TRABAJO ARTÍCULO CIBERDEFENSA

PRESENTADO POR:

MY. EJC. GUSTAVO ADOLFO CAÑON ROMERO.

MY. EJC. CRISTIAN DAVID RENGIFO DIAZ

MY. EJC. EDISON FERNANDO JIMENEZ ROSERO.

MY. EJC. RUBEN DARIO GUARNIZO TORRES.

PRESENTADO AL SEÑOR:

HAIDER OSPINA NAVAS MsC.

ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO”

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

HABILIDADES PRACTICAS EN EL CIBERESPACIO

BOGOTÁ D.C. 08 DE AGOSTO DE 2024

DESAFÍOS Y TENDENCIAS EN LA IDENTIDAD DIGITAL PARA LA SEGURIDAD DE LAS INFRAESTRUCTURAS CRÍTICAS

Introducción

La identidad digital se ha convertido en un componente esencial de la vida moderna, especialmente en el ámbito de la ciberseguridad. A medida que las infraestructuras críticas, como redes eléctricas, sistemas de transporte y servicios de salud, se vuelven cada vez más dependientes de tecnologías digitales, la gestión de la identidad digital se vuelve crucial para garantizar la seguridad y la integridad de estos sistemas. Este artículo examina los desafíos y tendencias actuales en la gestión de la identidad digital, con un enfoque particular en su relevancia para la seguridad de las infraestructuras críticas.

Definición de Identidad Digital

La identidad digital se refiere a la representación en línea de una persona o entidad, que incluye información personal, perfiles en redes sociales, y datos de transacciones. En el contexto de las infraestructuras críticas, la identidad digital es fundamental para garantizar que solo las personas autorizadas tengan acceso a sistemas sensibles. La identidad digital no solo abarca datos personales, sino también credenciales de acceso, comportamientos en línea y la reputación digital de un individuo o entidad (Truora, n.d.).

Componentes de la Identidad Digital

1. **Datos Personales**: Información como nombre, dirección, número de teléfono y correo electrónico.
2. **Credenciales de Acceso**: Contraseñas, tokens de seguridad y métodos de autenticación multifactor.
3. **Perfiles en Redes Sociales**: Información que refleja la actividad y la interacción de un individuo en plataformas sociales.
4. **Historial de Transacciones**: Registros de compras, interacciones y comunicaciones en línea.

Importancia de la Identidad Digital en Infraestructuras Críticas

La gestión adecuada de la identidad digital es crucial tanto para individuos como para organizaciones que operan infraestructuras críticas. La seguridad de estos sistemas depende de la autenticación y autorización efectivas de los usuarios. Un acceso no autorizado puede resultar en interrupciones del servicio, pérdida de datos y daños a la reputación de la organización. Además, la identidad digital es fundamental para la implementación de políticas de seguridad y cumplimiento normativo.

Ejemplos de Infraestructuras Críticas

- **Redes Eléctricas**: La protección de los sistemas de control que gestionan la distribución de energía es esencial para evitar apagones y ataques cibernéticos.
- **Sistemas de Transporte**: La seguridad en el acceso a sistemas de control de tráfico y transporte público es vital para la seguridad pública.
- **Servicios de Salud**: La protección de los datos de pacientes y el acceso a sistemas médicos es crucial para garantizar la continuidad de la atención.

Desafíos en la Identidad Digital

1. Verificación de Identidad

La verificación de identidad es uno de los mayores desafíos en la seguridad de las infraestructuras críticas. Con el aumento de ataques cibernéticos, garantizar que una persona sea quien dice ser es esencial para proteger sistemas críticos. La autenticación tradicional, basada en contraseñas, es cada vez más vulnerable a ataques de phishing y técnicas de ingeniería social. Por lo tanto, es necesario implementar métodos de autenticación más robustos, como la autenticación multifactor (Jumio, 2023).

2. Confianza Digital

La confianza de los usuarios en la seguridad de sus datos es crucial. Las violaciones de datos y el fraude en línea erosionan esta confianza, lo que puede tener consecuencias graves para la seguridad de las infraestructuras críticas. Las organizaciones deben establecer medidas de seguridad transparentes y

efectivas para garantizar a los usuarios que sus datos están protegidos. Esto incluye la implementación de políticas de privacidad claras y la comunicación proactiva sobre las medidas de seguridad adoptadas (KeepCoding, 2024).

3. Regulación y Cumplimiento

La falta de un marco regulatorio claro puede dificultar la implementación de soluciones de identidad digital seguras. Las organizaciones deben cumplir con regulaciones que protegen la información personal y garantizan la seguridad de las transacciones. La normativa, como el Reglamento General de Protección de Datos (GDPR) en Europa, establece requisitos estrictos sobre cómo se deben gestionar y proteger los datos personales. Las organizaciones que operan infraestructuras críticas deben asegurarse de que sus prácticas de gestión de identidad digital cumplan con estas regulaciones (Mitek Systems, 2024).

4. Inteligencia Artificial y Sesgos Algorítmicos

La inteligencia artificial se utiliza para mejorar la verificación de identidad, pero también plantea desafíos en términos de privacidad y discriminación algorítmica. Los sesgos en los algoritmos pueden afectar la eficacia de las soluciones de verificación. Por ejemplo, los sistemas de reconocimiento facial han sido criticados por su inexactitud en la identificación de personas de diferentes razas y géneros. Esto puede llevar a decisiones erróneas en la verificación de identidad y, en última instancia, a la exclusión de ciertos grupos de individuos (Techopedia, 2024).

5. Amenazas Cibernéticas

Las amenazas cibernéticas son una preocupación constante para la seguridad de las infraestructuras críticas. Los ataques de ransomware, el phishing y las violaciones de datos son solo algunas de las tácticas utilizadas por los ciberdelincuentes para comprometer la identidad digital de los usuarios. La creciente sofisticación de estos ataques requiere que las organizaciones implementen soluciones de ciberseguridad avanzadas y actualizadas para proteger sus sistemas (Prigge, 2022).

Tendencias en la Identidad Digital

1. Autenticación Multifactor

Se espera un aumento en el uso de sistemas de autenticación que combinan varios métodos, como contraseñas y biometría, para mejorar la seguridad en las infraestructuras críticas. La autenticación multifactor (MFA) añade una capa adicional de seguridad al requerir que los usuarios proporcionen dos o más formas de identificación antes de acceder a un sistema. Esto puede incluir algo que saben (una contraseña), algo que tienen (un token o dispositivo) y algo que son (biometría) (Jumio, 2023).

2. Carteras de Identidad Digital

La adopción de carteras digitales que permiten almacenar y compartir datos identificativos de manera segura está en aumento. Estas soluciones facilitan la gestión de la identidad sin comprometer la privacidad. Las carteras digitales permiten a los usuarios controlar qué información comparten y con quién, lo que es especialmente importante en el contexto de las infraestructuras críticas, donde la protección de datos sensibles es fundamental (Truora, n.d.).

3. Identidad Reutilizable

La creación de identidades digitales reutilizables permitirá a los usuarios utilizar sus datos personales en múltiples plataformas sin crear identidades separadas. Esto simplificará la experiencia del usuario y reducirá el fraude. Las identidades reutilizables también pueden facilitar la interoperabilidad entre diferentes sistemas y servicios, lo que es crucial para la seguridad de las infraestructuras críticas (Mitek Systems, 2024).

4. Regulaciones Gubernamentales

La implementación de regulaciones sobre la identidad digital, como las propuestas en la Unión Europea, mejorará la emisión y aceptación de identidades digitales. Estas regulaciones son fundamentales para garantizar la seguridad y la privacidad de los datos en un entorno digital en constante evolución. Las organizaciones que operan infraestructuras críticas deben estar preparadas para adaptarse a estos cambios regulatorios y asegurarse de que sus prácticas de gestión de identidad digital cumplan con las nuevas normativas (Prigge, 2022).

5. Educación y Concientización

La educación y concientización sobre la identidad digital son tendencias emergentes que pueden ayudar a mitigar los riesgos asociados con la gestión de la identidad. Las organizaciones deben invertir en programas de capacitación para sus empleados, enfocándose en la importancia de la seguridad de la identidad digital y las mejores prácticas para proteger la información personal. La concientización sobre las amenazas cibernéticas y las técnicas de ingeniería social es fundamental para fortalecer la seguridad en las infraestructuras críticas (KeepCoding, 2024).

Estrategias para Mejorar la Gestión de la Identidad Digital

1. Implementación de Políticas de Seguridad

Las organizaciones deben desarrollar e implementar políticas de seguridad claras que aborden la gestión de la identidad digital. Estas políticas deben incluir directrices sobre la creación y gestión de contraseñas, el uso de autenticación multifactor y la protección de datos personales. La capacitación regular de los empleados sobre estas políticas es esencial para garantizar su cumplimiento.

2. Uso de Tecnologías Avanzadas

La adopción de tecnologías avanzadas, como la inteligencia artificial y el aprendizaje automático, puede mejorar la verificación de identidad y la detección de fraudes. Estas tecnologías pueden analizar patrones de comportamiento y detectar actividades sospechosas en tiempo real, lo que permite a las organizaciones responder rápidamente a posibles amenazas.

3. Auditorías y Evaluaciones de Seguridad

Las organizaciones deben realizar auditorías y evaluaciones de seguridad de manera regular para identificar vulnerabilidades en sus sistemas de gestión de identidad digital. Estas evaluaciones pueden ayudar a las organizaciones a implementar mejoras y adaptarse a las amenazas emergentes.

4. Colaboración y Compartición de Información

La colaboración entre organizaciones y la compartición de información sobre amenazas cibernéticas pueden mejorar la seguridad de las

infraestructuras críticas. Las alianzas estratégicas pueden facilitar el intercambio de mejores prácticas y la implementación de soluciones de seguridad más efectivas.

5. Enfoque en la Privacidad del Usuario

Las organizaciones deben priorizar la privacidad del usuario en sus prácticas de gestión de identidad digital. Esto incluye la implementación de políticas de privacidad claras y la transparencia en el uso de datos personales. Al fomentar la confianza entre los usuarios, las organizaciones pueden mejorar la seguridad de sus sistemas.

Aplicabilidad De La Identidad Digital En Conflictos Globales

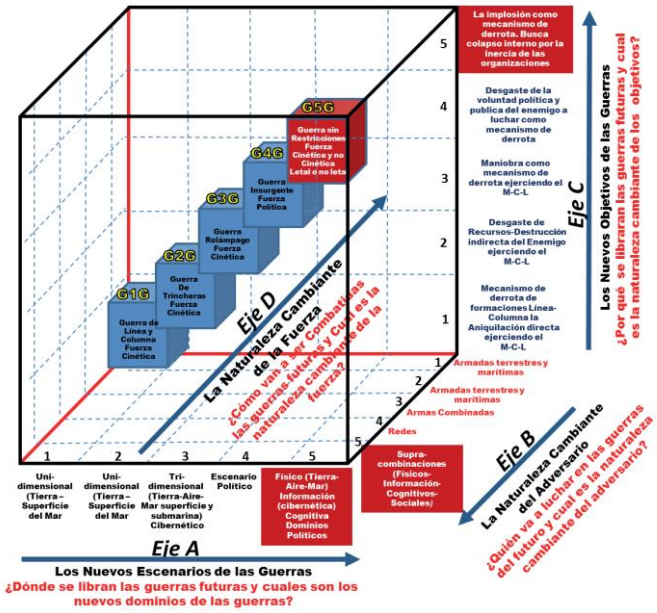
La Guerra como la conocemos clásicamente ha tenido una evolución la cual a estado desarrollándose durante siglos, he incluso tienen mucho que ver con las revoluciones industriales o como el ser humano integra la tecnología a sus propias capacidades. El modelo de guerras generacionales propuesto por Lind *et al* (1984; 2004), Hammes (2005; 2006; 2007), Liang & Xiangsui (2002), logra establecer que existen elementos indispensables para la idealización de una “tipología generacional de la guerra” (Álvarez, 2007). Estos elementos esenciales son: la naturaleza cambiante de la fuerza, los nuevos dominios del conflicto; la naturaleza cambiante de los adversarios; y la naturaleza cambiante de los objetivos (p. 189).

Según Liang & Xiangsui (2002), hasta la fecha, los elementos básicos de los campos de batalla en la guerra (dominios), soldados (adversarios), propósito (objetivos) y armas (fuerza), nunca han sido cuestionados (Álvarez, 2017, p. 189). No obstante, este comportamiento a cambiado, principalmente por el hecho de que existen diversos factores que ahora influyen en las conexiones complejas de la forma de hacer la guerra. Por ejemplo, los impactos políticos, sociales, económicos, tecnológicos de la era de la información y la globalización (Álvarez, 2017).

En este contexto, Reed (2008), a considerado establecer que existen cuatro elementos esenciales de la guerra y su evolución sobre ejes separados los cuales se analizan mediante un modelo tridimensional. La tipología

generación de la guerra en la Grafica N° 1 cumple con cada uno de estos elementos.

Grafica 1. Tipología Generacional de la Guerra.



Fuente: Adaptada de Reed, D.J. (2008).

En esta grafica eventualmente ya hace falta una nueva generación. La cual corresponde a las Guerras de Sexta Generación (G6G). El presenta ensayo tiene en cuenta teóricamente las dos ultimas generaciones. Las Gerras de Quinta y Sexta generación, que presentan conceptos avanzados en la evaluación de la guerra moderna, caracterizados por el uso de tecnologías avanzadas y tácticas no convencionales. En primer lugar, la Guerras de Quinta Generación (G5G), se centran en la manipulación de la percepción y la influencia sobre las poblaciones y gobiernos. Se caracteriza por uso de tecnologías de información avanzadas, ciberoperaciones, y tácticas psicológicas para desestabilizar a los adversarios sin recurrir a un conflicto militar directo.

Por otra parte, la Guerra de Sexta Generación (6GW) es un concepto aún en desarrollo que se prevé como una evolución de la 5GW. Se caracteriza por la incorporación de tecnologías emergentes como la inteligencia artificial, la robótica avanzada, armas autónomas, y la biotecnología para crear un campo de batalla dominado por sistemas autónomos y una integración profunda de capacidades cibernéticas y espaciales.

En ese orden de ideas, en este ensayo se pretenden explorar las amenazas cibernéticas que pueden ser empleadas como herramientas de guerra en un contexto moderno teniendo en cuenta la infinita complejidad que pueden desarrollarse en torno a estos nuevos retos y desafíos de la seguridad y defensa contemporánea.

Explorando las amenazas.

Las amenazas cibernéticas en la Guerra de Quinta Generación (5GW) representan una evolución significativa en la forma en que se llevan a cabo los conflictos, donde el objetivo principal es influir y manipular percepciones más que alcanzar una victoria militar directa (Schneider, 1995). En este contexto, las operaciones de información y la ciberseguridad se entrelazan para crear un campo de batalla donde la mente y la confianza pública son los objetivos primarios (Arreola, 2016). Una de las amenazas más prominentes en este ámbito es el phishing y el spear phishing. Estas técnicas de ingeniería social se utilizan para engañar a individuos y organizaciones, obteniendo acceso a información sensible y comprometiendo sistemas internos (Rueda, 2020). Los atacantes se valen de correos electrónicos y mensajes que parecen legítimos para inducir a sus víctimas a revelar contraseñas, datos financieros y otra información crítica.

El malware, en sus diversas formas, también juega un papel crucial. Los programas maliciosos pueden infiltrarse en sistemas para robar datos, espiar a usuarios o causar daños directos (García, s.f). Entre estos, el ransomware se ha destacado como una amenaza particularmente disruptiva, ya que cifra los archivos de los usuarios y demanda un rescate para su liberación, afectando tanto a individuos como a grandes organizaciones y gobiernos (Paniagua, 2022). Los ataques de denegación de servicio distribuida (DDoS) son otra herramienta común en la 5GW, donde se inunda un sistema con tráfico excesivo, causando interrupciones significativas en los servicios y dificultando la operatividad de infraestructuras críticas (Chavez, 2011).

Además, los ataques man-in-the-middle (MitM) permiten a los ciberatacantes interceptar y modificar las comunicaciones entre dos partes sin su conocimiento, robando información o insertando datos falsos. Los exploits de día cero, que aprovechan vulnerabilidades no descubiertas en software y

hardware, proporcionan a los atacantes acceso sin restricciones a sistemas vulnerables antes de que los desarrolladores puedan implementar parches de seguridad (Caro, 2013).

Un aspecto central de la 5GW es el ataque a infraestructuras críticas. Los ciberataques dirigidos a sectores esenciales como energía, agua, transporte y telecomunicaciones pueden desestabilizar sociedades enteras. Los sistemas SCADA (Supervisory Control and Data Acquisition), que supervisan y controlan procesos industriales, son objetivos comunes, ya que su compromiso puede resultar en interrupciones devastadoras.

La guerra psicológica y la desinformación son elementos clave en la 5GW (Nuño, 2020). El uso de propaganda y desinformación a través de redes sociales y otros canales de comunicación busca influir en la opinión pública y socavar la confianza en instituciones gubernamentales y procesos democráticos. Campañas bien orquestadas pueden sembrar discordia, polarizar sociedades y manipular elecciones. La capacidad de manipular narrativas y difundir noticias falsas permite a los actores hostiles influir en decisiones políticas y sociales sin necesidad de un enfrentamiento militar directo.

Las amenazas cibernéticas en la Guerra de Sexta Generación (G6G) representan una transformación aún más avanzada y compleja del conflicto moderno, donde las tecnologías emergentes como la inteligencia artificial, la robótica avanzada, y la biotecnología se integran profundamente en las estrategias de guerra (Barrero & Álvarez, 2022). En este nuevo paradigma, las operaciones cibernéticas no solo buscan comprometer sistemas de información, sino también controlar y manipular sistemas autónomos y dispositivos interconectados. Los ataques a sistemas autónomos son una amenaza significativa en la G6G. Los robots, drones y otros sistemas autónomos utilizados en el campo de batalla pueden ser comprometidos para deshabilitarlos o incluso reprogramarlos para atacar a sus operadores originales. La capacidad de infiltrarse en estos sistemas y tomar control de ellos puede dar a los atacantes una ventaja táctica considerable.

La inteligencia artificial (IA) se convierte en una herramienta doblemente peligrosa en la G6G (El País, 2023). Los ciberataques basados en IA pueden

identificar y explotar vulnerabilidades en sistemas y redes de manera mucho más efectiva y rápida que las técnicas tradicionales (Skyone, 2024). Los algoritmos de aprendizaje automático pueden analizar grandes volúmenes de datos para encontrar puntos débiles y desarrollar ataques personalizados, incrementando la eficiencia y letalidad de los ciberataques. La IA también puede ser utilizada para crear deepfakes (Visus, 2021), que son videos o audios falsos que parecen extremadamente reales. Estos pueden ser utilizados para difamar a individuos, influir en la opinión pública y sembrar confusión y desconfianza.

El Ciberespionaje avanzado sigue siendo una amenaza crítica en la G6G, pero con un nivel de sofisticación mucho mayor (Red Seguridad, 2023). Las técnicas de Ciberespionaje ahora integran la inteligencia artificial para automatizar la recolección de datos y evadir detección. Los atacantes pueden infiltrarse en redes para robar información clasificada o sensible y utilizarla para obtener ventajas estratégicas o económicas. Los ataques a la cadena de suministro también se vuelven más prevalentes. Comprometer software o hardware en cualquier punto de su ciclo de vida permite a los atacantes insertar puertas traseras o malware que pueden ser activados cuando el producto final es implementado. Esto es particularmente peligroso en un entorno donde los dispositivos están cada vez más interconectados.

La guerra cibernética espacial emerge como un nuevo frente en la G6G. Los satélites y sistemas espaciales son esenciales para las comunicaciones, navegación y recolección de inteligencia (Guedes, 2023). Comprometer estos sistemas puede resultar en interrupciones significativas y desventajas estratégicas. Además, la biociberseguridad (García, 2021) se convierte en un área de creciente preocupación. La manipulación de datos genéticos y los ataques a dispositivos médicos conectados son ejemplos de cómo las amenazas cibernéticas pueden afectar directamente la salud y la seguridad de las personas. Los ataques a la Internet de las Cosas (IoT) también representan un riesgo considerable, ya que comprometer dispositivos IoT puede crear botnets masivas, espiar a los usuarios y causar daños físicos a través de sistemas conectados como vehículos autónomos y hogares inteligentes.

Conclusiones.

La identidad digital es un componente esencial para la seguridad de las infraestructuras críticas. A medida que las amenazas cibernéticas evolucionan, es fundamental que las organizaciones adopten medidas proactivas para gestionar la identidad digital y enfrentar los desafíos emergentes. La implementación de tecnologías avanzadas, el cumplimiento de regulaciones y la educación de los usuarios serán clave para proteger la integridad de los sistemas críticos. La gestión efectiva de la identidad digital no solo protege a las organizaciones, sino que también garantiza la seguridad y la confianza de los usuarios en un entorno digital cada vez más complejo.

Las amenazas cibernéticas en la Guerra de Quinta Generación se centran en la manipulación de información y la desestabilización de infraestructuras críticas a través de técnicas avanzadas de ciberseguridad. Estas tácticas no solo buscan comprometer sistemas y redes, sino también influir en la percepción pública y debilitar la cohesión social y gubernamental, demostrando que en la 5GW, la batalla se libra tanto en el ciberespacio como en las mentes de las personas.

Por otra parte, las amenazas cibernéticas en la Guerra de Sexta Generación son increíblemente diversas y sofisticadas, aprovechando las tecnologías emergentes para crear un campo de batalla dominado por sistemas autónomos y capacidades cibernéticas avanzadas. La capacidad de integrar inteligencia artificial, biotecnología y ataques a sistemas espaciales y de la cadena de suministro subraya la necesidad de estrategias de defensa avanzadas y resilientes para proteger las infraestructuras críticas y las sociedades modernas en este nuevo y complejo entorno de guerra.

De manera que, las instituciones de seguridad y defensa deben prepararse efectivamente en para el desarrollo de capacidades que permitan enfrentar estas amenazas y de esta manera enfrentar estos riesgos y amenazas en el presente.

Referencia.

Jumio. (2023). Identidad Digital 2023, ¿cuáles son las tendencias y principales desafíos? Recuperado de https://www.prensariohub.com/identidad-digital-2023-cuales-son-las-tendencias-y-principales-desafios/

KeepCoding. (2024). Los principales desafíos de la identidad digital. Recuperado de https://keepcoding.io/blog/desafios-de-la-identidad-digital/

Mitek Systems. (2024). Las tendencias en identidad digital para 2024. Recuperado de https://www.miteksystems.com/es/blog/tendencias-identidad-digital-2024

Prigge, R. (2022). Encuesta de Identidad Digital Global 2022. Jumio.

Techopedia. (2024). Las 5 principales innovaciones de tendencias en verificación digital. Recuperado de https://www.techopedia.com/es/5-innovaciones-tendencias-verificacion-digital-2024

Truora. (n.d.). ¿Qué es la identidad digital, su importancia y desafíos? Recuperado de https://blog.truora.com/es/identidad-digital

Álvarez-Calderón, C. E. (Ed.). (2018). Escenarios y desafíos de la seguridad multidimensional en Colombia. Sello Editorial ESDEG. https://doi.org/10.25062/9789585652835

Álvarez-Calderón, C. E., Santafé-García, J. & Urbano-Morales, Ó. (2018). Metamorphosis Bellum: ¿Mutando a guerra de quinta generación? En C. Álvarez (Ed). *Escenarios y desafíos de la seguridad multidimensional en Colombia.* Sello Editorial ESDEG. https://doi.org/10.25062/9789585652835

Barrero-Barrero, D., & Álvarez Calderón, C. E. (2022). Mutación de la guerra y amenazas contemporáneas en el multidominio criminal y terrorista. Revista Científica General José María Córdova, 20(39), 549-570. https://dx.doi.org/10.21830/19006586.1024

Caro, A. (2013). *Man In The Middle Attacks On Ssl/Tls.* [Trabajo fin de máster] Universidad Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/18443/6/acaroalTFM0113memoria.pdf

Chávez, J. (2011). *Simulación y análisis de mecanismos de defensa ante los ataques de denegación de servicios (DoS) en redes de área local convergentes.* Escuela Politécnica Nacional. https://bibdigital.epn.edu.ec/bitstream/15000/4282/1/CD-3905.pdf

El País. (2023, 30 de mayo). *Los principales creadores de la IA alertan sobre el "peligro de extinción" que supone esta tecnología para la humanidad.* El País. https://elpais.com/tecnologia/2023-05-30/los-principales-creadores-de-la-ia-alertan-sobre-el-peligro-de-extincion-que-supone-esta-tecnologia-para-la-humanidad.html

García Lirios, C. (2021). Bioseguridad y ciberseguridad percibidas ante la COVID-19 en México. Estudios en Seguridad y Defensa, 16(31), 137-160. https://doi.org/10.25062/1900-8325.293

García, R. (s.f.). *Seguridad Informática y el Malware.* Universidad Piloto de Colombia. https://openaccess.uoc.edu/bitstream/10609/145831/7/rapasoTFM0622memoria.pdf

Guedes, R. (2023, 10 de mayo). *Guerra Cibernética: Tipos, Armas, Objetivos y Ejemplos de Guerra Tecnológica.* Ciberprisma. https://ciberprisma.org/2023/05/10/guerra-cibernetica-tipos-armas-objetivos-y-ejemplos-de-guerra-tecnologica/#:~:text=La%20guerra%20cibern%C3%A9tica%20es%20una,de%20comunicaci%C3%B3n%20e%20infraestructura%20cr%C3%ADtica.

Hammes, T. (2005). War Evolves into the Fourth Generation, en Contemporary Security Policy, Volume 26, No.2, pp. 189-221

Hammes, T. (2006). The Sling and the Stone: On War in the 21st Century, New York: Zenith Books.

Hammes, T. (2007). Fourth Generation Warfare Evolves Fifth Emerges, en Military Review, May-June, pp. 14-23.

Liang, Q. & Xiangsui, W. (2002). Unrestricted Warfare: China's Master Plan to Destroy America, Panama City: Pan American Publishing Company.

Lind, W. (2004). Understanding Fourth Generation War, en Military Review, September-October, pp. 12-16.

Lind, W.; Nightengale, K.; Schmitt, J.; Sutton, J.; Wilson, G. (1989). The Changing Face of War: Into the Fourth Generation Warfare, en Marine Corps Gazette, Volume 73, No. 10, pp. 22-26.

Nuño-Rodríguez. (2020). *La guerra por la mente pública.* Revista Fuerza Aérea EUA. https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%202%20Issue%201/02-Rodriguez_s.pdf

Paniagua, R. (2022). *Anatomía del ransomware.* [Trabajo de Grado]. Univesitat Oberta de Catalunya – Univesitar autonoma de Barcelona. https://openaccess.uoc.edu/bitstream/10609/145831/7/rapasoTFM0622memoria.pdf

Red Seguridad (2023, 17 de febrero). *¿Qué es el Ciberespionaje y qué papel juega en las relaciones entre estados?* Red Seguridad. https://www.redseguridad.com/actualidad/que-es-el-ciberespionaje-y-que-papel-juega-en-las-relaciones-entre-estados_20230217.html

Reed, D. (2008). Beyond the War on Terror: Into the Fifth Generation of War and Conflict, en Studies in Conflict & Terrorism, Volume 31, No.8, pp. 684-722.

Rueda, J. (2020). *Estudio monográfico: impacto de la técnica de ataque de Phising en Colombia durante los últimos cinco años.* Universidad Nacional Abierta y a Distancia UNAD.

https://repository.unad.edu.co/bitstream/handle/10596/38721/jaruedaq.pdf?sequence=1&isAllowed=y

Schneider, J. (1995). Cybershock: Cybernetic Paralysis as a New Form of Warfare, en Military Theory Readings, pp. 2-9.

Skyone. (2024, 22 de febrero). *AI generativa en ciberseguridad: cómo impulsar la defensa de los datos críticos.* Skyone. https://skyone.solutions/es/blog/ia-generativa-en-ciberseguridad/

Visus, A. (2021). *Que es un Deep fakes, cómo se crean, cuáles fueron los primeros y futuro.* ESIC. https://www.esic.edu/rethink/tecnologia/deep-fakes-que-es-como-se-crean-primeros-y-futuros