Defensa cibernética

Tecnologías de engaño y defensa de blanco móvil

DOI: 10.29236/sistemas.n176a5

Resumen

En la dinámica actual de las organizaciones y sus retos para avanzar en medio de las tensiones nacionales e internacionales, se hace necesario actualizar las estrategias de ciberseguridad empresarial para entender y aprovechar las inestabilidades e inciertos en favor del logro de sus objetivos estratégicos. En este entorno asimétrico y disruptivo, donde las certezas escasean y los ciberataques conllevan asimetrías inherentes relacionadas con información, capacidades, riesgos, oportunidades y regulaciones, el reto ya no es solo proteger, sino defender y anticipar escenarios, adoptando una postura estratégica que complemente las prácticas tradicionales. De esta forma, las tecnologías de engaño (*Deception Technologies*) y las defensas de blanco móvil (*Moving Target Defense - MTD*) emergen como soluciones estratégicas fundamentales para invertir estas asimetrías a favor de los profesionales de seguridad/ciberseguridad y habilitar nuevas capacidades cibernéticas que permitan aprender continuamente los patrones de ataque y evolucionar los señuelos para desviar los recursos del adversario. La adopción de estas tecnologías representa un cambio de paradigma hacia una defensa cibernética más dinámica y vigilante, orientada a crear confusión estratégica y jugar ahora en el mismo terreno del adversario: distracción y engaño.

Palabras clave

Tecnologías de engaño, disuasión, defensa, asimetrías, ciberseguridad

Introducción

La dinámica del mundo actual y la acelerada transformación digital establece un escenario asimétrico y disruptivo que reta cualquier estrategia corporativa. En este contexto, las tensiones internacionales y los desarrollos tecnológicos emergentes establecen el nuevo referente de las empresas para mantenerse y permanecer en el largo plazo, sin perjuicio de las diferentes posturas que una organización pueda tener para tratar de sortear los embates de cambios súbitos o mareas tecnológicas que puedan afectar la esencia de su negocio o transformar el sector donde opera (Bax & Jaggi, 2025).

En este contexto, el reto de la ciberseguridad no está en proteger y asegurar la operación de la empresa, sino en defender y anticipar los escenarios posibles y probables que puede enfrentar la organización, y desde allí, avanzar en el desarrollo y actualización de las capacidades cibernéticas que le permitan dar cuenta de su promesa de valor para sus clientes. Por tanto, es un imperativo estratégico que las empresas situadas ahora en un ecosistema digital de negocios, de forma regular, exploren y analicen las propuestas y servicios tecnológicos de seguridad para enfrentar las asimetrías propias de los ciberataques actuales (Cano, 2024).

Si bien tecnologías recientes y altamente publicitadas como la inteligencia artificial son de consulta obligada para revisión, otras alternativas, como la gestión continua de exposición a amenazas (*Continuous Threat Exposure Management* – CTEM, en inglés), las tecnologías de engaño (*Deception Technologies*, en inglés) y las defensas de blanco móvil (*Moving Target Defense* - MTD, en inglés) deben ser consideradas como parte fundamental de la actualización y adaptación de las capacidades cibernéticas disponibles en las organizaciones, que buscan distraer, demorar, confundir y disuadir a los posibles adversarios de la empresa en el contexto actual.

Las organizaciones que buscan anticipar los movimientos de sus posibles atacantes, no sólo deben estar al día en sus prácticas básicas de gestión de la seguridad, sino que permanentemente deben cuestionar lo que han aprendido hasta el momento, desconectar los fundamentos propios de su modelo de seguridad y control, para crear nuevas conexiones con las tendencias y señales débiles identificadas en el entorno, y así proponer nuevas distinciones que permitan una actualización del panorama de amenazas potenciadas con tecnologías emergentes y disruptivas (Day & Schoemaker, 2019).

En consecuencia con lo anterior, se desarrolla esta reflexión con el fin de analizar algunas tecnologías emergentes y disruptivas aplicadas al reto de anticipar en la gestión de la ciberseguridad empresarial, no como un ejercicio exclusivamente técnico, sino como una lectura estratégica que las organizaciones deben desarrollar, no solo proteger y asegurar la operación, sino para crear valor y nuevas experiencias en sus clientes, que hoy demandan soluciones creativas, identificar tendencias emergentes y generar ideas viables que transformen la manera de hacer las cosas.

Múltiples denominaciones para el entorno actual

Todos los reportes internacionales coinciden en que las organizaciones si hay algo que deben hacer en la actualidad, es navegar en entornos inciertos e inestables donde la premisa es que las certezas escasean y las turbulencias abundan. Por tanto, reconocer y ajustar sus planteamientos estratégicos es una tarea que en muchos casos dependerá si se enfrenta a una disrupción (afectación estructural del mercado o sector) o perturbaciones (causadas por crisis globales, desastres naturales o accidentes). En este sentido, se han presentado diversas formas de entender la realidad actual del mundo con acrónimos que buscan sugerir marcos de acción y análisis para que las empresas logren entender y superar sus propios miedos y avanzar con paso firme hacia el logro de sus objetivos estratégicos (Verweire, 2023).

A continuación, se presenta en la tabla 1 un breve resumen de los acrónimos más utilizados a nivel global en la actualidad.

Tabla 1

Acrónimos para entender el mundo actual

Acrónimo	Detalle	Fuente
VUCA - *Volatile, Uncertainty, Complexity, Ambiguity*	Volátil, Incierto, Complejo, Ambigüo	1980 – Escuela de Guerra de EE.UU.
TUNA - *Turbulent, Uncertainty, Novelty, Ambiguity*	Turbulento, Incierto, Novedoso, Ambigüo	2016 - Ramírez, R. & Wilkinson, A. (2016). *Strategic reframing. The Oxford Scenario Planning Approach*. Oxford, UK. Oxford Press
BANI - *Brittle, Anxious, Non-linear, Incomprehensible*	Frágil, Ansioso, No-lineal, Incomprensible	2020 - Instituto para el Futuro (Centro de Pensamiento) ubicado en Palo Alto, CA. USA
NAVI – *Nonlinear, Accelerated, Volatile, Interconnected*	No-lineal, Acelerado, Volátil, Interconectado	2025 – EY – Bax, H. J. & Jaggi, G. (2025). What if disruption isn't the challenge, but the chance? *EY*. https://www.ey.com/en_gl/megatrends/what-if-disruption-is-not-the-challenge-but-the-chance

Nota: Elaboración propia.

Cualquiera de las lecturas que se tenga o se elija para comprender el mundo la incertidumbre, la volatilidad y la No-linealidad, son parte inherente de las características que las organizaciones deben atender. En esta misma línea, los riesgos cibernéticos se hacen parte de estas características las cuales se exacerban por cuenta de las tensiones geopolíticas internacionales y la evolución natural de las amenazas digitales. Por lo tanto, las empresas del siglo XXI deben procurar mantener un sistema de vigilancia estratégica cibernética que le permite advertir los cambios y tendencias en el contexto digital para prepararse y sortear las amenazas emergentes que se puedan generar (Bodji et al., 2025).

Entender la dinámica del mundo, resulta siendo la base conceptual y práctica de la gestión del riesgo cibernético, que no busca "predecir" lo que va a ocurrir, sino establecer los distintos escenarios posibles y probables que resulten de interés para la compañía, y de esta forma, tomar las decisiones claves y las acciones estratégicas que reconozcan cómo se puede propagar dicho riesgo y disminuir sus impactos.

Asimetrías de un ciberataque

Para enfrentar los retos que implica entender, atender y superar un ciberataque, es necesario comprender las asimetrías inherentes que este evento conlleva. En este ejercicio, cinco temas resultan claves como fundamento de las reflexiones y las exigencias que se tienen tanto hacia las organizaciones y su relación con el entorno, como desde la perspectiva del atacante como actor clave que busca generar incierto, inestabilidad y caos. A continuación, se detallan en la tabla 2.

Entender estas asimetrías en el escenario actual, es lo que permite a la organización establecer algunos referentes de revisión y análisis para tratar de anticipar los futuros movimientos de sus adversarios. Ignorar esta asimetría en los análisis actuales del panorama de amenazas, implica generar nuevos puntos ciegos en los modelos de seguridad y control, y abrir mayores espacios de maniobra a los atacantes, que buscan cada vez más mimetizarse utilizando la niebla de los conflictos, la diversidad de efectos y la sorpresa como fundamento de su agenda de desestabilización.

Tecnologías emergentes y disruptivas para la gestión del riesgo cibernético

Las asimetrías mencionadas y contextualizadas en la incertidumbre, la volatilidad y la No-linealidad del mundo actual, crean "tormentas digitales adversas" que las organizaciones deben tratar de identificar, anticipar y atender para tener una mejor preparación y limitar los impactos de sus posibles efectos en las organizaciones.

Para ello, actualmente adicional a las tecnologías tradicionales que

Tabla 2
Asimetrías de un ataque cibernético

ASIMETRÍAS	EXPLICACIÓN	IMPACTOS
Asimetría de **información**	El adversario tiene un **mayor nivel de conocimiento** de la infraestructura tecnológica objetivo que la organización.	Generar mayores puntos ciegos que el adversario puede aprovechar. (***Objetivo:*** *Generar sorpresa*)
Asimetría de **capacidades**	El adversario conoce mejor que la organización **el tiempo y los recursos necesarios para acceder al objetivo** (y llevar a cabo actividades de seguimiento).	Implementar de forma acelerada técnicas, tácticas, procedimientos y herramientas novedosas para concretar el ataque. (***Objetivo:*** *Crear inestabilidad*)
Asimetría de **riesgos**	El adversario tiene un **mayor nivel de comprensión del riesgo** que implica llevar a cabo determinadas operaciones cibernéticas en comparación con la organización.	Mejorar la inteligencia para planear y ejecutar con éxito la acción adversa contra la organización. (***Objetivo:*** *Aumentar efectividad*)
Asimetrías de **oportunidades**	El adversario tiene **un mayor nivel de comprensión de la información que puede adquirir y/o la capacidad de disrupción, denegación, degradación y destrucción** en comparación con la organización.	Diseñar y ejecutar escenarios con mayor capacidad de daño y exposición para la organización. (***Objetivo:*** *Diversidad de efectos*)
Asimetría de **regulaciones**	El adversario puede **entrar en conflicto o no con las normativas o iniciativas de regulación global o nacional** para generar amenazas emergentes e innovadoras.	Generar de tensiones entre Estados y particulares que reten los límites tradicionales de las regulaciones y tratados nacionales e internacionales. (***Objetivo:*** *Aumentar las inestabilidades nacionales y globales*)

Nota: Adaptado de: Smeets, 2022, p. 159

operan en las organizaciones como son firewalls de nueva generación, EDR (*Endpoint Detection and Response*), XDR (*eXtended Detection and Response*), SOC (*Security Operation Center*) analíticos, SOAR (*Security Orchestration, Automation, and Response*) y demás siglas que sugieren los proveedores, la práctica muestra que es necesario avanzar en los temas de disuasión como factor determinante para complementar las estrategias actuales de seguridad y control que tienen las empresas.

La disuasión implica crear un entorno donde se inviertan las asimetrías del ciberataque a favor de los profesionales de ciberseguridad / seguridad, con el fin de degradar la gestión de riesgos del adversario y su inteligencia previa, para que cambie de objetivo (no de intención) y que, la organización inicialmente seleccionada ya no sea de

su interés (Burton, 2018). Lograr este resultado, implica que la organización ha alcanzado un nivel de madurez en la gestión de su infraestructura de seguridad y control, donde ahora el reto no es la protección sino la defensa: distraer, demorar, confundir y engañar.

Para ello, han venido evolucionando dos alternativas como las tecnologías de engaño (*Deception Technologies*) y las defensas de blanco móvil (*Moving Target Defense*) como alternativas interesantes para entrar en el mismo juego del adversario: distracción y engaño como fundamento de su acción. A continuación, en la tabla 3 se hace un resumen de estas dos propuestas sus ventajas y limitaciones con el fin de motivar una mejor comprensión de las mismas.

A pesar de que la implementación de estas tecnologías tiene sus retos particulares investigaciones recientes revelan hallazgos que muestran su viabilidad y efectividad para las organizaciones: (Ferguson-Walter et al., 2021)

- La implementación de tecnologías de engaño defensivo son eficaces, incluso si un atacante es consciente de su uso.
- El ciberengaño es eficaz si el atacante simplemente cree que puede estar en uso, aunque no lo esté.
- Las herramientas cibernéticas defensivas y el engaño psicológico impiden a los atacantes penetrar en los sistemas informáticos para filtrar información.

A la fecha se tienen tecnologías de engaño adaptativas basadas en inteligencia artificial (*honeypot* adaptativos) que son sistemas señuelo inteligentes que imitan activos críticos de la red, utilizando IA (Inteligencia Artificial) y aprendizaje automático (ML) para: (Datta & Acton, 2025)

- Atraer y engañar al malware basado en inteligencia artificial generativa (GenAI).
- Aprender continuamente los patrones de ataque y comportamientos del adversario.
- Evolucionar sus señuelos para mantener al atacante comprometido y distraído, y así, desviar sus recursos.

Y como todo sistema de basado en inteligencia artificial hay que considerar sus limitaciones propias como son: (Datta & Acton, 2025)

- Sesgo de datos o Modelo / Alucinaciones.
- Reentrenamiento continuo y diligente de los sistemas de IA de defensa para mantener su eficiencia y resiliencia.
- Baja confianza especialmente con “vectores de ataque novedosos”, lo que genera un posible retraso en la respuesta.

Conclusiones

En el arte y la ciencia de anticipar en la gestión del riesgo cibernético,

Tabla 3
Tecnologías de engaño y tecnologías de blanco móvil

Característica	Tecnologías de engaño (*Cyber Deception*)	Tecnologías de blanco móvil (*Moving Target Defense* - MTD)
Descripción	Buscan confundir y desinformar activamente a los atacantes, influenciando sus decisiones con información falsa (ej. *honeypots*, *honeytokens*, *honeyfiles*, vistas de red engañosas)	Buscan aumentar la incertidumbre y complejidad para el atacante mediante el cambio dinámico y continuo de las configuraciones del sistema o red (ej. mutación de IP, anonimización, diversificación de configuración)
Ventajas	• Nivelan asimetrías atacante-defensor. • Corrompen la toma de decisiones del atacante (desvío, distorsión, agotamiento de recursos). • Recopilan inteligencia valiosa sobre TTPH (Técnicas, Tácticas, Procedimientos y Herramientas) del atacante. • Habilitan la adaptación de las capacidades cibernéticas de forma proactivas y estratégica. • Complementan defensas tradicionales al ser evasivas.	• Aumentan la incertidumbre y complejidad para el atacante. • Invalidan el reconocimiento y la inteligencia base del atacante. • Hacen más difícil el aprendizaje de las reglas de detección por parte del atacante. • Confunden las herramientas automatizadas de reconocimiento del atacante. • Altera la vista de la superficie de ataque del adversario dificultando la ingeniería de exploits confiables y su persistencia en el sistema(s) objetivo.
Limitaciones	• Riesgo de detección por atacantes sofisticados. • La mutación y falsa representación pueden ser costosas o descubiertas. • Riesgo de divulgación accidental y alerta al atacante. • Preocupaciones éticas y legales (fraude, engaño, intrusión).	• Limitaciones por infraestructura física (subredes, conexiones estáticas). • Espacios de IP limitados en ciertos entornos. • Las soluciones basadas en *Software Defined Networking* (SDN)[1] pueden ser costosas y pueden requerir cambio de switches de red. • El mantenimiento de la consistencia en entornos dinámicos es un desafío.

Nota: Basado en Jajodia et al, 2016; Heckman et al., 2015

la tecnología juega un papel importante, no sólo en la implementación, sino en su comprensión y entendimiento de sus posibilidades y alcances. En este sentido, las organizaciones no sólo deben reconocer las bondades de los avances técnicos disponibles, sino situar las mismas en el ejercicio permanente de retar lo que se conoce, y en la capacidad y versatilidad de los atacantes modernos.

[1] Soluciones para generar direcciones IP aleatorias por flujo y crear vistas de red engañosas, permitiendo un control granular sobre las comunicaciones de dispositivos individuales.

En este sentido, la disuasión como control renovado en un escenario donde se privilegia el engaño y la distracción, resulta de interés para incorporar y actualizar en las estrategias actuales de seguridad y control de las empresas (Huang & Zhu, 2023). Por lo tanto, no sólo es entrar en la misma dinámica del adversario, sino saber jugar el juego y no dejarse sorprender por el posible ejercicio de contrainteligencia que ahora va a desarrollar el atacante, al ver que lo que antes era estático y conocido, ahora será dinámico y muchos veces incierto o desconocido.

El ejercicio de inteligencia para reconocer al adversario se hará ahora más intenso y retador para los profesionales en ciberseguridad, que más allá de caracterizar patrones y tendencias relevantes, deberá interpretar y movilizar sus análisis para visualizar lo que está ausente o no se ve, asumir la ambigüedad como la base de sus reflexiones y reconocer en las anomalías la esencia del ejercicio de defensa (Martin, 2019). Esto es, evolucionar de una vista técnica y aplicada (que seguirá siendo importante y relevante) hacia el desarrollo de habilidades para interpretar los cambios del entorno y las asimetrías propias de los ataques para encontrar las señales débiles que sugieran transformaciones claves que lleven a posibles alteraciones del panorama de amenazas.

De esta forma, la defensa cibernética no sólo será empujada a un siguiente nivel de evolución donde se habilitan capacidades para confundir, desviar y agotar los recursos de los atacantes, mientras se obtiene inteligencia estratégica sobre sus TTPH (Técnicas, Tácticas, Procedimientos, Herramientas) y posibles intenciones, sino que se plantea un cambio de paradigma hacia una postura vigilante, dinámica y más consciente del adversario, donde el juego infinito de defensa y ataque entra en nuevo nivel: crear confusión significativa en el descubrimiento y ataque de activos digitales en tiempo real, de forma automatiza y, ahora como servicio.

Referencias

Bax, H. J. & Jaggi, G. (2025). What if disruption isn't the challenge, but the chance? *EY*. https://www.ey.com/en_gl/megatrends/what-if-disruption-is-not-the-challenge-but-the-chance

Bodji, A., Glaser, G. & Teixeira, T. (2025). Resilience through transparency. How the midstream is key for more resilient supply chains. *Arthur D'little Insights*. https://www.adlittle.com/en/insights/viewpoints/resilience-through-transparency

Burton, J. (2018). Cyber Deterrence: A Comprehensive Approach? NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf

Cano, J. (2024). The Virtuous Circle of the Adversary: Challenges and

Threats for Modern Organizations. *ISACA Journal*. 3. https://www.isaca.org/resources/isaca-journal/issues/2024/volume-3/challenges-and-threats-for-modern-organizations

Datta, P. & Acton, T. (2025). Promises and Perils of Generative AI in Cybersecurity. *MIS Quarterly Executive*. *24*(2). 167-184. https://aisel.aisnet.org/misqe/vol24/iss2/5/

Day, G. & Schoemaker, P. (2019). *See soon, act faster. How vigilant leader thrive in an era of digital turbulence*. Cambridge, MA. USA: MIT Press.

Ferguson-Walter, K. J., Major, M. M., Johnson, C. K. & Muhleman, D. H. (2021). Examining the Efficacy of Decoy-Based and Pyschological Cyber Deception. *30th USENIX Security Symposium (USENIX Security 21)*. 1127–1144.

Heckman, K. E., Stech, F. J., Thomas, R. K., Schmoker, B., & Tsow, A. W. (2015). *Cyber denial, deception and counter deception: A framework for supporting active cyber defense* (1a ed.). Springer International Publishing.

Huang, L., & Zhu, Q. (2023). *Cognitive security: A system-scientific approach*. Springer International Publishing.

Jajodia, S., Subrahmanian, V. S., Swarup, V., & Wang, C. (Eds.). (2016). *Cyber deception: Building the scientific foundation* (1a ed.). Springer International Publishing.

Martin, P. (2019). *The rules of security. Staying safe in a risky world*. Oxford, UK. Oxford University Press.

Smeets, M. (2022). *No Shortcuts. Why States Struggle to Develop a Military Cyber-Force*. USA: Oxford University Press.

Verweire, K. (2023). *Strategy in Turbulent Times: How to Design a Strategy that is Robust and Future-Proof*. Lannoo.

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*