grupales y la mayoría de la gente tendría ingresos de diferentes fuentes. Finalmente, el último es un mundo en el que casi todos se verían sobrepasados por la tecnología.

Había tres perspectivas comunes en estos mundos. La primera, el modelo de educación que utilizamos hoy, en el que una persona se centra en aprender algo a lo largo de su educación secundaria y la universidad y espera utilizar dichos conocimientos toda su vida. La segunda, que la gente tendría más responsabilidad en encontrar y prepararse para el tipo de trabajo que quiera hacer. La tercera, que la naturaleza de los trabajos sería entre un 20% y un 30% grupal.

La ciberseguridad es un ejemplo interesante de esto, pues hay cientos de miles de puestos de trabajo que no llegan a cubrirse. Con la expansión en el campo de la ciberseguridad, se necesitan encontrar formas de identificar, preparar y conseguir gente nueva que destaque. Un argumento en contra es que, ya que la demanda de profesionales supera la oferta en ciberseguridad, probablemente, los softwares de IA ocuparán dichos puestos.

El aprendizaje profundo de las redes neuronales: combatiendo los Malware[1]

Nuestras defensas en temas de seguridad como nación no están lo suficientemente preparadas para enfrentarse a las amenazas que nos acechan. Históricamente, el Gobierno estadounidense y el sector de defensa han clasificado los ataques al Estado y a otras ramas de sus redes, lo que significa que el sector comercial no era consciente de los detalles críticos de dichos ataques y no podía desarrollar

[1] También conocidos como "softwares maliciosos".

tecnología para combatirlos. En consecuencia, el objetivo de Anup Ghosh, fundador y CEO de Invincea, una compañía de Sophos, consistía en desarrollar defensas que no necesitaran la firma de amenazas para combatirlas. Finalmente, el Dr. Ghosh participó en un programa en el que la idea básica era ver el cuerpo completo del software malicioso e identificar los atributos principales del mismo que se pudieran aprender. Si se crea un modelo se pueden identificar variantes del mismo. La compañía desarrolló estas técnicas utilizando el aprendizaje profundo de las redes neuronales y funcionó especialmente bien.

La informática cuántica: aplicaciones e implicaciones

Las compañías consideran que la informática cuántica es una tecnología emergente que puede servir como un facilitador estratégico a largo plazo para llevar a cabo análisis predictivos avanzados. La informática cuántica ha recibido gran financiación en los últimos años y está recibiendo especial atención de empresas con grandes necesidades analíticas informáticas.

Algunas organizaciones se centran en el tipo de problemas que la informática cuántica puede resolver. Este tipo de dificultades de análisis de datos no se pueden resolver mediante las técnicas tradicionales. Recientemente, ha habido grandes inversiones en este campo por parte de Google, Microsoft, IBM y el Gobierno estadounidense.

Al mismo tiempo, la informática cuántica tiene muchas aplicaciones beneficiosas, así como algunas que van a suponer complicaciones para Estados Unidos y el resto del mundo.

El contexto de la Inteligencia Artificial

La Inteligencia Artificial (IA) existe desde hace más de sesenta años. El 13 de septiembre de 2017, el Gobierno estadounidense anuncio su voluntad de explotación de datos, utilizando y aplicando IA en muchos de nuestros problemas en defensa. La primera señal de IA es la habilidad de aprender de los datos que se recogen continuamente.

Cuando se habla de IA para ciberseguridad, se debe también hablar de la ciberseguridad para la IA. Hay que proteger nuestros modelos de datos. Desde un punto de vista comercial, las empresas son las más competitivas. ¿Son los datos una ventaja estratégica? Sí, en el Departamento de Defensa, pero menos en el sector comercial. ¿Beneficiará la IA más al atacante o al defensor? La IA está cargada de promesas y peligros, se puede utilizar tanto en el ámbito ofensivo como en el defensivo y es demasiado pronto para saber qué lado saldrá ganando.

El espacio, los satélites y la infraestructura crítica

El antiguo espacio, el nuevo espacio y la economía del nuevo espacio

En el espacio hay saturación, disputas y competitividad. En los últimos 30-35 años, el espacio ha sufrido grandes cambios y, durante ese tiempo, también la Tierra, principalmente la sociedad, ha cambiado. Nuestra forma de entender el espacio, sus usos e implicaciones ha evolucionado.

El espacio es una industria con un precio de 340.000 millones de dólares al año, sin incluir los usos secundarios y terciarios. Setenta naciones tienen activos, intereses importantes, en el espacio. Se ha convertido en algo esencial. Es un área más comercial. A esto hay que sumarle la dinámica cambiante del uso que se le da y el papel que desempeña en la sociedad. Es una amenaza cambiante y creciente y la tecnología avanza a gran velocidad. Es una parte importante de los intereses comerciales y siempre ha sido parte esencial del ámbito militar. Todos los países del mundo con intereses en el espacio están moviendo sus actividades económicas a este ámbito.

Por lo tanto, ¿está Estados Unidos preparado para tratar esto como una cuestión política y de seguridad en el futuro? El espacio es una infraestructura crítica del futuro estadounidense y ahora nos encontramos en un momento en el que se necesita renovar las políticas de este ámbito.

Satélites, grandes y pequeños: implicaciones de seguridad

Nos encontramos ante una capacidad que siempre ha estado en manos de los gobiernos y que ahora está pasando a manos comerciales, con financiación privada. Las aplicaciones comerciales necesitan seguridad.

El mercado exige tanto como los gobiernos en temas de seguridad. Los intereses de seguridad convergentes de los sectores público y privado han dado lugar a innovaciones que necesitan impulsarse de la mano de prácticas de seguridad. Los riesgos de seguridad de amenazas no identificadas crecen cada día. Se espera que el Gobierno estadounidense y las empresas trabajen juntas para desarrollar y evolucionar en seguridad.

Desde la perspectiva de la seguridad, la pérdida de activos en el espacio es una preocupación. Parte de dicha preocupación es el hecho de que se tarda en llevar un activo al espacio entre 15 y 20 años y unos segundos en perderlo.

Desde el punto de vista gubernamental, también existe un riesgo de aversión desde el lado del Gobierno. El Gobierno suele querer invertir 15 años en desarrollar un programa porque quiere asegurarse un éxito rotundo. ¿Existe alguna alternativa?

Infraestructura crítica – posicionamiento, navegación y tiempo

Las políticas obsoletas tienen un impacto negativo en la seguridad

El GPS y GNSS[2] son servicios proporcionados por el Gobierno, gratuitos y presentes en casi toda infraestructura crítica. Fundamentan nuestra forma de vida y nuestra economía. Al mismo tiempo, constituyen una desventaja, pues no tenemos ningún respaldo en caso de que fallen.

Además, los sistemas espaciales de posicionamiento, navegación y tiempo se rigen por una política obsoleta (NSPD-39), que data del año 2004. Esta política necesita ser actualizada.

Otro reto es que este área envuelve la colaboración público-privada, lo que incluye la cuestión sobre la cantidad de información que se comparte. ¿Debería ser el espacio otro sector de infraestructura crítica?

A la vez que se impulsa la tecnología y nos introducimos en el nuevo espacio, no debemos olvidar la seguridad. Hay que implementar el mismo enfoque que con la seguridad terrestre. Esto significa que hay que percibir los riesgos y amenazas que existen y diseñar un sistema de seguridad en consecuencia. Hay que aprender del pasado y la industria debe entender los riesgos que conlleva. Un fallo en la seguridad puede provocar muchos problemas y cuesta dinero.

La nueva carrera espacial toma forma

China está liderando el camino hacia el espacio. Europa ha servido de apoyo al desarrollo del programa espacial chino. Hay un gran flujo de científicos europeos que se marchan a China debido a la gran burocracia que existe en Europa. Como consecuencia, China ha evolucionado muy rápido en poco tiempo, dejando incluso obsoletos algunos de nuestros sistemas.

Ciberseguridad en el sector de servicios financieros

Una radiografía del ecosistema

Los bancos se encuentran en primera línea en lo que a ciberataques diarios se refiere, ya que ahí es donde se encuentra el dinero. El sector está dedicando grandes recursos a la ciberseguridad.

[2] Sistema global de navegación por satélite.

FS-ISAC[3]

El FS-ISAC consiste en alrededor de 7.000 instituciones financieras, ahora en 39 países, con alrededor de 100 trabajadores en 8 países. Es uno de los vehículos principales de intercambio de información de amenazas e incidentes, tanto para temas informáticos como físicos. Todo el trabajo del FD-ISAC es voluntario, es decir, no es una agencia gubernamental. Es una organización 501(c)6 sin ánimo de lucro que fue fundada por sus 7.000 miembros.

El FS-ISAC también lleva a cabo actividades conjuntas con el Departamento del Tesoro de Estados Unidos en los que investigan diferentes tipos de ciberataques en distintas áreas de la industria para simular respuestas a los mismos.

También es receptivo a las sugerencias de decretos de leyes presidenciales y ha iniciado una filial separada, el FSARC[4], para colaborar de manera más estrecha en el intercambio de información, inteligencia, análisis e implementación del derecho, para responder así a la amenaza que el sistema financiero estadounidense experimenta.

El FS-ISAC trabaja en colaboración con el Gobierno estadounidense para entender las amenazas del sector. Es, por tanto, una plataforma de colaboración, investigación y apoyo mutuo.

También ha llevado a cabo actividades interesantes en temas de *malware*. Otra de sus filiales, Sheltered Harbor, aumentó la resiliencia de la industria para hacer frente a catástrofes, basándose en el concepto de asistencia mutua.

Finalmente, el oficial de inteligencia del FS-ISAC ha desempeñado un papel fundamental en la promoción de la colaboración junto con la implementación del derecho.

BITS: Tecnología y división de políticas en la Mesa redonda de servicios financieros

El BITS es un grupo centrado en riesgos y amenazas en ciberseguridad. Una de sus prioridades es la mayor unificación de la reglamentación en temas de ciberseguridad. Asimismo, también pretende fomentar la colaboración entre los sectores público y privado con el objetivo de mejorar las políticas en este ámbito. Asimismo, aspira a mejorar la estructura operacional para fomentar la respuesta rápida.

[3] *Financial Services-Information Sharing and Analysis Center* (Intercambio y análisis de información de los servicios financieros).
[4] *Financial Systemic Analysis and Resilience Center* (Centro de resiliencia de análisis financieros sistémicos).

El BITS también investiga el impacto de las nuevas tecnologías y, en cuanto al sector financiero, tiene las siguientes preocupaciones:

1. Inteligencia artificial: ¿cómo utilizarla para automatizar la gobernanza de datos?
2. Informática cuántica: ¿puede la informática cuántica pueda descifrar una encriptación?
3. Nube informática: ¿cómo se establecen controles?
4. *Blockchain*: puede mejorar los sistemas de autenticación.
5. Defensa cibernética activa: ¿cuáles son sus límites?

Asimismo, el BITS trabaja para desarrollar procesos de respuesta ante catástrofes. Una de las mayores preocupaciones es la regulación de la seguridad de datos. El BITS pretende establecer un diálogo abierto sobre cómo manejarlos y protegerlos.

Tomando un rumbo diferente: neutralizar la amenaza con un navegador remoto

Un enfoque menos tradicional en ciberseguridad implicaría el uso de navegadores remotos. Estos navegadores serían de un solo uso, de usar y tirar, y se encontrarían disponibles en la nube. No se conocería la dirección IP del usuario y, por lo tanto, este nunca quedaría expuesto. No habría que preocuparse de la información que entra en la red del usuario.

Israel: el ciber-poder (estudio de caso)

El papel del Gobierno en la innovación tecnológica

Israel es un ejemplo interesante del resultado positivo de intervención gubernamental. Al principio de la década de 1990, el país tenía un claro problema: una brecha entre la importación y la exportación. Durante las décadas de 1950 y 1960 las exportaciones eran principalmente agrarias y, cuando llegó la revolución industrial al principio de la década de 1990, la economía cambió por completo.

El Gobierno desarrolló un programa pionero conocido como YOZMA[5], con en el que buscaba a inversores con los que compartiría los riesgos de invertir en la industria tecnológica pero en el que los beneficios fueran percibidos solo por los inversores. Este programa tuvo mucho éxito y hoy Israel es conocida como la nación “start-up” o “hi-tech”.

[5] En hebreo quiere decir “iniciativa”.

Este éxito se repitió con otro programa relacionado con el agua. Israel era un país seco y necesitaba agua. El Gobierno decidió intervenir y, gracias a ello, las reservas de agua de Israel son suficientes incluso para proporcionar suministro a sus países vecinos, como Jordania.

La construcción de un ciber-ecosistema en Israel

El Gobierno israelí sabía que el país necesitaba un potente sistema de ciberseguridad. Para conseguirlo tenía que averiguar cuáles eran las preexistentes ventajas con las que contaba y descubrió que le faltaba más investigación y capital humano en este campo.

Ante esto, el Gobierno desarrolló un programa a escala nacional. Con 14 y 15 años se comienza a aprender habilidades informáticas. Asimismo, debido al servicio militar obligatorio, Israel entrena a los mejores para trabajar en ciberseguridad. El país examina a los mejores estudiantes entre 14 y 15 años y les prepara para convertirse en expertos en este ámbito. Además, el Gobierno ha colaborado con las universidades y, a día de hoy, cuenta con seis centros de investigación en este ámbito.

Las lecciones que se han aprendido, mirando hacia el futuro

El Gobierno tuvo éxito porque había una verdadera necesidad. El programa tuvo éxito porque el Gobierno trabajó por entender el problema y el ecosistema como un todo. Asimismo, el marco correcto para desarrollar esto tiene que tener en cuenta cómo iniciar y animar a los negocios a invertir. Finalmente, el desarrollo no puede ocurrir si no hay una base sobre la que comenzar.