Newsletter
Centro de Investigaciones y Estudios Estratégicos
ANEPE

Editorial

Maratón del Ciberdominio: inscripciones abiertas

Los conflictos armados vienen desde tiempos ancestrales modificando su forma, mas no su fondo.Se comenzó con el enfrentamiento hombre a hombre, para dar cabida después a la utilización de armas como aviones, tanques y barcos. Para mediados del siglo XX, la bomba nuclear era el descubrimiento más dañino, pero a la vez más eficaz para la resolución de las guerras.Ahora, cuando comenzamos el siglo XXI, una nueva modalidad de ataque se ha hecho presente en la actualidad: el concepto de "ciber".

Cibercrimen, ciberseguridad y ciberdefensa son los temas más abordados por los países con mayor desarrollo, ya que se prevé que sea la nueva manera de llevar una guerra, sin necesidad de tanta violencia física, sino que atacando directamente a las fuentes de información de gobiernos y organizaciones internacionales, lo que podría generar un quiebre en el sistema financiero o en los servicios básicos de un país; y todo esto a través de una red de computadores. Si bien es un tipo de guerra menos cruento, es de los más dañinos, ya que afectaría directamente a todos los ciudadanos, y no a un objetivo dirigido, como era en las guerras anteriores, que buscaban atacar una célula terrorista, o desestabilizar un gobierno. Aquí se ataca a todos los ciudadanos poniéndolos en riesgo.

A este respecto, el principal elemento que genera discusión y controversia es el de Inteligencia Artificial, IA, (o AI por sus siglas en inglés). Esta creación hace referencia a máquinas que realizan acciones para optimizar sus resultados. Estas máquinas son capaces de aprender y de resolver problemas, todo esto a través del "machine learning".

Ahora, con la modernización de los elementos bélicos, entramos en una singular carrera armamentista, donde lideran Estados Unidos y China en el desarrollo de la IA, compitiendo velozmente por cuál potencia desarrolla un sistema más complejo y capaz de combatir los conflictos.

Estados Unidos, si bien invierte en desarrollo de nuevas tecnologías cibernéticas, lo hace principalmente desde el sector privado, lo que para un futuro, si es que el gobierno no se apropia de esto, puede volverse en su contra, ya que no se debe olvidar que en el sector privado esta tecnología es de las más rentables y requeridas por países con alto desarrollo. China por su parte, lo realiza desde el gobierno, lo que estandariza su producción a los más altos niveles y sirve realmente como un método de ciberdefensa.

Se trata de minimizar el riesgo de ciberataques, que como se menciona anteriormente, pueden traer consecuencias impensadas, por lo que la tendencia al desarrollo de este ámbito tiene un alcance global, y crece de manera exponencial.

Ahora bien, cabe plantearse la necesidad de establecer un acuerdo respecto al uso de armas cibernéticas. Tal acuerdo no existe debido a que todavía no se toma debida consideración de los posibles alcances de este tipo de ataques, ya que hasta ahora no han sido mundialmente significativos, y porque ningún gobierno ha llegado a modernizar sus sistemas para protegerlos de un ataque informático. De seguir así, actuando de manera ineficiente y dubitativa respecto de este importante tema, las consecuencias de un ataque –o de una guerra cibernética– tendrán repercusiones nunca antes vistas.

¿Cuáles serán las acciones que correspondería seguir frente a este tema? ¿Cómo se comportarán los países en caso de ataques cibernéticos? Como Centro de Investigaciones y Estudios de Estratégicos, dejamos abierta la invitación al debate e intercambio en esta materia.

CIEE-ANEPE

La guerra caliente

Rufino Contreras

Computing, 3 de enero 2018

Antes había un campo de batalla y los ejércitos convenían día y hora para medir sus fuerzas. Respetaban las treguas para retirar los cadáveres y heridos del campo de batalla. Y al oscurecer, cada uno a su trinchera a descansar. Ahora en la guerra actual, no sabes por donde te vienen los enemigos. Cada vez está más extendido el ataque de falsa bandera, países que se amparan en el anonimato para atacar impunemente dejando falsos señuelos para incriminar a terceros. [...] Los grupos terroristas se mueven entre sombras para financiarse e instruir a su comunidad de fanáticos.

En la "guerra hibrida" actual confluye la actividad de los propios estados que hacen el uso del sabotaje a centros críticos (caso Stuxnet y la central nuclear de Irán) o de injerencias para influir en la política de un país concreto, (los correos electrónicos de Clinton robados por hackers rusos). [...] El departamento de Seguridad Nacional de Estados Unidos ha prohibido a las agencias gubernamentales utilizar el software de la firma rusa Kaspersky Labs ante el temor de nuevas filtraciones. En España, los incidentes de alta peligrosidad se han duplicado en un año, y los responsables institucionales de seguridad temen señalar con el dedo la procedencia de los ataques por temor a afectar las relaciones bilaterales.

[...] La ciberguerra de ahora busca la contundencia viral, inutilizar infraestructuras críticas y desactivar países (Rusia lo hizo hace cinco años con Georgia en 2008 y más recientemente con Ucrania, como consecuencia de la crisis de Crimea). La guerra de la información puede ser más agresiva cada vez, y hay a disposición otros armamentos de destrucción masiva como lo son la IA (Inteligencia Artificial) y el Machine Learning que, utilizados de una forma espuria, pueden convertirse en demoledoras bombas de relojería. Las guerras ya no son lo que eran, ya dijo Einstein que la cuarta guerra mundial sería a pedradas. Pero de momento, controlar los mensajes, crear una verdad paralela ("fake reality") y envenenar la opinión pública son las tendencias más pujantes, adobadas con ataques de mayor calado a infraestructuras y empresas. Si hasta los noventa sufrimos una guerra fría, en estos momentos nos acosa una guerra más calentita.

CONTRERAS, Rufino. La Guerra Caliente. Computing. [En línea]. 2018. [Fecha de consulta: 17 de enero 2018]. Disponible en: <http://www.computing.es/seguridad/opinion/1102759002501/guerra-caliente.1.html>

La próxima carrera armamentista es la de la inteligencia artificial

Meredtih Rutland Bauer

Fifht Domain, 25 de enero 2018

En teoría, la única tecnología capaz de hackear un sistema dirigido por inteligencia artificial, es otro sistema de inteligencia artificial más poderoso. Esa sola razón explica por qué el ejército de Estados Unidos incorporó la inteligencia artificial, con una capacidad poderosa, en sus drones, que esperan proveer la más moderna ciberseguridad, por lo menos por ahora.

[...]Pero esta carrera por el mejor sistema de IA, recién comienza. [...] La complejidad y habilidades de adaptación de los sistemas de inteligencia artificial significan que reaccionan rápidamente a los ciberataques y pueden identificar y proteger cada posible punto de entrada al sistema que resguarda.

La inteligencia artificial global dentro de la industria de ciberseguridad ya está creciendo en el sector privado y se estima que alcanzará los $ 18.2 mil millones para 2023, [...] Una gran parte de ese crecimiento se debe a algoritmos de aprendizaje de amenazas que se utilizan para proteger a las empresas de los ciberataques.

[…] "Incluso el software de IA utilizado para proporcionar ciberseguridad se ve amenazado si aparece otro más fuerte, con algunas mejoras".

"Es una amenaza viable y muchos de los sistemas de ciberseguridad son objetos de ataque, incluyendo los que está diseñados para detectar las intrusiones"

[…] Estos ataques son muchas veces culpa de errores humanos, como por ejemplo cuando se entrega autorización para probar ciertas tareas del sistema, pero estas salen mal y terminan por producir consecuencias desastrosas. Una sola falla de un sistema súper-inteligente puede causar un evento catastrófico del cual puede que no exista modo de recuperarse.

[…] "Es como un arma cibernuclear, cuando la próxima guerra sea de carácter cibernético, será ganada solamente por quien sea el mejor en las matemáticas y algoritmos".

RUTLAND, Meredith. The next cyber arm race is in artificial intelligence. Fifth Domain. [En línea]. 2018. [Fecha de consulta: 29 de enero 2018]. Disponible en: <https://www.fifthdomain.com/dod/2018/01/24/the-next-cyber-arms-race-is-in-artificial-intelligence/>

Es hora de ponerse serios en cuanto a la ciberseguridad

Michael Fritze y Kathryn Schiller- Wurster
Defense One, 16 de enero 2018

Cuando escuchamos sobre un nuevo ataque cibernético, generalmente pensamos en un virus de software, que si bien es importante, puede ser resulto fácilmente. Pero solucionar problemas de hardware suele ser más complejo y requiere más dinero.

Este tipo de cosas no son inesperadas. Las consecuencias de las principales vulnerabilidades de los sistemas ha sido objeto de estudio en los últimos años. […] os informes reflejan que las fallas pueden surgir de un diseño informático deficiente, o por la inserción de un elemento malicioso en el sistema.

[…]Sin embargo, los legisladores norteamericanos se han centrado principalmente en la protección de software, de programas; pero es hora de invertir en protección de hardware, para protección en áreas de defensa, y la estrategia para realizar estas mejoras incluyen:

1. Crear una cibernética integral de hardware. La industria por sí sola, no puede resolver estos problemas de seguridad, los costos son muy altos, requieren la intervención del gobierno e intercambio de información sobre amenazas, para generar una red de seguridad, tanto para consumidores, como para los sistemas nacionales de seguridad.

2. […] Priorizar la investigación respecto de la seguridad de hardware, No se pueden resolver problemas nuevos, con herramientas antiguas.

Las propuestas del Departamento de Defensa de Estados Unidos van desde una inversión e recambio de chips seguros, para actualizar el sistema de seguridad. […]Ha llegado el momento de debatir los riesgos o la probabilidad de amenazas a la seguridad del hardware. El gobierno de EE. UU. Necesita tomar medidas rápidas

FRITZE, Michael. SCHILLER- WURTER, Kathryn. Time to get serious about hardware cybersecurity. Defense One. [En línea]. 2018. [Fecha de consulta: 17 de enero 2018]. Disponible en: <http://www.defenseone.com/ideas/2018/01/time-get-serious-about-hardware-cybersecurity/145210/?oref=d-river&utm_source=Sailthru&utm_medium=email&utm_campaign=ebb-1-17&utm_term=Editorial%20-%20Early%20Bird%20Brief>

Guerra de confianzas: Tendencias peligrosas en el ciberconflicto

Neal Pollard, Adam Segal y Matthew Devost.

War on the Rocks, 16 de enero 2018

[…]Durante la mayor parte de la corta historia del ciberespacio los analistas y legisladores en materia de defensa se han centrado en los ciberataques que generan destrucción y muerte.

[…]Ahora, el ciber conflicto ha tomado un camino diferente. Aunque las amenazas a industrias, fuentes de poder y refinerías se mantienen- y pueden ir en aumento, mientras más áreas se conecten al internet- los ciberataques han buscado- generalmente- minar la integridad de los sistemas políticos, económicos y sociales antes que destruir infraestructura.

La operación más importante del año pasado- el intento ruso de intervenir en las elecciones presidenciales estadounidenses de 2016, a través del hackeo al Comité Democrático Nacional, y por consiguiente la filtración de correos electrónicos y el uso de cuentas falsas de Facebook y Twitter- fue diseñada para socavar la confianza en las instituciones a través de la manipulación y distorsión de la información.

[…] Pero dada la realidad de la mayoría de los ataques cibernéticos hasta ahora, la única manera de preparase para la próxima ola de conflictos, es necesario darle más importancia a la integridad y confianza de los datos.

[…] Solo una operación cibernética ha causado daño físico- el malware Stuxnet- que causó que las centrifugadoras de la planta nuclear Natanz en Irán se salieran de control en 2010.

En diciembre de 2015, se produjo otro ataque, con menores daños, en Ucrania, donde hackers rusos apagaron las luces en la región Ivano-Frankovsk, dejando 60 estaciones energéticas sin luz, y cortándoles el suministro a más de 230.000 personas.

[…]Ninguno de estos ataques generó un quiebre importante en las operaciones, o en los efectos técnicos de los sistemas que fueron atacados. Los hackers, no buscaban principalmente atacar la confianza de los usuarios, sino que esta se vio dañada colateralmente. La meta era reducir el suministro, la pérdida de confianza vino por añadidura.

La erosión de la confianza se está transformando en la meta principal de los ataques, ya no es considerada un daño colateral. A raíz de un ataque, el individuo puede perder la fe tanto en su sistema computacional, como en las instituciones y valores en los que descansan esas redes.

Los ciberataques que apuntan a la confianza e integridad son más difíciles de detectar, prevenir y recuperar que los ataques meramente físicos. Cuando un ataque genera la negación de un servicio, y se cae el sitio, está claro que algo va mal y corresponde solucionarlo. Pero cuando se roba información es más difícil de detectar, aunque las herramientas de seguridad son capaces- generalmente- de determinar qué datos dejó el sistema. A pesar de esto, es extremadamente difícil analizar qué datos fueron manipulados, o debilitaron el sistema y más difícil aun es recuperar la confianza.

[…] Aunque no han ocurrido ataques de confianza en el sistema financiero, este sector es particularmente vulnerable a (in)filtraciones que barrerían con la confianza en los sistemas de pago que procesan transacciones diariamente. Un ejemplo son las casas de compensación que actúan como mediadores de las transacciones de valores para asegurar la transferencia sin errores de acciones, y en caso de que exista alguna complicación, estos actúan como garantías de la transacción […] los hackers podrían devastar el sistema financiero solo al insertar datos falsos, o cambiar los datos en las casas de compensación.

[…] Restaurar la integridad de los datos sería un proceso lento y laborioso de comparar datos con versiones anteriores, que podrían no existir. Incluso si lo hicieran, la comunidad de pago y liquidación tendría que ponerse de acuerdo sobre

la validez de las versiones anteriores. Convencer a los usuarios de que se ha restaurado la integridad de los datos tomaría mucho más tiempo. Algunas disputas sobre la integridad de la compensación o transferencias podrían no reconciliarse nunca.

[…] Como resultado de esto, en el futuro habrán más jugadores, más ataques y por ende más oportunidades para errores de cálculo. Como existen muy pocas regulaciones respecto al comportamiento cibernético, países del tamaño de China, o Bahréin pueden ser partícipes de estos ataques.

[…]¿Cómo disminuir esta amenaza? Gobiernos e industrias han destinado recursos significativos en proteger la privacidad y controles de seguridad. Mucho menos se ha hecho para prevenir la manipulación de datos en instituciones, o para recuperar la confianza en estas tras un ataque. […] Actualmente existen modelos que permiten medir y asegurar la integridad de los datos. Las compañías de ciberseguridad proporcionan calificaciones para la seguridad de empresas para resaltar la confianza de éstas. El siguiente paso, después de las medidas ya tomadas, sería establecer regulaciones para equiparar la confianza con el control, y lograr introducir esta regulación al sector privado.

[…] Los esfuerzos internacionales para desarrollar medidas de fomento de la confianza también desempeñarán un papel en el mantenimiento de la confianza. Del mismo modo que los analistas estadounidenses se han centrado principalmente en ciberataques destructivos, la diplomacia estadounidense se ha ocupado principalmente de las leyes y normas internacionales relacionadas con el ciberconflicto, en lugar de confiar en los ataques. Un grupo de expertos gubernamentales en la ONU, por ejemplo, respaldó la norma de que los estados no deberían interferir con la infraestructura crítica durante el tiempo de paz y no debería atacar a los equipos de respuesta a emergencias informáticas de otro país.

La mayoría de los ataques de confianza claramente caería por debajo del umbral para el uso de la fuerza o ataque armado en el derecho internacional. Si bien hay pocas esperanzas de que haya acuerdos internacionales sobre este tipo de operaciones cibernéticas, los Estados Unidos pueden trabajar con países de ideas afines para responder a las amenazas a las instituciones complejas. […] En un primer paso prometedor, en los últimos años, la OTAN ha creado una red de centros que ayudarán a la alianza a comprender mejor el peligro, incluido el Centro de Excelencia de la Cooperativa Cyberdefense en Tallin y el Centro de Excelencia de Comunicaciones Estratégicas en Riga.

La OTAN y la UE también establecieron recientemente el Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas en Helsinki. Esta red debería ser capaz de proporcionar una imagen completa de la amenaza a las instituciones democráticas, así como para generar contramedidas a los ataques contra los medios y las elecciones

[…] El riesgo inmediato es que la próxima ola de ataques a la confianza provoque un conflicto militar regional. Según funcionarios de inteligencia de Estados Unidos, a fines de mayo, los piratas informáticos de los Emiratos Árabes Unidos se infiltraron en las noticias del gobierno de Qatar y en las redes sociales, y plantaron citas falsas del líder de Qatar. El gobierno de Emiratos, junto con Arabia Saudita, Bahréin y Egipto, utilizaron las citas plantadas como un pretexto para prohibir los medios de comunicación de Qatar y romper las relaciones diplomáticas y comerciales con Qatar. Si bien los efectos de este truco en particular finalmente se contuvieron, los ciberataques que avergüenzan o amenazan la legitimidad de los líderes débiles podrían hacer que reaccionen de forma exagerada, dando lugar a un conflicto convencional. El otro temor es que los trucos de confianza se extiendan a Internet de las cosas, la salud, los registros legales y otras instituciones centrales de la sociedad moderna.

Estados Unidos tiene la oportunidad de elevar la confiabilidad a la par con los controles de seguridad y la privacidad en el ciberespacio. Con los actores maliciosos dirigidos cada vez más a la integridad de los datos, es importante para los gobiernos y las empresas proteger la confianza en los frágiles sistemas políticos, sociales y económicos conectados a Internet. Aun así, los estados, las corporaciones y las organizaciones internacionales no pueden hacerlo solos [...] Los estados y las personas han degradado la confianza en Internet, y ahora los estados y los ciudadanos tendrán que trabajar más arduamente para defenderla y reconstruirla.

POLLARD, Neal. SEGAL, Adam. DEVOST, Matthew. Trust war: Dangerous trends in cyber conflict. War on the rocks. [En línea]. 2018. [Fecha de consulta: 17 de enero 2018]. Disponible en: <https://warontherocks.com/2018/01/trust-war-dangerous-trends-cyber-conflict/>

¿Por qué no hay acuerdos sobre control de armas cibernéticas?

Erica Borghard y Shawn Lonergan

Defense One, 18 de enero 2018

Durante la Guerra Fría, cuando las potencias mundiales con capacidad nuclear se enfrentaban a crisis de inestabilidad y escalada, se formaron acuerdos para el control de éstas. Los regímenes de control de armas pueden alterar los incentivos militares para el uso de tecnologías ofensivas; limitar el daño a los estados en caso de que se utilicen estas tecnologías; y generalmente contribuyen a relaciones interestatales más estables, incluso entre adversarios. Con la emergencia de un dominio cibernético militarizado que crea las condiciones para malinterpretaciones que pueden llevar a un conflicto inadvertido, ¿por qué no existen regímenes de control para las armas cibernéticas?

Los regímenes tradicionales de control de armas no se pueden aplicar al ciberespacio por cuatro razones: es difícil medir la fuerza relativa de los estados en el ciberespacio, existe incertidumbre respecto a los efectos militares de la tecnología cibernética, los grandes desafíos de monitorear el comportamiento y su difícil aplicación.

Los regímenes de control de armas requieren que los estados tengan una comprensión básica de la fuerza relativa de cada uno para que un acuerdo pueda promover la estabilidad estratégica. Para las municiones convencionales, las armas nucleares, o incluso las ordenanzas químicas, se pueden contar cantidades de un gas virulento, lo que permite evaluar la fuerza comparativa. No se puede decir lo mismo para evaluar la fuerza relativa en el ciberespacio por dos razones.

En primer lugar, ¿Cómo puede un estado contar armas virtuales, que por definición no pueden destruirse y, en teoría, podrían regenerarse constantemente? En segundo lugar, a diferencia de las armas nucleares o los tanques, algunas armas cibernéticas carecen de letalidad universal; a menudo se requieren herramientas y accesos únicos para producir efectos contra sistemas específicos dirigidos.

En contraste, lo que puede ser medible en el ciberespacio es la habilidad técnica de los actores y ejecutores de amenazas cibernéticas- una medida cualitativa, más que cuantitativa de la capacidad-. Sin embargo, el uso de habilidades relativas para impulsar los regímenes de control de armas puede ser poco práctico debido a la dificultad de elaborar o aplicar acuerdos que limiten las habilidades o el acceso a la tecnología, particularmente cuando los gobiernos no son los únicos propietarios.

Los regímenes de control de armas también pueden formarse si los gobiernos pueden hacer cálculos razonables con respecto al probable efecto militar de los cambios tecnológicos. Sin embargo, el ritmo rápido e impredecible de la innovación tecnológica en el dominio cibernético complica estas evaluaciones. A nivel táctico, los vectores de ataque y las capacidades ofensivas están en constante evolución, a diferencia de la arena nuclear, donde las innovaciones tenían

plazos de desarrollo largos y a menudo se podían observar.

El retraso en la innovación nuclear dio a los estados espacio para ajustar los acuerdos de control de armas o desarrollar otros medios, tales como inteligencia personalizada o sus propios programas complementarios, para mitigar los temores planteados por los avances tecnológicos.

En el ciberespacio, la promesa abierta de innovación junto con técnicas rápidamente cambiantes que pueden surgir con poca o ninguna advertencia desafía la creación de cualquier acuerdo. Un acuerdo de control de armas cibernéticas corre el riesgo de ser obsoleto o restrictivo de alguna manera imprevista antes de que la tinta haya tenido tiempo de secarse.

Incluso si los estados fueren capaces de calcular las capacidades relativas y evaluar las implicaciones militares de las innovaciones tecnológicas, es poco probable que formen un acuerdo de control cibernético, cuando los gobiernos aún no son capaces de detectar trampas en el sistema. El problema de verificación contiene dos pilares: poder determinar el tamaño del arsenal de un estado y supervisarlo para garantizar el cumplimiento del acuerdo a futuro.

La determinación del cumplimiento en el dominio cibernético requeriría que los participantes accedan a las redes del gobierno. El software malintencionado se puede desarrollar casi en cualquier lugar, lo que significa que cualquier mecanismo de verificación requeriría que un gobierno abra todas sus redes para su inspección. Sería insondable que un estado permita que otro, o cualquier actor externo, tenga acceso sin restricciones a sus redes. Tal acceso proporcionaría a una parte externa información crítica sobre vulnerabilidades y posibles actos malintencionados, y podría violar el acuerdo que intenta hacer cumplir.

Una medida menos invasiva para evaluar el cumplimiento sería que el monitoreo se realice a través de medios técnicos nacionales de inteligencia. Durante la Guerra Fría, los espías analizaron imágenes recogidas de satélites que monitoreaban la postura nuclear de otro estado. El equivalente en el ciberespacio sería usar el ciberespionaje para recopilar información sobre las redes internas de otro estado. Sin embargo, aunque la recopilación de satélites es completamente pasiva, no es posible obtener acceso a datos de redes gubernamentales sensibles y evitar su posible fuga.

Si unEstado observa que un tercero penetra en sus redes, puede ser incapaz de distinguir entre la actividad de espionaje de rutina con el fin de monitorear el cumplimiento, otros fines de espionaje legítimos no relacionados con el cumplimiento, o la preparación para una operación ofensiva. Esto podría provocar que el estado objetivo responda de forma gradual. Por lo tanto, la incapacidad de percibir la intención podría, de nuevo, socavar la estabilidad que los acuerdos de control de armas debían crear.

Finalmente, incluso si se pudieran superar los obstáculos ya mencionados, la aplicación de cualquier acuerdo de control de armamentos sería difícil de implementar debido a dos factores: los problemas asociados con la atribución de un castigo proporcional. Primero, en caso de una violación, los estados tendrían que atribuirla con un nivel de confianza que justificaría una respuesta recíproca. Si bien las capacidades de atribución han mejorado indudablemente con el tiempo, no todos los estados tienen las mismas capacidades de atribución o confianza suficiente en ellos para justificar la acción. Esto es particularmente relevante dado que un estado que detecta una violación necesitaría convencer a otras partes del mismo tratado de que ocurrió una violación.

En segundo lugar, hacer cumplir un acuerdo de control de armamentos requiere respuestas proporcionales a la derogación observada. Esto es problemático por varias razones. Puede haber un desfase de tiempo significativo entre el momento en que se produce una derogación y el momento en que se observa realmente.

Por lo tanto, es probable que el efecto disuasivo de una respuesta se diluya con el simple paso del tiempo. Además, las limitaciones de recursos y acceso pueden limitar las capacidades que tiene un estado en un momento dado para responder, lo que significa que puede no ser necesariamente efectivo. Una posible alternativa podría ser utilizar elementos no cibernéticos del poder nacional para castigar una derogación de un acuerdo de control de armas cibernéticas. Sin embargo, elaborar una respuesta efectiva que dependa de elementos físicos de poder puede ser difícil de formular si la violación solo causó daño virtual [...].

BORGHARD, Erica. LONERGAN, Shawn. "Why are there not cyber arms control agreements". Defense One. [En línea]. 2018. [Fecha de consulta: 19 de enero 2018]. Disponible en: < http://www.defenseone.com/ideas/2018/01/why-are-there-no-cyber-arms-control-agreements/145289/?oref=d-river>

Países en alerta roja por la ciberguerra en 2018

Ellie Donnelly

Indepedent, 5 de enero 2018

Una ciberguerra de gran magnitud se predice para este año, de acuerdo a Ward Solutions, una empresa de seguridad cibernética.

[...] el año pasado, se observó una escalada en el número de ciberataques contra países, y se cree [...] que este año serán similares el número de ataques, quizás aumentando para que la población civil pueda sentir su impacto. Lo que cambiará, de acuerdo a lo provisto por Ward Solutions es la manera en que los países reaccionarán a estos ataques, ya que se espera que, principalmente los miembros de la OTAN, empiecen a esbozar principios para la guerra cibernética.

[...] "2018 será un año en que las amenazas a la ciberseguridad aumentarán, en cuanto a sofisticación y el tipo de daño que causarán" [...] Esperaríamos que ciertas naciones optaran por el ataque ofensivo a los hackers y trataran de desarmarlos antes de que pudieran atacar. Son estas estrategias ofensivas de ciberseguridad las que se convertirán en elementos centrales de la defensa nacional, y lo que les permitirá prevenir esos ataques"

[...] Se prevé que los cibercriminales utilizarán la inteligencia artificial y tecnologías de "machine learning"- proceso de inducción de conocimiento para computadores- para reforzar sus ataques y evadir las herramientas de seguridad de las empresas y gobiernos.

DONNELLY, Ellie. Countries on red alert for 2018 cyber war. Independent. [En línea]. 2018. [Fecha de consulta: 25 de enero 2018]. Disponible en: https://www.independent.ie/business/countries-on-red-alert-for-2018-cyber-war-36459446.html

Espía robot: China y Estados Unidos en la carrera por la Inteligencia Artificial

Bob Griffin

The Cipher Brief, 21 de enero 2018.

Cuando pensamos en la carrera armamentista, naturalmente lo asociamos a lo físico: misiles, satélites, jets de combate, submarinos y portaaviones. Si bien son elementos importantes para la guerra convencional, está emergiendo otro tipo de carrera, la de las armas tecnológicas en inteligencia artificial (IA) que traerá profundas implicaciones en el balance del poder del siglo xxi.

Al referirse a inteligencia artificial, la carrera armamentista es entre dos países; China y Estados Unidos. Tanto las implicancias económicas, como las consecuencias tácticas son muy altas para ambos países. Cada jugador tiene ventajas relativas, y el futuro tiene mucho que decir todavía, pero que quede claro; esta es una carrera de dos caballos de ahora en adelante.

China ha mantenido las aspiraciones de inteligencia artificial por casi una década, como lo evidencia Tianhe- IA, la supercomputadora que

encabezaba la lista el año 2010- siendo la primera vez que este honor iba para un país que no fuera Estados Unidos o Japón.

[…] La respuesta china a este suceso fue la elaboración de un manifiesto denominado "Una nueva generación de plan de desarrollo de inteligencia artificial", elaborado en julio del 2017. El plan establecía como meta "aprovechar las principales oportunidades para el desarrollo de inteligencia artificial, construir el mejor "jugador" en cuando a inteligencia artificial y liderar el mundo en este tema en 13 años más"

La mayoría de los observadores de estos temas creen que China puede alcanzar esta meta. Consideremos las fuerzas en juego.

1.Gobierno: inversión vs intervención

Para los gobiernos del mundo occidental, la inteligencia artificial es un concepto abstracto que es tan temido como buscado. Estados Unidos mantiene su tradicional postura de evaluar los riesgos y desventajas en vez de darle importancia a este invento, que llevaría a la mayor ola tecnológica que haya existido

La comprensión respecto de este tema en la actual administración es deficiente; y el congreso no es nada diferente.

Los sectores de inteligencia y defensa tienen el liderazgo dentro del gobierno para impulsar la urgencia de estos temas, pero no tienen todo el apoyo que se requiere.

[…]Lo opuesto ocurre en China. La inteligencia artificial es un componente crítico y ha recibido la atención, inversión y regulación correspondiente para surgir. Respecto al último elemento; la regulación, es necesario destacar algunas cosas. Si Estados Unidos insiste en adoptar un marco regulatorio que ralentiza la inserción de la IA en trabajos e industrias, este país se verá en desventaja material respecto a China. Esto se debe a que el gobierno chino invierte activamente en IA, desde su inicio con los chips, hasta los software que utilizan, pero constantemente está creando espacios para el desarrollo de esta, infraestructura, capital y herramientas; todo lo que sea necesario para lograr un desarrollo óptimo de la inteligencia artificial.

2.La prevalencia del robo

Algo que hemos aprendido la última década, es que el concepto de seguridad informática, es solo un concepto. En realidad, nada es seguro. Mientras la inteligencia artificial es un campo excepcionalmente abierto, en donde casi cada progreso se publica, y al mismo tiempo, las apuestas por esto se disparan, esa dinámica podría cambiar.

De ser así, sería esperable que empresas o gobiernos comiencen a robar lo que consideran de valor competitivo. Robar experiencia es difícil, pero robar algoritmos o códigos, no lo es.

Mientras el futuro de la inteligencia artificial es incierto, las partes en juego cumplirán un rol importante en determinar quién se convierte en el líder del ciberespacio.

Como un experto en tecnología y miembro de la comunidad de defensa e inteligencia, comparto mi sentimiento de urgencia y preocupación al actuar de mi contraparte en el gobierno.

La carrera por la inteligencia artificial es real, y depender casi completamente de un privado para desarrollarla, sería asumir un gran riesgo para el gobierno.

[…] Esto no es una sugerencia para que el gobierno asuma un rol más importante en el papel de inversionista […], sino que es para sugerir que la inteligencia artificial, y todo lo que la compone está recibiendo la atención que necesita por parte del mundo, y el gobierno debería ponerse a tono con este desafío. Esto significa más liderazgo, más experimentos que generen más datos. Esto no es una carrera armamentista que podamos permitirnos perder.

GRIFFIN, Bob. Spy, Robot: China and U.S. Locked in AI arms race. The Cipher Brief. [En línea]. 2018. [Fecha de consulta: 25 de enero 2018]. Disponible en: <https://www.thecipherbrief.com/column/cyber-advisor/spy-robot-china-u-s-locked-ai-arms-race>

Los "Shutdowns" significan que el gobierno sigue utilizando hardware y software antiguos... y eso es malo para la seguridad

Jeffrey M. Voth

Fifth Domain, 27 de enero 2018

La mayoría de las agencias federales sigue experimentando debilidad al proteger sus sistemas de información. Dadas las vulnerabilidades de seguridad a las que se enfrentan las instituciones federales cabe preguntar 1. ¿Cuánto se debe invertir en programas de ciberseguridad? y 2. ¿En qué se deberá invertir?

"Hemos sufrido un accidente de grandes magnitudes" declaró el ex director de la Agencia Nacional de Seguridad (NSA) Mike McConnel al NY Times, analizando las consecuencias de la reciente violación a los sistemas de la agencia. El gran énfasis en la ciberseguridad según el presupuesto federal de 2018 es que más de 20 mil millones de dólares en programas cibernéticos siguen pendientes en el balance. [...] Así entonces, responder la pregunta de cuanto y donde invertir involucra una decisión crítica para cada agencia. Encontrar el nivel óptimo de inversión en ciberseguridad será clave.

[...] Sin un presupuesto final establecido para el 2018, las agencias van a continuar operando en un ambiente de alta presion, con poca flexibilidad para crear o terminar programas.

Al desarrollar la estrategia de inversión en ciberseguridad de una organización, recomiendo un modelo analítico económico que procederé a presentar.

1.Analizar las pérdidas potenciales

El primer paso es considerar lo que la organización puede perder si su sistema de defensa es débil. Por ejemplo, las organizaciones del sector público que son responsables de mantener grandes bases de datos personales de los ciudadanos pueden incurrir en gastos significativos para reparar una violación de seguridad, dado que se debe reparar el sistema y también compensar a las personas por los daños.

2.Evaluar las probabilidades de ocurrencia

Con múltiples infracciones de seguridad por parte de externos y ex empleados, la NSA se enfrenta a una serie de nuevas amenazas, desde grupos rebeldes que han robado armas cibernéticas para utilizarlas en una red de crimen organizado transnacional. En una era de transformación digital, ninguna organización es inmune. Sin embargo, no todas enfrentan el mismo nivel de amenazas.

Por ende, ¿Cuan probable es una intrusión en la organización? ¿Cuál es la postura de la organización respecto a sus elementos digitales? ¿Cuál es su mayor preocupación? ¿Amenazas externas o internas?

3.Correcta asignación de recursos

Finalmente, generar un análisis de costo-beneficio para identificar cuanto se debe invertir en la ciberseguridad, y cuanto puede ganar la organización con su implementación.

Cuando los beneficios esperados, exceden los posibles costos, la decisión de invertir en ciberseguridad se hace más fuerte. El nivel óptimo de inversión es el equilibrio entre costos y beneficios.

Los decisores federales reconocen la necesidad de fortalecer la inversión para las agencias en cuanto a ciberseguridad.

Tal y como muestran las recientes violaciones a la seguridad de datos, las consecuencias de no proteger los archivos digitales son graves, tanto para el gobierno, como para la ciudadanía. [...] Claro que un plan generalizado no sirve para todos, es necesaria la utilización de este método para realizar una toma de decisiones inteligente respecto a materias de ciberseguridad.

VOTH, Jeffrey. Shutdowns means that government keeps using old hardware and software… and that is not good for security. Fifth Domain. [En línea]. 2018. [Fecha de consulta: 29 de enero 2018]. Disponible en: <https://www.fifthdomain.com/opinion/2018/01/26/shutdowns-mean-the-government-keeps-using-old-hardware-and-software-and-thats-bad-for-security/?utm_source=Sailthru&utm_medium=email&utm_campaign=ebb%2001.29.2018&utm_term=Editorial%20-%20Early%20Bird%20Brief>