

**Universidad de Miami, MICSUN VII, 13 – 15 de abril 2018**



**SEGURIDAD CIBERNÉTICA**

**E INFORMACIONAL**

En una época donde la tecnología avanza rápidamente y se está convirtiendo en un lugar común, los problemas de seguridad no pueden pasarse por alto. Ahora, rara es una guerra unilateral. No importa cuántos intentos se realicen para mejorar la tecnología y su seguridad, el cibercrimen también está evolucionando, haciendo los hackers aún más anónimos y peligrosos. Y aunque la neutralidad de la red y el anonimato en Internet podrían considerarse derechos básicos [modernos], estas políticas se aplican a todos. Los hackers comprenden la intensidad de la Web y mejoran sus técnicas para violar navegadores comunes, lenguajes de programación y sistemas operativos; objetivo de un hacker es asegurar una pieza en un directorio o archivo raíz de una computadora y permanecer oculto la mayor cantidad de tiempo.

Existen tres tipos de delito cibernético (infracciones de privacidad, delitos basados en transacciones y alteración de datos) y es a través de este espectro que el cibercrimen es un asesino silencioso. Las infracciones de privacidad se encuentran entre los delitos más comunes en la escala individual; esta área incluye la violación de la privacidad personal y corporativa, que generalmente conduce a chantajes y casos de robo de identidad. Los crímenes basados en transacciones tienen un enfoque más económico, donde el fraude, la piratería digital, el lavado de dinero y la falsificación dominan el área. Finalmente, la alteración de los datos se refiere principalmente al spam y la denegación de servicio; después de todo, solo un pequeño error en el código de una computadora puede marcar la diferencia.

**Denunciantes**

Pero no todos los hackers hacen el trabajo en beneficio personal. Por ejemplo, hay quienes intentan violar sistemas para sacar algo a la luz; específicamente, hay quienes desean hacer que algunos documentos del gobierno lleguen a la atención del público. Tales personas se conocen comúnmente como denunciantes. Se proporciona un resumen rápido de dos denunciantes conocidos internacionalmente.



Edward Snowden es un ex empleado de la Agencia Central de Inteligencia que filtró documentos confidenciales de la Agencia de Seguridad Nacional. En 2006, fue contratado por la CIA como un experto en TI y recibió autorización de alto secreto. Un año después fue colocado en Ginebra, Suiza; allí, "[él] se dio cuenta que era parte de algo que estaba haciendo más daño que bien". Después de ser despedido por romper archivos clasificados, fue contratado por Dell y continuó trabajando en la CIA y la NSA. En Hong Kong, en junio de 2013, se reveló que era la fuente de las filtraciones. La mayoría de América Latina expresó su apoyo, pero Ecuador se hizo cargo ofreciendo asilo político en conformidad con una cláusula de exención en un tratado de extradición firmado con los Estados Unidos; Las relaciones entre Estados Unidos y China sufrieron. Snowden vuela a Moscú, donde se le permite permanecer hasta 2020.



Julian Assange es un programador de computadoras y es mejor conocido por su sitio web WikiLeaks. Originalmente fundó esta "biblioteca gigante de los documentos más perseguidos del mundo" en 2006, pero solo adquirió importancia internacional cuando Chelsea Manning, un ex soldado estadounidense, reveló documentos de los EEUU en 2010. Ese mismo año fue detenido por acusaciones violación y abuso sexual. Los esfuerzos para apelar la decisión del Tribunal Superior de Londres han fallado tendrá que ser extraditado a Suecia. En agosto de 2012, la embajada ecuatoriana anunció que estaba otorgando asilo político a Assange. Un año más tarde presenta una queja ante las Naciones Unidas Arbitraria alegando que su "encarcelamiento" es el equivalente a una detención ilegal. En septiembre de 2016, Assange aceptó tiempo de prisión en los Estados Unidos a cambio del indulto de Chelsea Manning.

**Guerra Cibernética Doméstica/Industrial**

Pero, ¿es mejor más ciberseguridad y mejor tecnológica? De cierto modo, toda esta innovación tecnológica trae una situación comprometedora a los países bien desarrollados porque se han vuelto tan dependientes en algunas áreas que es casi imposible regresar a métodos y procesos no no técnicos. Con eso también viene lo que se conoce como el "Internet de las cosas", o IoT. Debido a que la tecnología se está generalizando e interconectando, los datos se intercambian tan rápido como se expande. Para empeorar las cosas, la cantidad de tipos de tecnología está aumentando a un ritmo exponencial, pero no hay una fuerza de trabajo lo suficientemente grande como para garantizar su protección.

     Al analizar el alcance de los problemas de ciberseguridad, uno debe mirar las estadísticas y tendencias. Por ejemplo, los ataques están evolucionando para incorporar más técnicas sin archivos, principalmente porque los antivirus tradicionales dependen de las detecciones de archivos; a su vez, las soluciones antivirus ahora se están complementando o reemplazando, pero curiosamente algunos usuarios simplemente ya no usan el antivirus; para que coincida con aquellos que desean una protección efectiva, la seguridad es cada vez más costosa y difícil de administrar. Otra tendencia fue la drástica disminución en el uso de ransomware y el aumento del malware cryptomining; finalmente, muchas personas se dieron cuenta de los peligros del ransomware y muchos optaron por nunca pagar los rescates, e incluso si lo hicieran, el hacker necesitaba encontrar una forma segura para que la transacción suceda; al final, la criptomoneda fue una alternativa más sigilosa y efectiva al ransomware.

     Las pequeñas empresas también sufren ya que la mayoría de los propietarios no toman la ciberseguridad tan en serio como deberían y/o no tienen los recursos necesarios para hacerlo. Las estimaciones recientes muestran que la mayoría de los ciberataques a pequeña escala se dirigen a las pequeñas empresas; a su vez, los propietarios de negocios tendrán más probabilidades de pagar rescates para restablecer la clientela y los datos privados; incluso entonces, alrededor del sesenta por ciento de las empresas cierran en el plazo de seis meses después de un ciberataque.

     Aunque se debe hacer mucho para garantizar la seguridad, los pasos más simples incluyen realizar actualizaciones de software, habilitar la autenticación de dos factores, realizar copias de seguridad de los datos regularmente, actualizar contraseñas y mantener un antivirus de calidad.

**Seguridad Cibernética y Educación**

     Por extraño que parezca, la industria de la educación superior es la mina de oro para los piratas informáticos que ahora se está apreciando cada vez más. La información que siempre se almacena en los archivos de la computadora incluye números de seguridad social, direcciones y un historial de contraseñas. Además, todos los pagos realizados, ya sea en persona o en línea, inician sesión y revelan los préstamos y las credenciales bancarias. Por suerte, la educación superior todavía puede tener un futuro seguro. La solución más ampliamente propuesta es crear conciencia de seguridad en el cuerpo estudiantil y sus familias y la administración. Los departamentos de TI, deberían estar más preocupados sobre qué hacer *cuando* ocurre un ataque, no *si*; también deberían probar regularmente el sistema buscando vulnerabilidades y riesgos, y buscar una respuesta proactiva a incidentes conocida como "búsqueda de amenazas dirigidas". Sin embargo, la creación de una medida más estricta para acceder a esta información se vuelve contra intuitiva si el objetivo es facilitar el uso para los estudiantes y los padres. Y si bien existe una ciber protección que puede garantizar la seguridad, no todas las instituciones tienen el presupuesto para adquirirla.

**Ciberseguridad y Cuidado de la Salud**

La información médica de un paciente es estrictamente confidencial, y mientras los hospitales y las instituciones de salud están bajo su custodia, el propietario es el paciente mismo; por lo tanto, la mayoría de los lugares implementan gobernanza de la información (GI), pero eso no es suficiente. Lo primero que debe hacer una institución de salud es comprender completamente qué característica de seguridad tiene (más de las veces, no sabía que tenían una función o dos). Otra cosa que los proveedores de servicios de salud deben entender es que no se trata de cuánto gastaron en seguridad, sino en el diseño de la misma; con una estructura defectuosa, y el hacker puede acceder fácilmente a un agujero que no está cubierto por el antivirus. Además, muchos analistas miran la brecha en sí misma, pero rara vez se olvidan de mirar el sistema como un todo; ¿quién sabe si se puede repetir en otro lugar? Por último, la mayoría de los empleados se olvidan de asistir a seminarios de seguridad porque están tan preocupados con sus trabajos inmediatos.



**Ciberseguridad y Energía**

La industria de la energía es una de las mayores infraestructuras en riesgo de un ciberataque. Por lo tanto, el sector de la energía debería fortalecer la preparación para la seguridad cibernética, coordinar la respuesta y la recuperación, y acelerar la investigación y el desarrollo de sistemas de suministro de energía. Sin embargo, el mayor desafío es que la mayor parte del poder [eléctrico] de una nación se mantiene de forma privada, por lo que es necesario que exista una fuerte conexión entre los gobiernos y el sector privado; sin una alianza fuerte, la conciencia situacional será difícil de lograr cuando no hay suficiente información para procesar. Si los hackers pudieran infiltrarse en la red de energía, tendrían la capacidad de causar atrocidades de poder generalizadas que pueden afectar a todas las áreas de la sociedad, poniendo en riesgo la salud y la seguridad de millones de personas. Para empeorar las cosas, los hackers de la energía tienen muchas formas diferentes de lograr el mismo objetivo; por ejemplo, algunas infracciones informadas se han dirigido a empresas de gasoductos de gas natural en los EE. UU. y Canadá que controlan más de la mitad de los oleoductos en el hemisferio occidental.

**Seguridad Cibernética y la Economía**

Es imposible lograr una medida de seguridad perfecta porque siempre hay algún nivel de pérdida, pero entendiendo qué nivel de pérdida aceptable queda por definir. Como la mayoría del sector empresarial está adoptando la transformación digital, algunos todavía se preguntan si la ciberseguridad debería ser parte de una estrategia global. De cualquier manera, los gobiernos, las industrias y las organizaciones de monitoreo deben implementar estándares que se deben aplicar conjuntamente a la industria de seguros. Otra cosa a considerar es la importancia del marketing en línea, incluyendo el uso de criptomonedas. Un escenario de baja probabilidad con alto impacto incluye un hackeo en el mercado bursátil; mientras que un pirata informático puede optar por bloquear el mercado de una sola vez, un resultado mucho peor sería manipular ciertas operaciones. Por otra parte, todos los intercambios, incluso los no regulados, son difíciles de controlar por completo, verificar cada vez más.



**Preocupaciones Militares**

Por último, pero no menos importante, el elefante en la habitación: la seguridad cibernética en relación con lo militar. La guerra cibernética ahora es más barata, más rápida y menos horripilante que la guerra tradicional. De cierto modo, las naciones pueden encerrarse en una guerra cibernética, una comparable a la Guerra Fría entre los Estados Unidos y Rusia en los años ochenta. En otras palabras, la guerra de la web se ha convertido en un juego de ajedrez que aún espera que se realice el primer movimiento.

     Cuando el militar comenzó a actualizar su software, la tecnología computacional estaba poco desarrollada. El tiempo avanzo y la responsabilidad del ejército creció con la cantidad de poder que obtuvo. Con la integridad de la comunicación segura comprometida, la toma de decisiones puede ser difícil porque incluso la interferencia más pequeña no puede determinarse de inmediato, ya que puede abarcar desde ataques cibernéticos hasta fallas del sistema e incluso errores humanos. Muchas de las armas modernas de los militares dependen de la tecnología, pero incluso más proyectos pasivos, desde drones hasta comunicaciones, son igualmente importantes. Los Departamentos de Defensa de todo el mundo están implementando más programas para reducir el riesgo de ciberataques y amenazas internas, muchas de las cuales planean aumentar el número de empleados de ciberseguridad.

Otro aspecto importante de los militares es salvaguardar los secretos. Mientras que algunos documentos se desclasifican y están disponibles para el público, otros deben o deben ser secretos, ya que revelarlos podría comprometer la integridad de cualquier situación.

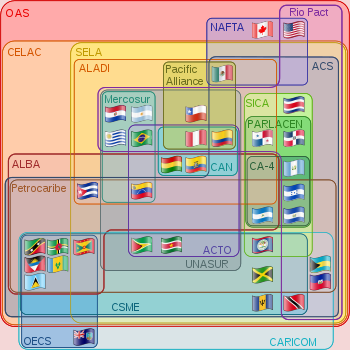
     Pero, ¿qué pasa con los casos en que el pirateo está patrocinado, ya sea por un grupo rebelde o por un gobierno? Entre el ciberterrorismo. La conciencia pública ha crecido desde el ataque a las Torres Gemelas el 12 de septiembre de 2001, sin embargo, la mayoría de las veces es un evento de piratería informático con solo un boletín semanal; una vez más, si hubiera infracciones en la seguridad nacional, los gobiernos harían lo posible por encubrirlo. De cualquier manera, un ataque cibernético es un arma asimétrica de gran igualación, pero hay poca evidencia que respalde que los militares la estén usando activamente en sus operaciones. En este momento, parece que los ciberataques y las armas cibernéticas son más para la actividad subrepticia y la señalización del estado que para fines de guerra, la pregunta sigue siendo si todo eso cambiará.

**Solución posible: Creación de la ULA**

Quizás una de las soluciones más idealistas para combatir el ciberterrorismo es a través de una especie de alianza latinoamericana similar a la Unión Europea. Crear una organización de este tipo requeriría una integración de las economías antes de políticamente unificarse. Primero, los países latinoamericanos tendrían que promover el libre comercio entre los estados miembros, generalmente empezando con la abolición de los aranceles; tal proyecto fue visto entre los Estados Unidos y la Unión Europea en un esfuerzo por socavar la influencia de China en el mercado pero debido a desacuerdos principalmente sobre la agricultura y el uso de organismos genéticamente modificados (OGM), el pacto conocido como la Asociación Transatlántica para el Comercio y la Inversión (ATCI) nunca pudo ponerse en acción. El segundo paso es crear una unión aduanera que lleve al establecimiento de un mercado común, donde los bienes, servicios, capital y personas puedan moverse libremente a través de las fronteras. Entonces se debe establecer una unión económica antes de establecer una unión política. Actualmente, la Unión Europea está, en el mejor de los casos, en el cuarto escalón, pero la situación de Europa no se puede aplicar exactamente a América Latina.

     Hay otras entidades políticas y económicas que fueron probadas en sueños de intentar alcanzar ese tipo de unión. Por ejemplo, Mercosur (Argentina, Brasil, Paraguay, Uruguay y Venezuela) muestra una gran promesa de éxito, especialmente después de la suspensión de Venezuela a fines de 2016, pero está teniendo problemas para asegurar las relaciones con la Unión Europea por varias razones en ambos lados, liberando el bloque para comenzar negociaciones comerciales con Canadá, Australia y Nueva Zelanda. Otro pequeño ejemplo es la Alianza del Pacífico (Chile, Colombia, México y Perú), cuyas metas son similares a las del Mercosur, pero están principalmente relacionadas con las zonas económicas que bordean su océano; mientras México cree que Canadá candidato prometedor, los expertos creen que el futuro del bloque depende de las relaciones comerciales con Brasil y Argentina. En una escala socioeconómica más amplia, el Sistema Económico Latinoamericano y del Caribe (SELA) cuyas negociaciones sobre el Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT) condujeron con éxito a nuevas políticas promulgadas posteriormente en la Organización Mundial del Comercio (OMC).

El comité en sí es la mayor alianza "exclusiva" que el hemisferio occidental tiene para ofrecer (aparte de la Organización de Estados Americanos).



Entonces, ¿cuál es la importancia de unificar América Latina con respecto a la ciberseguridad? Si el comité decide crear una alianza paralela a la Unión Europea, entonces un posible comienzo es usar los "Tres Pilares" (en la UE, son comunidades europeas, política exterior y de seguridad común, y cooperación en justicia y asuntos de interior). Al crear tal vínculo, los Estados miembros podrán combatir adecuadamente cualquier ciber-amenaza planteada no solo para los gobiernos latinoamericanos, sino también para las personas a que protegen… ¿o es CELAC ya en camino de serlo?

Si hay una cosa que se debe tener en cuenta, es la siguiente: para defenderte con éxito debes tener razón en tus cálculos y métodos cada vez ... pero solo necesitas tener razón una vez para tener un ataque exitoso.



Aquí hay una lista de términos, personas y eventos para comenzar su investigación:

|  |  |  |
| --- | --- | --- |
| cadena de suministro  computacion en la nube  control de acceso  ethernet  gusano  hacker  información privada/pública  malware  servidor de datos  suplantación de identidad  virus  WiFi | Albert Gonzalez  Anónimo  Chelsea Manning  Coleen Rowley  Daniel Ellsberg  Edward Snowden  Gary McKinnon  Mark Hodler  Julian Assange  W. Mark Felt | 1932: el Enigma es descifrado  1980: FBI y National CSS  1988: gusano Morris  2002: ataque contra el Internet  2009: ataque contra Google China  2010: gusano Stuxnet encontrado en Irán  2016: hackeo en las elecciones EEUU |
| IaaS  ISP  IDS  IPS  LAN  PaaS  SIEM  SaaS  VPN  WAN | Infraestructura como servicio  Proveedor de servicios de Internet  Sistema de detección de intrusiones  Sistema de prevención de intrusiones  Red de área local  Plataforma como servicio  Información de seguridad y gestión de eventos  Software como servicio  Red privada virtual  Red de área amplia | |

Además, las siguientes preguntas deben tenerse en cuenta cuando investigando el tema:

* ¿Es la ciberseguridad un derecho o un privilegio?
* ¿Debería un gobierno ser considerado responsable si pierde la identidad de las personas o documentos confidenciales? ¿Empresa / organización? ¿Individual?
* ¿Se convertirán los ciberataques en el mayor riesgo para los gobiernos?
* ¿Qué nivel de inversión se requiere para aumentar la seguridad en el sector público/privado?
* Como todo comienza a automatizarse, ¿cómo cambia el "Internet de las cosas"?

Esta sección tiene fuentes para comenzar cualquier investigación:

* "History Of The Enigma". *Cryptomuseum.Com*, 2012, http://www.cryptomuseum.com/crypto/enigma/hist.htm.
* "Tips De Seguridad Cibernética Para Mantener Tu Empresa Segura". 2017, https://es.workmeter.com/blog/tips-de-seguridad-cibernetica-para-mantener-tu-empresa-segura.
* Acurio del Pino, Santiago. "Delitos Informáticos: Generalidades". Pontificia Universidad Católica Del Ecuador, 2014.
* Anderson, Chris, and Richard H. Ledgett. “The NSA responds to Edward Snowden’s TED Talk.” *TED: Ideas Worth Spreading*, TED, 20 Mar. 2014, https://www.ted.com/talks/richard\_ledgett\_the\_nsa\_responds\_to\_edward\_snowden\_s\_ted\_talk.
* Central Intelligence Agency (2001). *Statement for the Record: Cyber Threat Trends*. Central Intelligence Agency.
* Colarik, Andrew M., et al. *Cyber Security and Policy : a Substantive Dialogue*. Auckland, New Zealand : Massey University Press, 2017.
* Davis II, John S. et al. *Stateless Attribution: Toward International Accountability In Cyberspace*. RAND Corporation, 2017.
* Defranco, Joanna F, and Proquest (Firm). *What Every Engineer Should Know about Cyber Security and Digital Forensics*. Boca Raton : CRC Press, 2014.
* El Economista. "América Latina Es Vulnerable A Ataques Cibernéticos". 2014, https://www.eleconomista.com.mx/tecnologia/America-Latina-es-vulnerable-a-ataques-ciberneticos-20160314-0147.html.
* Green, James A. *Cyber Warfare: A Multidisciplinary Analysis*. Oxon Abingdon, 2015.
* Henry, Shawn. "International Conference On Cyber Security". Fordham University, 2012.
* Hsu, D. Frank, and Dorothy Marinucci. *Advances In Cyber Security: Technology, Operations, And Experiences*. Fordham University Press, 2013.
* Lee, Timothy B. "How A Grad Student Trying To Build The First Botnet Brought The Internet To Its Knees". *The Washington Post*, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/.
* McLellan, Vin. "Case Of The Purloined Password". *The New York Times*, 1981, http://www.nytimes.com/1981/07/26/business/case-of-the-purloined-password.html?pagewanted=all.
* Mendoza, Miguel Ángel. "¿Ciberseguridad o seguridad de la información? Aclarando la diferencia". *Welivesecurity*, 2015, https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/.
* Nader, Karim. "Riesgos En La Seguridad Informática En Salud". *Elhospital.Com*, 2016, http://www.elhospital.com/temas/Seguridad-informatica-en-salud+111853.
* Notimérica. "¿Cómo Está Iberoamérica En Seguridad Informática?". 2017, http://www.notimerica.com/sociedad/noticia-iberoamerica-seguridad-informatica-20170727072947.html.
* Organización de los Estados Americanos. *TENDENCIAS DE SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE*. Symantec, 2014, http://www.symantec.com/content/es/mx/enterprise/other\_resources/b-cyber-security-trends-report-lamc.pdf.
* Roy, Joaquín et al. *Después De Santiago: Integración Regional Y Relaciones Unión Europea - América Latina*. Jean Monnet Chair, University Of Miami, 2013.
* Roy, Joaquín, and Roberto Dominguez. *The European Union And Regional Integration: A Comparative Perspective And Lessons For The Americas*. Jean Monnet Chair, University Of Miami, 2005.
* Shofield, Jack. "Google, Yahoo, Adobe And Who?". *The Guardian*, 2010, https://www.theguardian.com/technology/2010/jan/14/google-yahoo-china-cyber-attack.
* The Register. "Feds Investigating ‘Largest Ever’ Internet Attack". 2002, https://www.theregister.co.uk/2002/10/23/feds\_investigating\_largest\_ever\_internet/.
* Zeitz, Josh. "Foreign Governments Have Been Tampering With U.S. Elections For Decades". *Politico*, 2016, https://www.politico.com/magazine/story/2016/07/russia-dnc-hack-donald-trump-foreign-governments-hacking-vietnam-richard-nixon-214111.
* Zetter, Kim. "An Unprecedented Look At Stuxnet, The World's First Digital Weapon". *Wired*, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Al enviar su documento de posición, asegúrese de que el formato sea Times New Roman, letra de 12 puntos, espaciado de línea de 1.5, no más de una página (de doble cara). Los documentos deben entregarse antes del 8 de abril de 2018 a la medianoche, el domingo antes de la competencia.

No se requiere una bibliografía.

Envíe por correo electrónico los documentos de posición y cualquier pregunta / inquietud a micsuncepal@gmail.com.

"La verdadera ciberseguridad es prepararse para lo que viene...

no lo que fue último." - Neil Rerup



