

# La Aviación y el Espacio Cibernético— Convergencia de Ámbitos, Convergencia de Amenazas

EMILIO IASIELLO

## Introducción

La amenaza cibernética es uno de los peligros más comentados que enfrenta la comunidad internacional porque es global en alcance e impacta cualquier organización pública o privada que utiliza la *Internet*. Es un entorno que favorece al delincuente ya que hay pocas e ineficaces leyes que rigen la actividad que atraviesan las redes interconectadas, creando un ámbito funcional y sin fronteras. Como tal, los malhechores operan en un entorno oscuro donde sus actos se pueden esconder en grandes volúmenes de tráfico en la *Internet*. Los creadores de *malware* fabrican y venden sus creaciones sofisticadas, y no tan sofisticadas, en el mercado negro a actores de varios niveles de destreza para emplearlo en una amplia variedad de actividades hostiles que incluyen la perdurabilidad de la delincuencia cibernética; operaciones *hacktivistas* motivadas política o ideológicamente o el acceso oculto a redes y el robo de propiedad intelectual y documentos reservados que apoyan el espionaje industrial o de la nación estado. Recordando el viejo oeste de Estados Unidos de fines de los años 1800, no hay una presencia policial ni leyes penales comúnmente aceptadas que mantengan a los malhechores bajo control. Como resultado, los gobiernos extranjeros han reconocido la importancia de asegurar sus propias partes de esta red global, y algunos de ellos han redactado, o están redactando, estrategias nacionales de seguridad cibernética para tratar esta amenaza complicada y enigmática. Estados Unidos en particular ha tomado iniciativas agresivas para convertir la cibernética en un problema militar, esbozando en su *International Strategy for Cyberspace* (Estrategia internacional para el ciberespacio) de mayo de 2011 que “se reserva el derecho de emplear todos los medios necesarios—diplomático, informático, militar y económico—según sea prudente y consistente con las leyes internacionales pertinentes”.<sup>1</sup> Si bien es un primer paso positivo, el panorama comercial estadounidense permanece fragmentado y tribal en términos de seguridad cibernética de la organización, según se comprobó en los 15 Centros de Análisis e Intercambio de Información (ISAC; por sus siglas en inglés) establecidos federalmente y específicos a la industria<sup>2</sup> cuya misión es proporcionar información precisa y oportuna a los miembros interesados de la infraestructura crítica. El ISAC de Transporte (PT ISAC, por sus siglas en inglés) en particular tiene una labor ingrata de tratar de llevar a cabo esta función a lo largo de todos los sistemas de transporte público. A medida que las aeronaves se modernizan y adoptan la capacidad de operaciones interconectadas, la aviación confrontará actores hostiles, vulnerabilidades de equipo, *malware* programado, actividad maliciosa y retos de seguridad relacionados con este panorama de amenaza nuevo. En lugar de reaccionar a este entorno de amenaza dinámico y complejo, la aviación necesita tratar de manera preventiva las amenazas cibernéticas para adelantarse al problema o de lo contrario arriesgar ponerse al día en un entorno donde los malos están escondidos y las actividades hostiles ocurren en nanosegundos.

## Incidentes cibernéticos en la aviación que deben mencionarse

La industria de la aviación—y en particular el proceso de viajes aéreos—ha tenido el lujo inesperado de no ser el objetivo de ataques visibles y considerables. Si bien ha habido incidentes bien difundidos de supuesto espionaje cibernético, los actores que buscan lograr el acceso no autorizado en la base industrial de la aviación, no ha habido informes similares perceptibles de actores hostiles atacando una *aeronave en movimiento*; o sea, de pista a pista. La aviación necesita considerar esto como una gran oportunidad para tratar las fallas de seguridad cibernética en el equipo, comunicaciones o cualquier punto de acceso que pueda ser aprovechado por actores técnicamente experimentados. En el 2011 hubo varios incidentes notables de actores hostiles dirigiendo sus operaciones cibernéticas malvadas contra los intereses de la aviación. Se sospecha que la mayoría de ellos fueron llevados a cabo por actores de espionaje ya que la mayoría se enfocaron en lograr acceso no autorizado a redes para fines de recopilación de información consistente con el comportamiento de actores de espionaje. No mostraron una intención destructiva típica de un *hacktivista* (por ejemplo, mediante ataques distribuidos de negación de servicio, degradación de un sitio *web*, etc.), ni tampoco implementaron campañas de *spam* de correo electrónico y correos electrónicos con virus *Trojan* para lograr acceso y obtener información personal identificable para fines de monetización como lo hacen típicamente los delincuentes cibernéticos.

- **Abril de 2011:** *L-3 Communications* fue el blanco de *hackers* utilizando *SecurIDs* comprometidos, un sistema de autenticación de dos factores. *L-3* no tenía claro si el ataque tuvo o no éxito, pero el evento fue significativo en que fue la primera vez que se utilizaban *SecurIDs* para intentar lograr acceso a una red.<sup>3</sup>
- **Mayo de 2011:** *Lockheed Martin* fue el blanco en una campaña de espionaje cibernético. Aparentemente, los agresores poseían las *seeds*—claves al azar codificadas por el fabricante—utilizadas por al menos algunos de los mandos (*job*) de *hardware* de *SecurID*, al igual que números de serie y el algoritmo subyacente utilizado para asegurar los dispositivos. Esta actividad fue detectada de manera oportuna y no hubo informes de que la información fuese robada o comprometida.<sup>4</sup>
- **Mayo de 2011:** *Northrop Grumman* fue el blanco en una campaña de espionaje cibernético similar a la de *Lockheed Martin*. Los agresores trataron de lograr acceso empleando *RSA Seeds* comprometidas. La actividad fue detectada antes de que se pudiesen robar la información.<sup>5</sup>
- **Octubre de 2011:** Un virus de computadora infectó las cabinas de los vehículos no tripulados estadounidenses, *Predatory Reaper*, anotando todas las pulsaciones de los pilotos a medida que volaban misiones por control remoto sobre Afganistán y otras zonas de guerra. La remoción del virus requirió múltiples esfuerzos indicando que el virus era resistente a la mitigación.<sup>6</sup>
- **Diciembre de 2011:** Irán alega haber explotado una vulnerabilidad conocida del GPS para engañar al vehículo no tripulado para que aterrizara en Irán.<sup>7</sup>

Tal como se ilustra en los ejemplos anteriores, no ha habido un ejemplo real de un actor hostil intentando impactar una aeronave durante el proceso del viaje aéreo. Sin embargo, si analizamos el progreso del entorno de la amenaza cibernética, podemos apreciar un paisaje dinámico donde los malhechores han aumentado continuamente sus capacidades y actividades en muy poco tiempo. El *malware* en sí ha cambiado dramáticamente. Desde el *Morris Worm* de 1988 cuyas consecuencias no intencionales causaron ataques de negación de servicio, hasta el descubrimiento del *Stuxnet* en el 2010, concebido para atacar *software* y equipo industrial específico, muestra cuán rápido las armas cibernéticas han logrado un nivel sofisticado de emplazamiento de armas.

Fecha	Fuente	Ataque	Blanco	Vector
6 de abril de 2011	 China	<b>Comunicaciones L-3</b> Un correo electrónico con fecha del 6 de abril, enviado a 5000 empleados del contratista L-3 del DOD de E.UU., advierte sobre un intento de ataque efectuado con SecurID Seeds comprometidos. No está claro si el ataque tuvo éxito (fue revelado medio mes antes). Este es el primer ataque hecho con semillas RSA comprometidas.		SecurID comprometidas
21 de mayo de 2011	 China	<b>Lockheed Martin</b> Este es el primer ataque que se conoce (y el único reconocido oficialmente hasta el momento) perpetrado con semillas SecurID comprometidas que atacan a un contratista de la Defensa. El ataque fue detectado antes de que pudiesen robar información clasificada. Como precaución, se cerraron 100.000 cuentas.		SecurID comprometidas
26 de mayo de 2011	 China	<b>Northrop Grumman</b> Tercer contratista de la Defensa atacado utilizando semillas RSA comprometidas. El ataque fue detectado antes de que pudiesen robar información clasificada. El acceso remoto fue cerrado.		SecurID comprometidas
8 de octubre de 2011	? Se desconoce	<b>Vehículos aéreos no tripulados estadounidenses</b> Un virus de computadora infectó las cabinas de los vehículos no tripulados estadounidenses, Predator y Reaper, anotando todas las pulsaciones de los pilotos a medida que volaban misiones por control remoto sobre Afganistán y otras zonas de guerra. El virus fue detectado hace dos semanas en el Sistema de Control Terrestre (GCS) en la Base Aérea Creech, Nevada, y no ha interrumpido las misiones de vuelo de los vehículos aéreos no tripulados, mostrando una fortaleza inesperada de manera que múltiples intentos fueron necesarios para eliminar el virus de las computadoras en Creech.		Malware genérico a través de un USB stick
9 de diciembre de 2011	 Irán	<b>Lockheed Martin RQ-170 Sentinel</b> Un RQ-170 Sentinel hace un aterrizaje forzoso en Irán. Después de unos días, según informes del Christian Science Monitor, Irán pudo capturar el RQ-170 estadounidense explotando una vulnerabilidad conocida en el GPS, engañando a la aeronave a que aterrizara en Irán.		¿Piratería al GPS?

Figura 1. Lista de algunas actividades notables producidas por Hackmageddon.com<sup>8</sup>

## Incidentes en aeropuertos que deben mencionarse

Los aeropuertos han sido víctimas de supuestas actividades ilícitas por parte de actores. En un aeropuerto hay muchos posibles puntos de entrada digitales que pueden ser el blanco para la interrupción. Las comunicaciones entre el control de tráfico aéreo y la aeronave, los servicios de abordaje y registro de pasajeros (que son accesibles en la *Internet*), los sistemas para procesar pasajeros, redes virtuales privadas en los aeropuertos (empleadas para asegurar las conexiones en la *Internet* entre la red privada de una organización y un empleado a distancia) y las redes inalámbricas son tan solo algunos de los sistemas dentro del entorno de un aeropuerto que pueden ser atacados y explotados para fines viles. Algunos incidentes recientes destacan la posible amenaza de actores hostiles tratando de lograr el acceso no autorizado a las redes de los aeropuertos.

- **Agosto de 2012:** Una empresa de seguridad digital en Boston descubrió un *malware* escondido en la red virtual privada (VPN, por sus siglas en inglés) en un aeropuerto internacional importante fuera de Estados Unidos. La amenaza pudo haber comprometido todo, desde la información personal de los empleados hasta la seguridad de los pasajeros, alegó la empresa. El ataque empleó el *malware Citadel Trojan* para leer las pantallas de los empleados quienes se conectaron por control remoto a la red del aeropuerto.<sup>9</sup>

- **Junio de 2012:** *Software* de juego infectado fue dirigido por un servidor de comando para atacar el Aeropuerto Internacional Incheon de Corea del Sur en un intento de interrumpir el tráfico de vuelo vía un ataque *DDoS*.<sup>10</sup>
- **Junio de 2011:** Vuelos fueron afectados en la Terminal 3 del Aeropuerto Internacional Indira Gandhi cuando el Sistema de Procesamiento de Pasajeros de Uso General (CUPPS, por sus siglas en inglés) falló y estuvo sin funcionar por casi doce horas. Las investigaciones iniciales revelaron que el uso de un “código malicioso” de un lugar remoto desconocido causó la falla del CUPPS.<sup>11</sup>

En dos de esas ocasiones, hubo poco conocimiento de los individuos responsables por los ataques. En el incidente de Corea del Sur, un hombre fue arrestado quien se presume haber comprado el *software* para juegos de agentes de inteligencia de Corea del Norte. Ya sea a sabiendas o no, estos ejemplos muestran el panorama variado de actores que pudiesen ser responsables de los ataques cibernéticos perpetrados contra los aeropuertos.

## Actores de amenaza cibernética — ¿Quiénes son los malos?

El anonimato de la *Internet* proporciona una larga lista de actores estatales y no estatales que operan bajo un manto de oscuridad. Los ataques específicos y no específicos que originan de esas fuentes han afectado a los sectores público y privado alrededor del mundo. Si bien hay pruebas limitadas que esos actores atacan la aviación mediante medios cibernéticos, el volumen está sujeto al cambio basado en la intención del actor al igual que sus capacidades y los recursos necesarios para llevar a cabo esos ataques. Con base en la evolución del *hacking*, todos los sectores industriales estadounidenses han sido víctimas de actores viles en un momento u otro. La agricultura<sup>12</sup>, la base industrial de la Defensa<sup>13</sup>, la energía<sup>14</sup>, finanzas<sup>15</sup>, el gobierno<sup>16</sup>, cuidado de la salud<sup>17</sup>, militares<sup>18</sup>, y el agua<sup>19</sup> han enfrentado actividades cibernéticas hostiles de uno o más de los siguientes grupos de actores de amenaza:

- **Hactivistas:** Los *hactivistas* son *hackers* motivados política o ideológicamente para llevar a cabo actividades hostiles y a veces destructivas en apoyo a una causa o creencia. Grupos como *Anonymous* participan en operaciones contra blancos para castigar una transgresión percibida o llamar la atención a una situación. El comportamiento típico del *hactivista* incluye ataques de negación de servicio distribuido (DDoS, por sus siglas en inglés) que inunda el servidor de un sitio web de tanto tráfico que lo torna inoperable; degradación de sitios web, que es una forma de grafiti electrónico para enviar mensajes; *doxing* que es un proceso donde se roba y se publica en la *Internet* la información personal (por ejemplo, la dirección, número de teléfono e información personal identificable, etc.). Los *hactivistas* han demostrado repetidamente su voluntad para llevar a cabo operaciones cibernéticas ofensivas contra empresas que ellos piensan merecen servir de escarmiento. Si una aerolínea cae en la mira de un grupo *hactivista*, se espera que una actividad cibernética hostil, como mínimo, atacaría las páginas web de la aerolínea.
- **Hackers:** Los *hackers* (piratas cibernéticos) penetran las redes por la emoción del reto, o para alardear en la comunidad de *hackers*, entre otros motivos. Se diferencian de los *hactivistas* en que sus motivos no están basados ni en la política ni en la ideología. Si bien logran acceso a una red o computadora utilizada para requerir un nivel de destreza que separaba a los *hackers* expertos de los novatos, ahora los *hackers* pueden descargar *script* y protocolos de ataque de la *Internet* para lanzarlos contra los blancos.<sup>20</sup> Es más, esas herramientas para atacar se han tornado cada vez más sofisticadas a la vez que se han tornado más fáciles de utilizar, negando la necesidad de un individuo de ser un experto para lanzar ataques. Los sitios

de *hacking* cuentan con herramientas gratis, instrucciones y una plétora de *hackers* expertos que sirven de mentores para aquellos con menos experiencia.

- **Actores no estatales:** Los actores de naciones estados típicamente emplean el espionaje cibernético para recopilar información confidencial e información sobre la propiedad intelectual de sus blancos. Sin embargo, dependiendo de la intención de los actores de la nación estado, lograr acceso no autorizado a redes objetivos se puede aprovechar para hacer un reconocimiento y trazar un mapa de la red para poder obtener información de inteligencia para un ataque más adelante. Esto se considera el equivalente cibernético de “preparación de inteligencia del campo de batalla”.
- **Grupos terroristas:** Si bien los grupos y las organizaciones terroristas prefieren ataques cibernéticos contra sus blancos, hay un caudal de información cada vez mayor sobre el uso del ámbito cibernético por los terroristas. Principalmente, los terroristas emplean el ciberespacio para el reclutamiento, difusión de propaganda, provocación, radicalización, financiamiento, entrenamiento, planificación e investigación.<sup>21</sup> Sin embargo, ciertos líderes terroristas a veces han exhortado a los islamistas radicales a que usen la *Internet* para fines más operacionales. En el 2004, Imam Samudra, el individuo responsable de manipular los bombardeos en el club nocturno en Bali, publicó una autobiografía detallando el uso de cometer delitos cibernéticos contra los intereses de Estados Unidos para llevar al país a la bancarrota.<sup>22</sup> Después de la muerte de Osama Bin Laden en el 2012, un vídeo de Al-Qaeda promovió una *jihād* electrónica contra Estados Unidos.<sup>23</sup>
- **Infiltrados:** Un infiltrado a sabiendas o no puede proveerles a los actores hostiles acceso directo a redes y sistemas que ellos quieren atacar para interrumpir, destruir o manipular. Según un estudio, ellos son las fuentes principales de delitos en computadora.<sup>24</sup> Los infiltrados son cualquier individuo que tiene acceso directo o indirecto a una computadora o red específica.

## Amenazas futuras de *malware* y la aviación

Las amenazas cibernéticas a las redes críticas de la infraestructura continúan evolucionando a medida que el panorama global se torna cada vez más interconectado. Esencialmente, mientras más compleja y avanzada se torna la red, más fallas técnicas y vulnerabilidades contiene, y más difícil se torna administrarla desde un punto de vista de seguridad. La industria de la aviación está desplazándose hacia un entorno más interconectado para mejorar todos los aspectos de los viajes aéreos, desde una aeronave en tierra hasta el despegue. La Autoridad Federal de la Aviación de Estados Unidos calcula que para el 2020 la mayoría de las aeronaves civiles del mundo habrán implementado el Sistema de Difusión de Vigilancia Dependiente Automática (ADS-B, por sus siglas en inglés), una tecnología de vigilancia avanzada, que reemplazará al radar como el principal medio para rastrear aeronaves. Durante todos los aspectos del viaje, la información fluirá a través de este entorno interconectado desde estaciones terrestres al control de tráfico aéreo a la aeronave en vuelo. Si bien no se podrá tener acceso a esta tecnología directamente vía la *Internet*, dos anécdotas de gran impacto revelan cómo actores duchos han diseñado herramientas cibernéticas para penetrar exitosamente e impactar sistemas que no son accesibles fácilmente vía la *Internet* sino de su propia red.

- **Stuxnet:** Descubierta en el 2010, *Stuxnet* es un gusano informático concebido para atacar los sistemas de control *Siemens*. Probablemente una memoria USB lo introdujo a la red cerrada.<sup>25</sup> El *malware* fue diseñado solamente para los sistemas de control de supervisión y adquisición de datos (SCADA, por sus siglas en inglés) que fueron configurados para controlar y moni-

torear procesos industriales específicos.<sup>26</sup> Esta fue la primera vez que un arma cibernética ataca un sistema de tipo específico e impacta con éxito sus operaciones. Este gusano dañó con éxito unas 1.000 centrifugas.

- **OPERACIÓN BUCKSHOT YANKEE:** En el 2008, el Departamento de Defensa de Estados Unidos sufrió un compromiso significativo de sus redes de computadoras militares clasificadas. Comenzó cuando una unidad *flash* fue insertada en una computadora portátil militar en una base en el Oriente Medio. El código malicioso de la unidad *flash*, colocado por una agencia de inteligencia extranjera, se cargó a sí mismo a una red administrada por el Comando Central de EE.UU. Ese código se esparció sin ser detectado en los sistemas clasificados y no clasificados, estableciendo el equivalente a un punto de partida digital del cual se pudiesen transferir datos a servidores bajo control extranjero.<sup>27</sup>

Tan solo porque la industria de la aviación no ha sufrido un ataque cibernético sustancial como un *DDoS*, o un incidente como los descritos arriba, no significa que no puede suceder y no se debe dar por sentado que a causa de que las redes operacionales no están conectadas a la *Internet* que esos sistemas están protegidos del *malware*. Actos destructivos o perturbadores de *malware* (por ejemplo, *Stuxnet*, o el *malware Shamoon* del 2012 que barrió con 30.000 computadoras en la red saudí *Aramco*, borrando completamente los discos duros)<sup>28</sup> son tan solo una avenida disponible para los actores hostiles. A medida que la aviación adopta la tecnología ADS-B sumamente interconectada, varias fuentes de información serán enviadas al ADS-B incluyendo pero no limitado a las siguientes:

- **Tráfico:** Un piloto podrá tener acceso a información sobre el tráfico aéreo, incluyendo altitud, rumbo, velocidad y distancia a la aeronave.
- **Tiempo:** Las aeronaves equipadas con una tecnología UAT ADS-B podrán recibir informes de las condiciones del tiempo y del radar meteorológico mediante el servicio de difusión de información de vuelo (FIS-B, por sus siglas en inglés).
- **Terreno:** La tecnología ADS-B difunde una transparencia del terreno para que los pilotos la puedan ver en la cabina.
- **Información de vuelo:** No se debe confundir con FIS-B, servicio de difusión de información del tráfico (TIS-B, por sus siglas en inglés) transmite información de vuelo que se puede leer.<sup>29</sup>

Toda mala interpretación o manipulación a sabiendas de información de vuelo crítica puede lograr resultados dañinos igual que cualquier otro ataque cibernético. Sin embargo, en este caso, la manipulación de datos puede ser un catalizador para ocasionar daños físicos a la aeronave e impactar directamente la seguridad de los pasajeros.

## Conclusión

La industria de la aviación continúa progresando para crear un entorno en la *Internet* que interconecte exitosamente los componentes multifacéticos del panorama de la aviación. La revisión del Sistema Nacional Aeroespacial hará los viajes más convenientes y seguros, facilitando el intercambio de información a niveles sin precedente para informar mejor a los operadores y aumentar la eficacia a la vez que mantiene un nivel elevado de seguridad. Sin embargo, la tecnología involucrada en implementar un proceso de comunicaciones ininterrumpido provee una infinidad de oportunidades de las que los actores hostiles se pueden aprovechar. Aunque la aviación ha evadido con éxito la atención de actores cibernéticos hostiles, esto puede que cambie continuamente particularmente a medida que los entornos interconectados atraen el interés de actores que consideran la aviación como un blanco posible—actores de naciones estados

pueden atacar la aviación para el acceso para consideraciones futuras; los delincuentes cibernéticos pueden atacar la aviación para robar datos confidenciales o chantajear las operaciones de las aerolíneas para fines monetarios; y los *hacktivistas* pueden atacar la aviación para castigar las presuntas infracciones o para llamar la atención a sus causas políticas o ideológicas. El único factor constante entre estos actores es que son dinámicos, capaces de adaptarse rápidamente a sus entornos operativos. Si la aviación no ha sido atacada al punto que las otras lo han sido es porque estos actores aún no han reconocido cómo la aviación pudiese promover sus objetivos respectivos, y no porque no son capaces de hacerlo. La aviación está en una posición singular porque tiene la oportunidad de planificar para esas amenazas antes de que se tornen demasiado abrumantes o costosas de arreglar. Esperar para tratarlas porque aún no son un problema será equivalente a cerrar la puerta del establo cuando el caballo ya se ha escapado. □

#### Notas

1. The White House, *International Strategy for Cyberspace* (Estrategia Internacional para el Ciberespacio); mayo de 2011; consultado en: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).
2. Página web del *National Council of ISACs*, consultada en: <http://www.isaccouncil.org/membersacs.html>.
3. William Jackson, "Another Major Defense Contractor Hacked, RSA Tokens Likely Involved" (Otro contrato importante de la defensa fue pirateado, *RSA Tokens* probablemente involucrados), *Government Computer News*, 1o de junio de 2011, consultado en: <http://gcen.com/Articles/2011/06/01/Defense-contractors-L3-Lockheed-hacked.aspx?p=1>.
4. Matthew J. Schwartz, "Lockheed Martin Suffers Major Cyberattack" (*Lockheed Martin* sufre otro ataque cibernético importante), *Information Week*, 31 de mayo de 2011, consultado en: <http://www.informationweek.com/government/security/lockheed-martin-suffers-massive-cyberatt/229700151>.
5. Jeremy Kaplan, "Northrop Grumman May Have Been Hit With a Cyberattack" (*Northrop Grumman* puede que haya sufrido ataque cibernético), *Fox News*, 1o de junio de 2011, consultado en: <http://www.foxnews.com/tech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/>.
6. Noah Shachtman, "Computer Virus Hits U.S. Drone Fleet" (Virus de computadora ataca flota de aviones no tripulados de EE.UU.), *Wired Magazine*, 7 de octubre de 2011, consultado en: <http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/>.
7. Scott Peterson, "Iran Hijacked US Drone, Says Iran Engineer" (Según ingeniero iraní, Irán secuestró aeronave no tripulada estadounidense), *Christian Science Monitor*, 15 de diciembre de 2011, consultado en: <http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video>.
8. *Hackmageddon.com*, consultado en: <http://hackmageddon.com/?s=aviation>.
9. Michael Dolgow, "Cyberwars Reach a New Frontier: The Airport" (Guerras cibernéticas alcanza frontera nueva: El aeropuerto), *Bloomberg Businessweek*, 15 de agosto de 2012, consultado en: <http://www.businessweek.com/printer/articles/67128-cyberwars-reach-a-new-frontier-the-airport>.
10. Jeff Goldman, "South Korean Man Arrested Over Airport Cyber Attacks" (Surcoreano arrestado por ataques cibernéticos al aeropuerto), *ESecurity Planet*, 5 de junio de 2012, consultado en: <http://www.esecurityplanet.com/print/network-security/south-korean-man-arrested-over-airport-cyber-attacks.html>.
11. Manan Kakkar, "CBI Believes Cyber Attack Led to IGI Airport's Technical Problems in June" (CBI cree que ataque cibernético fue causa de problemas técnicos en Aeropuerto IGI en junio), *ZdNet*, 25 de septiembre de 2011, consultado en: <http://www.zdnet.com/blog/india/cbi-believes-cyber-attack-led-to-igi-airports-technical-problems-in-june/710>.
12. Eduard Kovacs, "US Department of Agriculture Sites Hacked in Protest Against Mohammed Movie" (Sitios web del Departamento de Agricultura de EE.UU. fueron pirateados en protesta contra película de Mahoma), *NewsSoftpedia*, 21 de septiembre de 2012, consultado en: [://news.softpedia.com/news/US-Department-of-Agriculture-Sites-Hacked-in-Protest-Against-Mohammed-Movie-293926.shtml](http://news.softpedia.com/news/US-Department-of-Agriculture-Sites-Hacked-in-Protest-Against-Mohammed-Movie-293926.shtml).
13. *Office of the National Counterintelligence Executive*, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace" (Espías extranjeros roban en el espacio cibernético secretos económicos de Estados Unidos), octubre de 2011, consultado en: [http://www.ncix.gov/publications/reports/fecie\\_all/Foreign\\_Economic\\_Collection\\_2011.pdf](http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf).
14. Ellen Nakashima, "U.S. Said to Be Target of Massive Cyber Espionage Campaign" (Se rumora que EE.UU. es el blanco de campaña masiva de espionaje cibernético), *Washington Post*, 10 de febrero de 2013, consultado en: <http://www.washingtonpost.com/world/US-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/>.
15. Matthew J. Schwartz, "Bank Attackers Restart Operation Ababil DDoS Disruptions" (Los que atacaron banco comienzan nuevamente interrupciones DDoS Operación Ababil), *Information Week*, 6 de marzo de 2013, consultado en: <http://www.informationweek.com/security/attacks/bank-attackers-restart-operation-ababil/240150175>.

16. Bryan Krekel, “*Capabilities of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*” (Capacidades de la República Popular China para llevar a cabo guerra cibernética y explotación de redes de computadora), *US China Economic and Security Review Commission*, octubre de 2009, consultado en: [http://www.dodea.edu/Offices/Safety/upload/14\\_china\\_spy.pdf](http://www.dodea.edu/Offices/Safety/upload/14_china_spy.pdf).
17. RSA, “*Cybercrime and the Healthcare Industry*” (El delito cibernético y la industria del cuidado de la salud), 2010, consultado en: [http://www.rsa.com/products/consumer/whitepapers/11030\\_CYBHC\\_WP\\_0710.pdf](http://www.rsa.com/products/consumer/whitepapers/11030_CYBHC_WP_0710.pdf).
18. Bob Orr, “*Pentagon Expands Cyber Defense Amid Daily Attacks*” (Pentágono amplía defensa cibernética en medio de ataques diarios), *CBS News*, 6 de febrero de 2013, consultado en: [http://www.cbsnews.com/8301-18563\\_162-57568079/pentagon-expands-cyber-defense-amid-daily-attacks/](http://www.cbsnews.com/8301-18563_162-57568079/pentagon-expands-cyber-defense-amid-daily-attacks/).
19. Ellen Nakashima, “*Foreign Hackers Target U.S. Water Plant in Apparent Malicious Attack*” (*Hackers* extranjeros atacan sistema de agua potable en supuesto ataque malicioso), *Washington Post*, 18 de noviembre de 2011, consultado en: [http://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN\\_blog.html](http://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html).
20. *Government Accountability Office*, “*Cybersecurity: Threats Impacting the Nation*” (Seguridad cibernética: Amenazas que impactan a la nación), GAO-12-666T, 24 de abril de 2012, consultado en: <http://www.gao.gov/assets/600/590367.pdf>.
21. *United Nations Office on Drugs and Crime* “*The Use of the Internet for Terrorist Purposes*” (El uso de la *Internet* para fines terroristas), 2012, consultado en: [http://www.unodc.org/documents/frontpage/Use\\_of\\_Internet\\_for\\_Terrorist\\_Purposes.pdf](http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf).
22. Alan Sipress, “*An Indonesian’s Prison Memoir Takes Holy War into Cyberspace*” (Memorias de prisionero indonesio lleva Guerra Santa al espacio cibernético), *Washington Post*, 14 de diciembre de 2004, consultado en: <http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html>.
23. Jack Cloherty, “*Virtual Terrorism: Al-Qaeda Video Calls for Electronic Jihad*” (Terrorismo virtual: Video de al-Qaeda es un llamado a *jihad* electrónica), *ABC News*, 22 de mayo de 2012, disponible en: <http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875>.
24. *Government Accountability Office*, “*Cybersecurity: Threats Impacting the Nation*,” GAO-12-666T, 24 de abril de 2012, consultado en: <http://www.gao.gov/assets/600/590367.pdf>.
25. Robert McMillan, “*Siemens: Stuxnet Hits Industrial Systems*” (*Siemens Stuxnet* ataca sistemas industriales) *Computer World*, 14 de septiembre de 2010, consultado en: [http://www.computerworld.com/s/article/print/9185419/Siemens\\_Stuxnet\\_worm\\_hit\\_industrial\\_systems?taxonomyName=Network+Security&taxonomyId=142](http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142).
26. Nicholas Falliere, “*Stuxnet Introduces First Root Kit for Industrial Control Systems*” (*Stuxnet* introduce primer *root kit* para sistemas industriales de control), *Symantec*, 9 de agosto de 2010, consultado en: <http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices>.
27. William J. Lynn, “*Defending a New Domain*” (Defendiendo un ámbito nuevo), *Foreign Affairs*, septiembre/octubre de 2010, consultado en: <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.
28. *Reuters*, “*Saudi Aramco Says Hackers Too Aim at Its Production*” (*Aramco* saudí alega que *hackers* también quieren atacar su producción), *New York Times*, 9 de diciembre de 2012, consultado en: [http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?\\_r=0](http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0).
29. *Federal Aviation Administration*, “*ADS-B Frequently Asked Questions*” (Preguntas comunes sobre ADS-B), consultado en: <http://www.faa.gov/nextgen/implementation/programs/adsb/faq/>.



**El Sr. Emilio Iasiello** es Jefe de Analista de Amenazas en iSIGHT Partner, una empresa global de inteligencia cibernética que brinda apoyo a entidades federales y comerciales para que administren riesgos cibernéticos, comprendan su entorno de la amenaza y les ayude a priorizar sus inversiones contra esas amenazas que impactan sus negocios o misión. Desde el 2002 ha trabajado en el análisis de amenazas cibernéticas tanto como contratista para el gobierno y en calidad de empleado civil con el Departamento de Estado y Departamento de Defensa respectivamente. Iasiello ha escrito varios artículos sobre el desarrollo de una nueva metodología analítica de amenazas cibernéticas y en la cadena de suministros IT.