

EL INTERNET DE LAS COSAS EN EL CAMPO DE BATALLA

Comandante de Caballería (CGET) Javier Aldea Álvarez de Lara

RESUMEN

En un mundo donde la tecnología redefine constantemente los límites de lo posible, el Internet de las Cosas en el Campo de Batalla (IoBT) emerge como una fuerza transformadora en la esfera militar. Este avance promete revolucionar no solo la eficiencia operativa sino también la toma de decisiones y estrategia en tiempo real.

Adaptando las capacidades avanzadas del Internet de las Cosas (IoT) a los desafíos del ámbito bélico, el IoBT se enfrenta a la tarea de mejorar significativamente los sistemas de mando, control, comunicaciones e inteligencia (C3I). Su implementación es vital para fortalecer la autonomía y soberanía tecnológica en operaciones militares.

Sin embargo, la incorporación de esta tecnología conlleva desafíos notables, siendo la ciberseguridad el más crítico de todos. Este artículo explora cómo el IoBT está configurando el futuro de las operaciones militares, equilibrando oportunidades sin precedentes con riesgos significativos que requieren una gestión meticulosa.

Palabras clave: Ciberseguridad, soberanía tecnológica, eficiencia operativa, toma de decisiones.

THE INTERNET OF THINGS ON THE BATTLEFIELD

ABSTRACT

In a world where technology constantly redefines the boundaries of the possible, the Internet of Things on the Battlefield (IoBT) emerges as a transformative force in the military sphere. This advancement promises to revolutionize not just operational efficiency but also real-time decision-making and strategy.

Adapting the advanced capabilities of the Internet of Things (IoT) to the challenges of the military realm, the IoBT faces the task of significantly enhancing command, control, communications, and intelligence (C3I) systems. Its implementation is vital for strengthening technological autonomy and sovereignty in military operations.

However, the incorporation of this technology brings notable challenges, with cybersecurity being the most critical of all. This article explores how the IoBT is shaping the future of military operations, balancing unprecedented opportunities with significant risks that require meticulous management.

Key words: Cybersecurity, technological sovereignty, operational efficiency, decisión making.

1. INTRODUCCIÓN

Los ejércitos, al igual que todas las instituciones que han perdurado a lo largo de los tiempos, han ido evolucionando con el propósito de adaptarse a los cambios que ocurrían en su entorno. Una de las principales variaciones a las que se han tenido que enfrentar las fuerzas armadas han sido las diferentes revoluciones industriales que han ido sucediéndose a lo largo de historia. Como fruto de esta adaptación, el armamento, los vehículos y el equipo ha evolucionado junto con la doctrina de empleo y la logística necesaria para su sostenimiento.

La máquina de vapor abrió un camino que fue seguido por el acero, la electricidad o la informática (Fig. 1) y que ha desembocado en la actual industria 4.0 dominada por tecnologías que borran las líneas entre las esferas físicas, industriales y biológicas. La robótica, la biotecnología, la inteligencia artificial o el internet de las cosas (IoT) son los avances a los que las fuerzas armadas (FAS) de los distintos países tienen que hacer frente para no verse superados y, por tanto, subordinados por aquellos que lideren el cambio.

Revolución industrial a través del tiempo

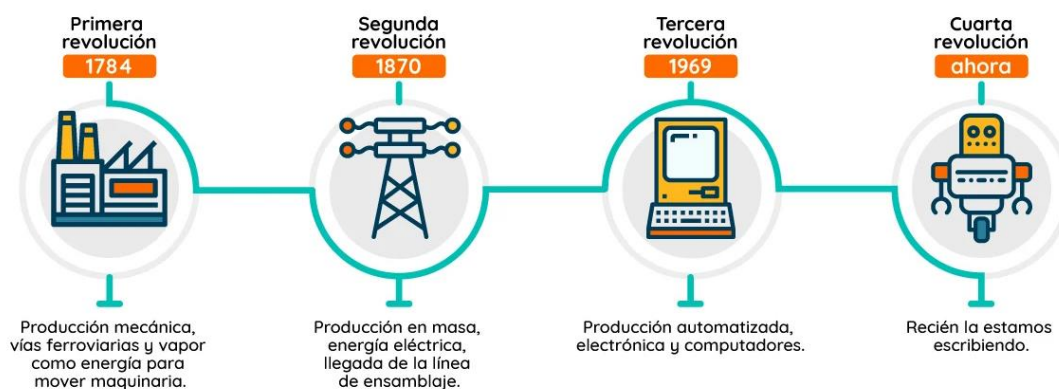


Figura 1. Revolución industrial a través del tiempo. Fuente: nuevaescuelamexicana.sep.gob.mx

Con el avance del IoT, hemos sido testigos de cómo tecnologías originalmente diseñadas para el uso civil están siendo adaptadas y adoptadas por los sectores militares, dando lugar a lo que ahora conocemos como el Internet of Battlefield Things (IoBT) o IoT en el campo de batalla. Este desarrollo transforma la naturaleza de las operaciones militares mediante la integración de tecnologías avanzadas IoT adaptadas a los rigores y requisitos específicos del ámbito militar. Esta convergencia tecnológica promete no solo mejorar la eficiencia operativa

sino también revolucionar la toma de decisiones y la estrategia en tiempo real. Sin embargo, la implementación del IoT trae consigo desafíos significativos y riesgos que deben ser meticulosamente gestionados para garantizar la seguridad y efectividad de estas tecnologías en entornos altamente demandantes y a menudo hostiles.

El camino hacia la integración efectiva del IoT está plagado de complejidades técnicas y éticas. Cada nuevo dispositivo conectado potencialmente aumenta la superficie de ataque, elevando el riesgo de ciberataques que podrían comprometer operaciones críticas. Además, la integridad y la seguridad de los datos recogidos a través de estos dispositivos son de suma importancia, dado que la información errónea o manipulada podría tener consecuencias desastrosas en decisiones tácticas y estratégicas (Suri et al., 2016).

Mirando hacia el futuro, el IoT no solo es una herramienta potencial para mejorar la efectividad militar, sino también un desafío para los estrategas y tecnólogos. La adopción de esta tecnología debe considerar cuidadosamente las implicaciones de seguridad, las necesidades de robustez en entornos adversos, y la ética de la automatización en operaciones militares. A medida que exploramos las capacidades del IoT, también debemos enfrentarnos a preguntas sobre cómo y cuándo se debe utilizar esta tecnología, cómo se puede proteger contra el mal uso y qué lecciones se pueden aprender de otras implementaciones tecnológicas en sectores similares de alta seguridad.

Para hablar del IoT, en primer lugar, debemos definir el IoTⁱ. Esta puede ser una tarea compleja ya que varía según la visión que tiene la persona que lo define sobre qué activos son más relevantes. La forma más completa de describir esta tecnología es como una infraestructura de red que incluye cosas físicas y virtuales con identidades únicas integradas, que utilizan interfaces inteligentes y tienen la capacidad de autoconfiguración. Además, características como la interconexión, la ubicuidad, la capacidad de detección y actuación, y la inteligencia integrada, definen a los sistemas IoT, destacando su potencial para transformar la interacción entre objetos y tecnología en diversos contextos globales y cotidianos (IERC, 2014).

2. EVOLUCIÓN DEL IOT: MÁS ALLÁ DEL SIMPLE AVANCE TECNOLÓGICO

El IoT, que inicialmente conectaba dispositivos en contextos domésticosⁱⁱ y comerciales facilitando diversas funciones automatizadas, ha evolucionado hacia aplicaciones más complejas y críticas. En el ámbito militar, esta evolución se manifiesta como el IoT, donde la integración de tecnologías IoT se adapta para mejorar las capacidades operativas y estratégicas de las fuerzas armadas.

El loBT no solo se centra en la conectividad entre dispositivos, sino que también optimiza la recopilación, análisis y distribución de datos en tiempo real en el campo de batalla. Este proceso no ha sido simplemente una adopción de tecnologías existentes, sino una adaptación compleja que responde a los desafíos únicos del entorno bélico.

El concepto de loBT toma raíz en la década de los 2000, con la expansión del IoT en sectores industriales y de consumo. Sin embargo, su adaptación para aplicaciones militares comenzó a considerarse seriamente a medida que las ventajas de tener dispositivos interconectados se hacían evidentes en contextos civiles, tales como la mejora en la eficiencia operativa y la capacidad de gestión remota. La posibilidad de aplicar estas tecnologías en el campo de batalla prometía una revolución en la manera en que se llevan a cabo las operaciones militares, ofreciendo desde mejoras en la logística hasta en la toma de decisiones estratégicas en tiempo real (Abdelzaher, 2017).

El desarrollo del loBT ha sido impulsado por varias innovaciones tecnológicas clave. En primer lugar, la miniaturización de dispositivos y sensores ha permitido su incorporación en equipamiento militar sin comprometer la movilidad de las tropas o la funcionalidad del equipo. Además, los avances en la comunicación inalámbrica y en la seguridad de la información han sido fundamentales para asegurar que las comunicaciones entre dispositivos loBT sean rápidas y seguras, aspectos fundamentales cuando se trata de operaciones que pueden requerir decisiones en fracciones de segundo bajo condiciones de alto riesgo.



Figura 2. Ejemplo de red loBT *ad hoc* multicapa. Fuente: Fragkou et al. (2022)

Una de las áreas más estudiadas en la evolución del IoT ha sido su adaptación para operar de manera fiable en los duros entornos del campo de batalla. Esto ha incluido no solo mejoras en la robustez física de los dispositivos, sino también en su capacidad para funcionar en entornos con conexión limitada o en condiciones de interferencia significativa. Asimismo, ha sido necesario desarrollar algoritmos específicos que puedan analizar y actuar sobre grandes volúmenes de datos en situaciones de incertidumbre o bajo condiciones cambiantes, características comunes en escenarios militares.

El IoT está siendo cada vez más integrado en las estrategias de defensa y ha comenzado a influir en la doctrina militar. La capacidad de obtener y analizar datos en tiempo real proporciona una ventaja significativa. Esto permite a las fuerzas armadas no solo responder más rápidamente, sino también anticipar movimientos enemigos y optimizar la logística y la distribución de recursos. Además, el IoT facilita operaciones coordinadas y sincronizadas entre diferentes unidades y tipos de fuerzas, lo que puede ser decisivo en operaciones complejas y multidimensionales.

Después de muchos años dedicados al desarrollo de tecnologías orientadas exclusivamente al ámbito militar, la industria en colaboración con las FAS de varios países ha concluido que el camino más efectivo para progresar es mediante la adopción de tecnologías de uso dual. La teoría de la dualidad sostiene que los avances tecnológicos deben basarse en una plataforma común que permita ajustar ciertos aspectos específicos según el objetivo final deseado. No obstante, la efectividad de estos sistemas depende de su seguridad, enfatizando la necesidad de diseñar IoT con altos estándares de protección.

A diferencia de los sistemas tradicionales de telecomunicaciones, el IoT funciona en entornos altamente hostiles, lo que requiere un enfoque meticuloso en la confidencialidad, integridad y disponibilidad para proteger la información y garantizar la fiabilidad de las operaciones militares (Wrona, 2015).

Por un lado, la confidencialidad impide el acceso no autorizado a la información sensible. En el IoT, esto implica proteger los canales de comunicación y los datos gestionados y almacenados tanto en los dispositivos terminales como en los sistemas de *back-end*ⁱⁱⁱ. La filtración de datos puede comprometer operaciones militares y otorgar ventajas al enemigo.

Sin embargo, la integridad asegura que la información no se altere sin autorización, manteniendo su exactitud y fiabilidad. En el IoT, esto tiene un impacto significativo tanto en los datos que se envían al centro de mando como en los que reciben los dispositivos inteligentes. Incidentes como el derribo del UAV RQ170 Sentinel en Irán en diciembre de 2011 por una suplantación de señales GPS subrayan la importancia de mantener la integridad para evitar

serias consecuencias operativas. Además, la integridad es esencial para prevenir ataques que puedan vulnerar el sistema.

Por otro lado, la disponibilidad asegura que la información y los sistemas más importantes sean accesibles cuando sean necesarios, lo cual es vital para maximizar la utilidad del IoT en entornos militares. Los ataques de “privación de sueño”, que agotan la batería de los dispositivos y les impiden entrar en modos de ahorro de energía, resaltan la importancia de la disponibilidad. Esto pone de relieve la necesidad de investigar tecnologías de cero energía y recuperación de energía, un enfoque de recientes programas de DARPA (U.S. Defense Advanced Research Projects Agency, 2015).

3. RIESGOS ASOCIADOS

La integración del IoT en operaciones militares, aunque prometedora en términos de capacidades mejoradas, viene acompañada de una serie de riesgos y complicaciones que podrían tener graves repercusiones para la seguridad y la efectividad en el campo de batalla. Estos desafíos no solo son técnicos sino también estratégicos, afectando directamente la forma en que las operaciones militares son planeadas y ejecutadas.

El principal riesgo asociado con el IoT es la ciberseguridad, destacando la vulnerabilidad de las redes militares frente a ataques cibernéticos que podrían hacernos perder la iniciativa al paralizar operaciones principales. Dado que el IoT se basa en la interconexión de numerosos dispositivos, cada uno de estos puede convertirse en un posible punto de entrada para amenazas, lo que requiere un enfoque de seguridad en capas que abarque tanto la protección de la infraestructura como la de los datos (Azmoodeh *et al.*, 2019).

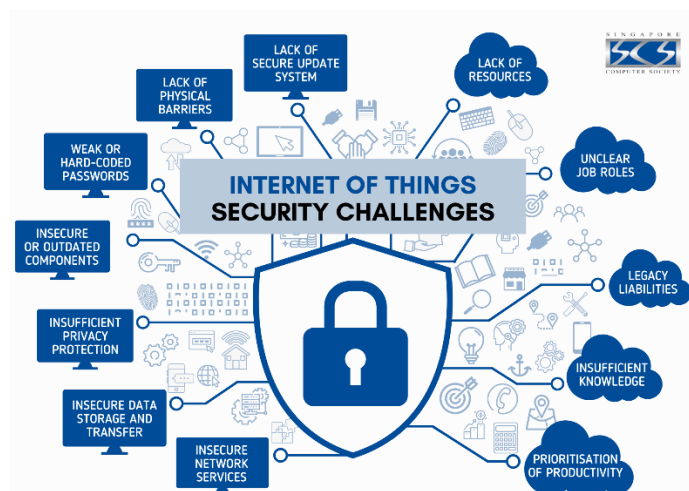


Figura 3. Retos de seguridad del IoT. Fuente: scs.org.sg

Además, la dependencia del loBT aumenta el riesgo de interferencias y sabotajes, donde los adversarios pueden intentar manipular la información o deshabilitar la comunicación. La integridad y la disponibilidad de los datos en tiempo real son esenciales para las decisiones operativas, por lo que cualquier compromiso en este sentido puede tener consecuencias desastrosas, desde la ejecución fallida de operaciones hasta pérdidas humanas.

Otro riesgo es la privacidad y seguridad de la información sensible que circula a través del loBT. La recopilación y procesamiento de grandes volúmenes de datos, incluyendo información clasificada, exigen medidas de seguridad rigurosas para prevenir su exposición o mal uso. Esto también incluye protecciones contra la recolección no autorizada de datos por parte de dispositivos IoT que podrían ser explotados por entidades externas. La Agencia Española de Protección de Datos (AEPD) señala que "es importante que las soluciones IoT implementadas no vulneren innecesariamente la privacidad de las personas" (AEPD, 2021). Esta afirmación resalta la necesidad de un equilibrio entre la implementación tecnológica y el respeto a la privacidad individual.

Finalmente, las barreras culturales y la resistencia al cambio dentro de las estructuras militares pueden obstaculizar la adopción efectiva del loBT (Fraga-Lamas *et al.*, 2016). La transición a nuevas tecnologías requiere no solo inversión en equipos y software sino también en la capacitación, adaptación y mentalización del personal a nuevas herramientas y metodologías. Este cambio cultural es básico para maximizar las ventajas del loBT y mitigar los riesgos asociados con su implementación.

4. POTENCIAL TRANSFORMADOR

El loBT está emergiendo como un catalizador de cambio fundamental en las operaciones militares, introduciendo una nueva era de guerra hiperconectada. Este desarrollo transformador no solo aumenta la eficiencia y precisión de las acciones militares, sino que también redefine los paradigmas existentes en la planificación y ejecución de operaciones.

Una de las mayores oportunidades es la optimización de los sistemas de mando, control, comunicaciones e inteligencia (C3I). La capacidad del loBT para proporcionar datos precisos y en tiempo real puede transformar la toma de decisiones, haciendo que las operaciones sean más ágiles y adaptativas a las condiciones cambiantes del campo de batalla. A través de una red densa de sensores y dispositivos conectados, las fuerzas armadas pueden obtener una comprensión en tiempo real del entorno operativo, lo que les permite tomar decisiones informadas con una rapidez sin precedentes (Uppal, 2023).

Gracias a la obtención de datos en tiempo real, los dispositivos IoT pueden monitorizar continuamente las condiciones del entorno, movimientos enemigos y el estado de los recursos propios, enviando esta información a los centros de comando para un análisis instantáneo. A través de la integración de datos, la capacidad para integrar información de diversas fuentes (aéreas, terrestres, marítimas) y sensores (visuales, térmicos, acústicos) en un solo sistema de gestión proporciona una visión holística que es esencial para la coordinación eficaz de las operaciones.

El IoT no solo proporciona datos, sino que también ofrece las herramientas para analizar y utilizar esa información de manera que optimice las operaciones y la toma de decisiones estratégicas. Algoritmos avanzados y aprendizaje automático^{iv} pueden revelar patrones y tendencias que no serían aparentes para los analistas humanos, proporcionando ideas que pueden anticipar movimientos enemigos o sugerir tácticas óptimas.

Además, el IoT facilita una logística más eficiente, permitiendo una gestión más dinámica de los recursos. Desde el seguimiento de inventarios en tiempo real hasta la predicción de necesidades de mantenimiento, el IoT puede reducir los tiempos de inactividad y asegurar que el equipo esté listo y disponible cuando más se necesite. Esto no solo mejora la preparación operativa, sino que también puede reducir significativamente los costes asociados con la gestión logística (Farooq y Zhu, 2018).

Otra oportunidad relevante es la mejora de la asistencia sanitaria en el campo de batalla. Con dispositivos *wearables*^v IoT diseñados para monitorizar la salud de los soldados, es posible gestionar mejor las emergencias médicas, proporcionando atención rápida y eficaz que puede salvar vidas. La tecnología IoT también puede ayudar en la rehabilitación y el seguimiento a largo plazo de las condiciones de salud, asegurando que el personal reciba la atención adecuada durante y después de las misiones (Dyk *et al.*, 2017).

El IoT también impulsa la innovación en armamento y tácticas de defensa. La integración de IoT en sistemas de armas y plataformas de vigilancia no solo aumenta la precisión y eficacia de estas herramientas, sino que también permite el desarrollo de nuevas estrategias que se apoyen en la superioridad tecnológica. Esto puede incluir desde enjambres de drones autónomos hasta sistemas de defensa cibernética avanzados, abriendo nuevas posibilidades para el enfrentamiento y la defensa en el siglo XXI.

5. COMPLICACIONES TÉCNICAS Y OPERATIVAS

La implementación del IoT no está exenta de desafíos técnicos y estos son tan variados como sus aplicaciones. Uno de los mayores es asegurar la interoperabilidad entre diferentes sistemas y tecnologías. Dado que el IoT implica la integración de una variedad de dispositivos y plataformas, es fundamental que todos estos componentes puedan comunicarse y operar de manera coherente. Esto requiere estándares comunes y protocolos de comunicación que aseguren la compatibilidad y eficiencia de las operaciones conjuntas.

Como miembros de la Unión Europea^{vi}, mantener la ética y el cumplimiento normativo en el uso del IoT es prioritario. Las decisiones sobre cómo y cuándo usar tecnologías que pueden operar de manera autónoma o semi-autónoma en contextos de combate plantean importantes cuestiones éticas y legales. Establecer marcos claros y responsables para el uso del IoT asegura que su implementación se alinee con los principios legales y morales, manteniendo la confianza pública y la legitimidad de las operaciones militares (Anderson *et al.* 2014).

También nos encontramos con la resiliencia frente a ataques físicos, cibernéticos y tácticas de desinformación que es necesaria para mantener la ventaja operativa y la seguridad de las fuerzas aliadas. Anwar *et al.* (2021) subrayan la importancia de la integridad y confiabilidad de la información y la red en entornos de combate. Estrategias de desinformación y la creación de honeypots^{vii} ayudan a confundir y desviar adversarios, mientras que la diversificación y redundancia de dispositivos y canales de comunicación aseguran la continuidad operativa y la disponibilidad de información crítica bajo condiciones adversas.

Además, la cuestión de la soberanía tecnológica es un desafío continuo. La dependencia de tecnología extranjera para componentes clave puede comprometer la seguridad nacional y la independencia operativa. Desarrollar capacidades internas para diseñar, fabricar y mantener tecnologías IoT es esencial para asegurar la autonomía y reducir la vulnerabilidad ante interrupciones en la cadena de suministro o manipulaciones externas (Ametic, 2022). La estrategia industrial de defensa española busca alcanzar esta independencia no solo para solventar el problema sino también para fortalecer el tejido industrial.

6. CONCLUSIONES

Las FAS se encuentran inmersas en un proceso de cambio motivado por los avances industriales que cada vez se producen con mayor velocidad. La rapidez

con la que se producen ha provocado que este proceso se haya convertido en un ciclo continuo en el que los periodos de estabilidad entre revoluciones han desaparecido. Este proceso de innovación, investigación, desarrollo, aplicación y monitorización no puede disminuir su velocidad o estancarse en alguna de fases podría obligarnos a enfrentarnos en desventaja ante el próximo conflicto.

Los desarrollos tecnológicos deben ir acompañados de un proceso de estudio que encuentre las tácticas, técnicas y procedimientos más adecuados para hacer uso de esta ventaja. La formación para aplicar esta doctrina debe ir acompañada de un fuerte esfuerzo de concienciación que ayude a visualizar su utilidad real y evite resistencias internas que frenen el proceso.

El entorno operativo al que nos enfrentamos cambia a la misma velocidad que los términos usados para definirlo, pasando por volátil, incierto, complejo, ambiguo, frágil, ansioso, no lineal o incomprensible. Esta inestabilidad afecta a la rapidez con la que tenemos que tomar las decisiones en el campo de batalla y a los efectos que produce la demora en su aplicación. La clave para disminuir el tiempo empleado es acortar, reducir o acelerar los procesos del ciclo de la decisión. Para ello, es esencial aplicar aquellas tecnologías que permiten esa mejora y nos permiten mantener la iniciativa durante toda la operación.

La optimización del proceso de toma de decisiones se consigue en muchos casos, no solo en el incremento de los datos obtenidos en tiempo real en los que se sustenta, sino en la automatización de gran número de procesos que requerían la intervención humana. Es aquí donde encontramos la fina línea que separa la rapidez y la ética asociada a la deshumanización. La eficacia y la responsabilidad deben de ser constantemente sopesadas, siempre de manera acorde a la situación, para poder desplazar en un sentido o en otro esta línea que las separa.

Esta no es la única dicotomía a la que nos debemos enfrentar. Para desarrollar sistemas tan avanzados de manera eficiente, es necesario hacerlo de forma global, buscando socios con los que compartir el proceso y que se especialicen cada uno de ellos en un aspecto determinado. Esta manera de afrontar el reto nos permite obtener nuevas tecnologías punteras utilizando un menor esfuerzo que desarrollándolo independientemente. El problema al que nos enfrentamos es que este sistema no nos permite alcanzar la soberanía tecnológica necesaria para evitar interferencias o dependencias externas que pueden afectar gravemente a las operaciones.

La gestión de los riesgos asociados con el IoT, junto con una inversión sostenida en áreas clave, es esencial para mitigar las vulnerabilidades y maximizar las capacidades de estas tecnologías emergentes. Mientras que el camino hacia una integración total del IoT está lleno de desafíos, las

recompensas potenciales en términos de ventaja táctica y operacional justifican un enfoque robusto y proactivo.

Por lo tanto, mientras avanzamos, es necesario que las FAS junto con la industria y el sector de la investigación colaboren estrechamente para desarrollar soluciones que no solo aborden los desafíos inmediatos, sino que también preparen el terreno para un futuro en el que el IoT sea una parte integral y segura de las operaciones militares. Esta colaboración será decisiva para asegurar que las oportunidades proporcionadas por el IoT puedan ser plenamente realizadas, llevando las capacidades militares a un nuevo nivel de sofisticación y eficacia.

Madrid, 16 de mayo de 2024

EL COMANDANTE

A handwritten signature in blue ink, consisting of a stylized 'A' with a horizontal line extending to the left and a vertical line extending downwards.

Fdo.: Javier ALDEA ÁLVAREZ DE LARA.
(4036)

NOTAS

ⁱ El término IoT fue utilizado por primera vez por Kevin Ashton en una conferencia en 1999.

ⁱⁱ El Internet de las Cosas (IoT) en el ámbito doméstico, conocido también como hogar inteligente o smart home, incluye una amplia variedad de dispositivos conectados que mejoran la comodidad, la eficiencia energética, la seguridad y la conveniencia en el hogar. Tales como termostatos inteligentes, asistentes virtuales, iluminación inteligente o electrodomésticos conectados.

ⁱⁱⁱ Los sistemas de back-end se refieren a la parte del software que no interactúa directamente con los usuarios, manejando la funcionalidad y lógica de procesamiento de datos detrás de las escenas. Estos sistemas son responsables de manejar la base de datos, el almacenamiento de datos, las aplicaciones y los servidores, proporcionando las capacidades necesarias para que las interfaces de usuario del front-end funcionen correctamente.

^{iv} El aprendizaje automático de los dispositivos implica utilizar modelos estadísticos que permiten a las máquinas mejorar su rendimiento en tareas específicas basándose en datos previos sin estar explícitamente programadas, mejorando así su funcionalidad y eficiencia de forma autónoma.

^v Son dispositivos diseñados para ser usados en el cuerpo, como accesorios o integrados en la ropa. Conectan e intercambian datos con el usuario y otros dispositivos vía Internet o Bluetooth, recopilando información a través de sensores para ofrecer datos útiles.

^{vi} La Unión Europea tiene una extensa normativa sobre el IoT y fue la primera institución en regular el uso de la Inteligencia Artificial.

^{vii} Es una herramienta de seguridad que simula sistemas vulnerables para atraer a atacantes, permitiendo su monitorización sin riesgo para sistemas reales. Se utiliza para recopilar datos sobre tácticas y mejorar medidas de seguridad, aunque requiere manejo cuidadoso para evitar ser detectado o contraproducente.

BIBLIOGRAFÍA

Abdelzaher, T. (2017) *Internet of Battlefield Things (IoBT) REIGN*. Disponible en: <https://iobt.illinois.edu/> [Consultado: 20 de noviembre de 2023].

AEPD (2021) *IoT (II): Del Internet de las Cosas al Internet de los Cuerpos | AEPD, Agencia española de protección de datos*. Disponible en: <https://www.aepd.es/prensa-y-comunicacion/blog/iot-ii-del-iot-al-iob> [Consultado: 6 de febrero de 2024].

Ametic, G. (2022) *Soberanía tecnológica y soberanía digital, Cinco Días*. Disponible en: https://cincodias.elpais.com/cincodias/2022/04/11/opinion/1649671425_912932.html [Consultado: 5 de febrero de 2024].

Anderson, K., Reisner, D. y Waxman, M. (2014) "Adapting the Law of Armed Conflict to Autonomous Weapon Systems", *International law studies*, 90, p. 1-27. [Consultado: 20 de marzo de 2024].

Anwar, A. H., Leslie, N. O. y Kamhoua, C. A. (2021) "Honeypot Allocation for Cyber Deception in Internet of Battlefield Things Systems", en MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM). San Diego, CA, USA: IEEE, pp. 1005-1010. Disponible en doi:10.1109/MILCOM52596.2021.9652927. [Consultado: 9 de enero de 2024].

Azmoodeh, A., Dehghantanha, A. y Choo, K.-K. R. (2019) "Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning", *IEEE Transactions on Sustainable Computing*, 4(1), pp. 88-95. Disponible en doi:10.1109/TSUSC.2018.2809665. [Consultado: 20 de abril de 2024].

Dyk, M., Chmielewski, M. y Najgebauer, A. (2017) "Combat triage support using the Internet of Military Things", en Ganzha, M., Maciaszek, L., y Paprzycki, M. (eds.) *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FEDCSIS)*. New York: IEEE (Federated Conference on Computer Science and Information Systems), pp. 835-842. Disponible en doi:10.15439/2017F186. [Consultado: 11 de enero de 2024].

Farooq, M. J. y Zhu, Q. (2018) "On the Secure and Reconfigurable Multi-Layer Network Design for Critical Information Dissemination in the Internet of Battlefield

Things (IoT)", *IEEE Transactions on Wireless Communications*, 17(4), pp. 2618-2632. Disponible en doi:10.1109/TWC.2018.2799860. [Consultado: 18 de enero de 2024].

Fraga-Lamas, P., Fernández-Caramés, T., Suárez-Albela, M., Castedo, L. y González-López, M. (2016) "A Review on Internet of Things for Defense and Public Safety", *Sensors*, 16(10), p. 1-44. Disponible en doi:10.3390/s16101644. [Consultado: 15 de enero de 2024].

Fragkou, E., Papakostas, D., Kasidakis, T. y Katsaros, D. (2022) "Multilayer Backbones for Internet of Battlefield Things", *Future Internet*. 14(6), p. 1-23. Disponible en doi:10.3390/fi14060186. [Consultado: 29 de enero de 2024].

IERC (2014) *Internet of Things*. Disponible en: https://www.internet-of-things-research.eu/about_iot.htm [Consultado: 10 de febrero de 2024].

Suri, N., Tortonesi, M., Michaelis, J., Budulas, P., Benincasa, G., Russell, S., Stefanelli, C. y Winkler, R. (2016) "Analyzing the applicability of Internet of Things to the battlefield environment", en 2016 International Conference on Military Communications and Information Systems (ICMCIS). pp. 1-8. Disponible en doi:10.1109/ICMCIS.2016.7496574. [Consultado: 15 de marzo de 2024].

Uppal, R. (2023) How Military or Battlefield Internet of Things (MIoT /BIoT) Will Provide Information Dominance, *International Defense Security & Technology*. Disponible en: <https://idstch.com/cyber/how-military-or-battlefield-internet-of-thingsmiot-biot-will-provide-information-dominance/> [Consultado: 19 de diciembre de 2023].

U.S. Defense Advanced Research Projects Agency (2015) *N-Zero Envisions «asleep-Yet-Aware» Electronics That Could Revolutionize Remote Wireless Sensors*. Disponible en: <https://cacm.acm.org/news/185910-n-zero-envisions-asleep-yet-aware-electronics-that-could-revolutionize-remote-wireless-sensors/fulltext?mobile=true?mobile=false> [Consultado: 5 de febrero de 2024].

Wrona, K. (2015) "Securing the Internet of Things a military perspective", en 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). pp. 502-507. Disponible en doi:10.1109/WF-IoT.2015.7389105. [Consultado: 15 de marzo de 2024].