NOTA DE FUTURO 3/2018

21 de marzo de 2018

*Julia López, Pablo Márquez y Silvia Rodríguez**

Looking into the crystal ball. ENISA
Informe sobre tecnologías emergentes y retos de seguridad

Nota de futuro: Looking into the cristal ball. ENISA
Informe sobre tecnologías emergentes y retos de seguridad

El presente documento es una síntesis y traducción de: Looking into the cristal ball. La versión original se puede encontrar en: https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball

3. Consolidación de ideas recogidas: áreas tecnológicas emergentes

Este apartado contiene información sobre la evolución de áreas tecnológicas que, se cree, serán un desafío para la ciberseguridad.

3.1. Internet of Things (Iot)[1]

Retos tecnológicos

El IoT ha sido considerado un área tecnológica emergente debido a su potencial a la hora de afectar al ser humano y liderar la transformación tecnológica. Los expertos piensan que su potencial implica numerosos retos tecnológicos.

La comunidad de seguridad es consciente de estos retos. El IoT desempeña un papel fundamental, pues ejerce funciones en distintas áreas en los entornos de los consumidores. Desde el punto de vista del mercado, el IoT:

- Es el nuevo contexto para repartir hardware, software y servicios a los consumidores.
- Crea numerosos datos reutilizables.
- Permite comercializar la vida y esfera privadas de los usuarios.
- Permite un desarrollo flexible de los entornos al mismo tiempo que facilita la unión entre consumidores.
- Constituye el siguiente nivel de convergencia de diferentes infraestructuras, datos y servicios.

Abordar la seguridad del IoT es complicado. A veces tiene objetivos demasiado generales y muy poco concretos; es parte de infraestructuras de mayor complejidad y tamaño; o maneja datos confidenciales. Asimismo, otro problema es la potencia informática que se encuentra inherentemente disponible en dispositivos interconectados, a la que puede darse un uso indebido.

[1] N. del T.: También conocido como Internet de las cosas.

* Alumnos en prácticas de la Universidad Pontificia de Comillas

En conjunto, el reto en el entorno y dispositivos del IoT consistirá en mantener un equilibrio entre el bajo coste y la seguridad de mercado. Si este equilibrio desaparece, hay riesgo de un fracaso de mercado de las aplicaciones IoT.

Retos de seguridad del IoT

El IoT será una oportunidad para las actividades cibercriminales de monetización. Será el centro de la seguridad nacional y el espionaje, tanto desde el punto de vista estatal como del de las empresas privadas. Además, los datos sobre el comportamiento de los usuarios se utilizarán en marketing.

Esta es una lista indicativa de las áreas donde se puede dar el uso indebido del IoT y su correspondiente amenaza:

- Los datos y funciones disponibles de aplicaciones IoT se pueden utilizar indebidamente en ciber amenazas como *phishing*[2], *ransomware*[3], ciber espionaje, filtración de datos, robo de identidad, etc.
- Dispositivos con poca seguridad que pueden hackearse y utilizarse indebidamente.
- Interfaces con poca seguridad pueden usarse indebidamente para penetrar en sus sistemas. Además, la ausencia de funcionalidad y fiabilidad de algunos productos, por ejemplo, respecto a las actualizaciones, impide la eliminación de vulnerabilidades.
- Las funciones, procesos y datos disponibles se pueden utilizar indebidamente con el objetivo de obtener beneficios ilícitos.
- Las empresas pueden estar interesadas en métodos para espiar a sus competidores.
- Grupos de activistas, terroristas o cibercriminales pueden utilizar los electrodomésticos de viviendas particulares o empresas para actividades ilegales.

Debido a la naturaleza de las aplicaciones IoT, los requisitos de confidencialidad, integridad y disponibilidad son altos. Por ello, para su protección, es necesario centrarse en el desarrollo de una arquitectura de seguridad a un más amplio nivel.

Plazo estimado de puesta en funcionamiento: de 2 a 5 años:

- La plataforma IoT se encuentra en sus primeras fases de desarrollo.
- El 5G y la virtualización permitirán interacciones entre dispositivos.
- La protección del IoT como un todo será difícil. Es más viable su protección orientada a diferentes sectores o aplicaciones.
- El IoT aumentará la superficie de ataque disponible.
- Los escenarios IoT necesitarán considerar la existencia de los controles de seguridad actuales.
- La protección de datos será necesaria para mantener la privacidad.

[2] N. del T.: Fraude electrónico.
[3] N. del T.: Programa informático malintencionado que tiene por objetivo restringir acceso a partes o archivos del sistema infectado y que suele pedir un rescate a cambio de solucionar el problema.

3.2. Interacción entre el uso de la tecnología y los retos sociales

Los cambios sociales desempeñan un papel importante en la adopción de la tecnología, pues promueven la creación de nuevos productos y su utilización. Los cambios sociales respecto a la digitalización son un gran fenómeno. Es necesario entender dichos cambios para identificar el comportamiento y las prácticas de los usuarios, e identificar posibles futuros escenarios.

La forma en la que se consume la información ha cambiado. Ahora, las generaciones más jóvenes no ven tanto la televisión como antes. La manera en la que los jóvenes se comunican e interactúan es diferente. La utilización de redes sociales ha crecido notablemente, lo que va en contra de algunos derechos humanos, como el derecho a la privacidad, en ciertas ocasiones.

Retos de seguridad consecuencia de los cambios sociales

Los retos de ciberseguridad, consecuencia de los cambios sociales, son importantes. Por ello, es necesario una mejor comprensión de los motivos, prácticas y psicología de los usuarios.

Se ha demostrado que una mejor concienciación sobre seguridad en los usuarios reduciría más del 50% de los incidentes consecuencia de fallos humanos. Esto demuestra la importancia de tales medidas.

Esta es una lista indicativa de las áreas donde la ciberseguridad y el comportamiento de los usuarios pueden extraer conclusiones:

- Debilidades provocadas por patrones de comportamiento.
- Debilidades provocadas por el uso.
- Exposición a amenazas debido a debilidades.
- Escenarios de uso indebido.
- Identificación y evaluación de activos importantes.
- Elaboración de controles de seguridad que pueden administrar personas no-expertas.
- Concienciación y entrenamiento, dependiendo de la edad de los grupos a los que se dirija.
- Equilibrio de las necesidades sociales, métodos educativos y patrones de comportamiento de los usuarios.
- Elaboración de cursos para lograr este equilibrio.

Plazo estimado de puesta en funcionamiento: de 2 a 5 años:

- El comportamiento de los usuarios necesita estudiarse y comprenderse mejor.
- Las prácticas de los usuarios necesitan tener en cuenta la ciberseguridad.
- Con la puesta en marcha de controles de seguridad básicos, se puede conseguir una reducción del riesgo.

3.3. La próxima generación de infraestructura informática

Retos tecnológicos

En distintas áreas informáticas, estamos presenciando la creación de la próxima generación de infraestructuras informáticas. Estas nuevas infraestructuras se caracterizan, ente otras cosas, por la

posibilidad de manejar estos sistemas de manera remota. Esto constituye un gran reto tecnológico, operacional y económico.

Retos de seguridad en la próxima generación de infraestructura informática

La próxima generación de sistemas nos proporcionan una visión más completa y coherente de los operadores y los usuarios. No obstante, existen riesgos, sobre todo teniendo en cuenta que las nuevas infraestructuras son redes de software y 5G.

Estos riesgos pueden estar relacionados con la eventual debilidad de los subsistemas, errores en configuración, incompatibilidad, lagunas de seguridad, etc. Además, el impacto de la materialización de dichos riesgos puede ser importante, pues puede afectar las operaciones de distintos usuarios.

En general, la próxima generación de infraestructura informática conllevará los siguientes retos de seguridad:

- Distintas opciones donde se pueden dar debilidades y/o vulnerabilidades debido a la heterogeneidad de los componentes.
- Abuso eficiente de las debilidades y/o vulnerabilidades debido a numerosas capas lógicas y físicas.
- Oportunidades de monetización a través de numerosos servicios ofrecidos y usuarios.
- Multitud de escenarios de ataque debido a los flujos de trabajo puestos en marcha en estas plataformas.
- Numerosos casos de abuso debido a los puestos administrativos involucrados.
- Implementación ineficiente de medidas de seguridad transversales que produzcan lagunas.
- Demasiadas formas de sobrepasar los controles de seguridad actuales.

Plazo estimado de puesta en funcionamiento: de 5 a 10 años.

Aportes de la próxima generación de infraestructura informática:

- Tradicionalmente, el abuso de la seguridad tiene lugar entre las capas del sistema. La próxima generación de infraestructura informática contará con numerosas capas que incrementarían el número de abusos.
- La próxima generación de infraestructura informática será un objetivo atractivo debido a la gran cantidad de información que se puede filtrar.
- Los defectos de los componentes pueden afectar a la confidencialidad e integridad de los datos.
- Nuevas formas de entender la interacción y los requisitos arquitectónicos de las nuevas infraestructuras virtuales, establecimiento de protección de acuerdo con estos.

3.4. Realidad virtual aumentada / Gamificación[4]

De forma general, las tecnologías de realidad virtual y *gamificación* se utilizan cuando se busca disociar un proceso de su aspecto físico. Esta tecnología permite la simulación de eventos

[4] N. del T.: en inglés: *gamification.*

catastróficos sin realmente experimentarlos. Por ejemplo, es muy habitual cuando alguien quiere obtener habilidades cuya obtención en la vida real sería peligrosa.

De momento, la importancia de la realidad virtual y la *gamificación* para la ciberseguridad es bastante baja. Esto cambiará cuando el mundo físico y el virtual se conecten. Aun así, la realidad virtual y la *gamificación* son de especial relevancia en cuanto a privacidad.

Retos tecnológicos

La realidad virtual aumentada es un área tecnológica que ha mejorado bastante. Dependiendo del sector o ámbito donde se utilice, puede ser bastante intrusiva y/o esencial para actividades humanas, sobre todo cuando se utiliza en sectores como la medicina, el ejército, el espacio o la aviación.

La realidad virtual aumentada se utiliza en la *gamificación* con fines lúdicos. Cuenta con un elevado número de usuarios en distintos ámbitos, por lo que los retos a los que se enfrentan dependen de los comentarios de los usuarios a través de sensores.

Retos de seguridad

Los retos son complejos, interconectados y de distintos ámbitos, debido a que es una tecnología que recoge datos de la experiencia de los usuarios. Dicha información puede ser muy personal y, dependiendo de donde se utilice, puede perjudicar a la vida humana.

La realidad virtual aumentada es un reto para la ciberseguridad en cuanto a:

- Seguridad y privacidad.
- El papel de los requisitos de confidencialidad, integridad y disponibilidad de la información y funciones que dichos sistemas ofrecen.
- Debilidades derivadas del uso o el mantenimiento.
- Escenarios de abuso internos.
- Amenaza de exposición debido a una débil integración de los componentes.

Plazo estimado de puesta en funcionamiento: de 2 (realidad virtual) a 10 años (realidad aumentada).

Aportes de la próxima generación de infraestructura informática:

- Se necesita entender los requisitos de seguridad de esta área tecnológica.
- La realidad virtual aumentada aportará nuevos campos de ataque y debilidades.
- La implicación del uso indebido de la realidad virtual aumentada sigue en estudio.

3.5. Sistemas autónomos[5]

Retos tecnológicos

Los sistemas autónomos están encontrando una implementación gradual, sobre todo actualmente, en el sector de la automoción. Los expertos han encontrado un número de retos relacionados a los ensayos:

- Perfeccionar la complejidad del entorno del sistema autónomo.

[5] N. del T.: ejemplo: vehículos.

- Gestionar los software y hardware complejos.
- Perfeccionar el mantenimiento de todos estos componentes.

Además, otros retos se relacionan con la falta de tolerancia y confianza en las funciones y resiliencia:

- Hay una necesidad de incrementar la tolerancia, evitación y eliminación de fallos.
- Establecimiento de confianza en las funciones del sistema y el funcionamiento de los sistemas autónomos.
- Incluso en casos de fallo, los sistemas autónomos necesitarán estar en posición de que se les pueda ajustar sus características.

Retos de seguridad

Los retos de seguridad en el ámbito de los sistemas autónomos tienen que ver con la resiliencia, confianza e integridad de los sistemas. Vale la pena mencionar que los sistemas autónomos son la interacción entre la seguridad y la protección. Por ello, a la hora de elaborar los problemas de seguridad de dichos sistemas, es necesario entender el uso de los controles de seguridad para garantizar protección, pero también el impacto que los fallos de seguridad tienen en la protección.

Más concretamente:

- La resiliencia de los sistemas autónomos es su habilidad de sobrevivir a varios tipos de fallos sin provocar daños personales, la muerte o un gran daño a diferentes activos. Para conseguir esto, es necesario el mantenimiento de distintos mecanismos, sobre todo aquellos de seguridad.
- Uno de los requisitos más importantes de los sistemas autónomos es la confianza, principalmente respecto a los componentes del sistema. Esto es muy relevante, sobre todo, en relación con los vehículos. También es importante resaltar que es necesaria una confianza en las funciones de los sistemas autónomos per se.
- El mantenimiento de la integridad es, asimismo, una necesidad, especialmente porque dichos sistemas pueden afectar a las vidas humanas.
- El desarrollo de modelos de confianza que interconecten sistemas autónomos, como, por ejemplo, dispositivos de intercambio de información o comunicación.

Plazo estimado de puesta en funcionamiento: más de 10 años.

Aportes de los sistemas autónomos:

- Los sistemas autónomos necesitan interactuar con otros componentes en base a modelos de confianza.
- La resiliencia de los sistemas autónomos adquirirá nuevas cualidades, dado su papel potencial en el tráfico y la salud.
- Los sistemas autónomos requerirán nuevos enfoques en temas de mecanismos de seguridad, especialmente en su interacción con dispositivos de menor confianza, como sensores.

3.6. El internet de las Bio-nano Cosas (IoBNT)

Retos tecnológicos

Tras la llegada del IoT, los científicos ven la posibilidad de combinar dispositivos con procesos biológicos y de miniaturización. La implementación del IoBNT como sistemas de computación con biología incorporada, facilitaría mucho determinadas cosas y un buen desarrollo traería consigo, además de grandes beneficios, nuevos retos éticos, sociales, legales económicos y políticos, entre muchos otros.

Para hacer frente a estos retos será necesario trabajar mucho en ello.

Retos de seguridad

El IoBNT traerá consigo la necesidad de resolver muchos temas de seguridad y ciberseguridad: el nivel de protección será lo más alto posible, dada la importancia de los activos. Será absolutamente necesario confiar en las funciones y en la comunicación de todas las partes involucradas en los procesos.

Tiempo estimado para la implantación: más de 10 años.

3.7. IA (Inteligencia artificial) y robótica

Retos tecnológicos

En términos informáticos, la inteligencia artificial son los ordenadores, sistemas, servicios y aplicaciones que perciben lo que hay a su alrededor y utilizan estos datos, potencialmente incompletos del medio ambiente, para maximizar la posibilidad de éxito en las tareas. Todas las técnicas y métodos vienen de algoritmos. Algunos ejemplos son: coches automáticos, drones, diagnósticos médicos, asistentes personales…

- El panorama que existe es bastante complejo.
- Los costes: en comparación con los costes de los humanos o componentes que serán reemplazados, los costes de la IA son muy significativos.
- Omnipresencia: las personas deben confiar en la efectividad de la IA, es importante que en la fase de adopción se tengan más en cuenta los beneficios a largo plazo que los inconvenientes a corto plazo.
- Gran cadena de suministros: en cada solución de AI, hay detrás un gran número de partes interesadas.
- Integridad algorítmica: la IA es una caja negra que generalmente no da lugar a verificaciones. El problema es mayor si tenemos en cuenta que los algoritmos están totalmente ligados a los datos que fueron utilizados para entrenar esta inteligencia y ponerla a prueba, por lo que, si los datos fueran modificados, también podrían verse modificados dichos algoritmos.

Retos en seguridad

Todas las tecnologías que facilitan la inteligencia y la toma de decisiones automatizada son necesarias para el desarrollo del IoT y la industria 4.0. Debido a la importancia de esto, la seguridad

debe ser máxima. ENISA ha identificado una serie de riesgos cibernéticos de seguridad. Destacan los siguientes aspectos:

- Se necesita más confianza en la IA, Los sistemas de robótica deben interactuar con los demás componentes que estén basados en sistemas seguros.
- La superficie en la que se puede atacar es muy grande.
- El panorama actual es bastante complejo: las amenazas a la robótica y a la IA son grandes y tienen un impacto directo en la salud, la seguridad y la privacidad de los ciudadanos.
- Falta de certeza.
- Transparencia: la transparencia en la toma de decisiones implica que la IA pueda justificar sus acciones y el proceso lógico de la toma de decisiones.
- Despliegue generalizado de la AI.
- Todas las partes interesadas no tienen los mismos puntos de vista respecto a los problemas de seguridad, por ello es mucho más complicado hacerlos frente en el proceso de integración.
- Dada la cantidad de datos personales y, por tanto, de la privacidad de los ciudadanos con la que trabaja la AI, existen muchos riesgos para las personas, las organizaciones y las empresas en las que repercute todo ello. Garantizar una correcta recolección de datos, un buen procesamiento de los mismos, la regulación son algunos de los principales retos que existen respecto a este tema.

4. Consolidación de las ideas recopiladas: Emergencia de sectores relacionados con la seguridad

4.1. Certificación

Conclusiones de la certificación:

- Los planes de certificación existentes no son los apropiados para los aparatos ligeros en comparación a los que se encuentran en el Internet de las cosas.
- Harán falta nuevos enfoques para el desarrollo de métodos alternativos para comprobar las funciones de ciberseguridad.
- ENISA apoya a la Comisión a la hora de consolidar los enfoques existentes.

4.2. Un terreno virtual, muchos actores: civiles, fuerzas policiales y sociedades militares en el ciberespacio

Conclusiones de la coordinación de acciones:

- Al igual que en otros ámbitos de la vida, como crisis y eventos catastróficos, hará falta coordinar las actividades de varios actores, incluyendo las fuerzas de defensa, policiales, y de rescate.
- La cooperación en cuanto a las cibercrisis es un área importante que debería abordarse.

4.3. Fiabilidad

Conclusiones de la fiabilidad:

- Se desarrollarán nuevos modelos de fiabilidad para satisfacer las necesidades interacciones de los componentes ad-hoc.
- Será imprescindible que las infraestructuras de fiabilidad existentes y novedosas cumplan los requisitos de interoperabilidad y rendimiento necesarios.
- Los modelos de fiabilidad serán importantes para la aceptación de las ofertas de servicios y por lo tanto se podrán incorporar sin ningún problema a la cartera de servicios.

4.4. Cobertura de seguridad del ciclo de vida completo

Conclusiones del ciclo de vida de seguridad:

- La inclusión de la seguridad en el desarrollo del ciclo de vida de los productos es una precondición necesaria para el mejoramiento de la seguridad de la infraestructura.
- La inclusión de la seguridad en el desarrollo del ciclo de vida de los productos es la única manera de incorporar los componentes de la tecnología de la información en los planes de gestión de seguridad integral.

4.5. Asuntos emergentes en el área de la codificación/encriptación

Conclusiones de la codificación/encriptación:

- La encriptación a nivel nacional-estatal se ve como un obstáculo ante la vigilancia lícita. Las naciones-estado invertirán en recursos para sobrepasar dicho obstáculo.
- Los proveedores tienen interés en que haya una protección de datos débil que les permita tener mejor presencia internacional con los estándares de seguridad uniformes que facilitarán los esfuerzos de desarrollo/integración del producto.
- La UE debería aprovechar los avances existentes de los servicios y tecnología de encriptación en esta área para implementar liderazgo en el mercado global.
- Se están desarrollando nuevos modelos de uso para las funciones de encriptación. Esto incrementará la necesidad de incluir funciones de encriptación en los productos de software y hardware.

4.6. Identificación

Conclusiones de la identificación:

- Se debe investigar la interrelación entre la identificación y la fiabilidad.
- Las nociones de anonimato, identidad y no repudio se deben incorporar a las infraestructuras de tecnología de la información, respetando los requisitos de privacidad y seguridad.

- La noción de identidad se debe localizar en una base más amplia, mientras múltiples datos de usuarios permitan que la definición de los perfiles exactos conecte a usuarios individuales en internet.

4.7. Inteligencia Artificial (IA) y el Aprendizaje Automático (AA) como herramientas de ciberseguridad

Conclusiones de la IA y del AA:

- La IA y el AA son herramientas importantes en el ámbito de la ciberseguridad. Se pueden utilizar para descubrir contexto en ámbito de la Inteligencia sobre Amenazas Cibernéticas (IAC).
- Otro ámbito prometedor es el uso de la IA y del AA en la identificación de patrones de ataque (ej. Basados en TI) y en la facilitación de la supervisión de gestión o aplicación de políticas de seguridad.

5. Lista de temas Universidad Bundeswehr

Durante la sesión de *brainstorming* del 3 de marzo de 2017, se ha llegado a los siguientes temas de interés mutuo:

→ La simulación de situaciones de riesgo con amenazas y materialización de riesgos es importante.
→ El riesgo y percepción de riesgos como tema para la organización propia. La percepción de riesgos es un punto que necesita ser detallado.
→ La predicción de la actividad botnet en la base del comportamiento del sistema como el reconocimiento de patrones, etc, es un elemento importante para la investigación, las simulaciones y también para el ejercicio.
→ El análisis de amenazas y los panoramas de amenazas, la evolución de las amenazas, etc, se considera como un área de innovación.
→ Con un multiproyecto fruto del esfuerzo y coordinación, la universidad está inmersa en un proyecto que trata la seguridad tecnológica. Ocurre en Alemania pero cualquier miembro de ENISA sería bienvenido.
→ La compartición de datos es una actividad que se necesita para las intervenciones militares en términos de riqueza. Este tema es muy relevante para emergencias cibernéticas.
→ Planear los operativos de seguridad. Eficiencia, temas de medios sociales, evaluaciones de los parámetros ambientales, etc.
→ ENISA considerará la llamada del EUROSTARS para evaluar la posibilidad de encontrar colaboradores.
→ ENISA establecerá contactos para futuras interacciones en los áreas de:

- CIIP (Programa de infraestructura global e integrada).
- Simulaciones.
- E-health (web e-Salud en España).
- Ejercicios cibernéticos y coordinación en emergencias.
- Trabajos en la red (software).

→ En la base de estas interacciones, tendrá lugar el desarrollo de un plan anual que se entregará específicamente cada tres meses. Este plan está sujeto a revisiones basadas en los programas hechos.

7. Grupo ENISA: puntos clave para los futuros programas de trabajo

Tras cuatro años de interacción, se han concretado los temas que se trabajarán en el futuro.

Entre los más importantes están los siguientes:

1. Implementación de la nueva estrategia de seguridad.
2. Política de ciberseguridad para Europa.
3. Guía para el GDPR (Reglamento General de Protección de Datos) y para el NIS (Sistema de Información de Red) para la industria europea.
4. Poner en vigor el nuevo mandato de ENISA.
5. Centrarse en la sinergia de la implementación de prácticas en Europa por temas de seguridad y construcción comunitaria.
6. Hacer hincapié en la educación, prestando especial atención a la evolución de NIS.
7. Proporcionar soluciones flexibles a los problemas del NIS y hacer que Europa sea más fuerte en términos de seguridad de las plataformas.
8. Buscar nuevas tecnologías y nuevo posicionamiento de tendencias.
9. Desarrollar una política industrial para Europa a fin de mejorar la seguridad cibernética. Esta política debe estar basada en la aceptación de soluciones, innovación y el respeto a la privacidad y a la competición justa.
10. Construcción comunitaria alrededor de un sistema tecnológico seguro e innovador, incluyendo criptografía y comunicación segura.
11. Examinar el impacto económico del NIS.
12. Coordinación entre los diferentes sectores.
13. Recomendaciones para la política común.
14. Flujo de datos en el IoT: garantía de seguridad para los usuarios.
15. Privacidad en el manejo de datos de identidad en el contexto de elDAS.
16. Mejorar las reacciones a los ciberataques.
17. Industria 4.0. La digitalización de la industria trae nuevos retos en cuanto a la tecnología. Debemos hacer que el nivel de seguridad tecnológica en la industria crezca.
18. ENISA debe definir el itinerario de una buena estrategia para el NIS.
19. Influenciar y educar con la ayuda del PSG (colegio de tecnología).
20. Armonización de las prácticas del NIS.
21. Llevar las estrategias nacionales al IoT y al CIIP.
22. Llegar a las nuevas áreas del NIS.
23. Hacer que aumente la actividad de los ciberejercicios.
24. Hacer que se cree un grado oficial de estudios de ingeniería de ciberseguridad.
25. Soberanía de datos y digital a nivel europeo.

26. La visualización de las funciones en la red ayuda a los proveedores a ser más ágiles y a reducir sus costes. Aun así su nueva composición, sus operaciones y su gran apertura hacen que se creen nuevos retos para la seguridad.
27. 5G. Como puede observarse en el 3G hoy en día, las redes 5G requerirán una seguridad compleja. Con una estandarización en una etapa temprana las soluciones en seguridad que se proporcionen ante las amenazas tendrán que construirse en la red desde el principio. Esto hará que los suscriptores, los aparatos, las comunicaciones y la red misma estén protegidos.