

Libro de resúmenes

*XVII Jornadas de Estudios de
Seguridad*

RECONFIGURANDO LA SEGURIDAD
INTERNACIONAL:
NUEVAS TECNOLOGÍAS,
OPORTUNIDADES Y DESAFIOS

Madrid

7 y 8 de mayo de 2025



Instituto Universitario General Gutiérrez
Mellado Universidad Nacional de
Educación a Distancia (UNED)

Coordinadores

Fernando García Blázquez

Subdirector Militar del IUGM

Clara Bañares Martín

Investigadora del IUGM

Ponentes

Luis Vicente Pérez Gil

Fulvio Queirolo Perellano

Jonnathan Jiménez Reina

Francisco José Oliva

Lucía Otero López

Soukaina Messou

David García Cantalapiedra

Mercedes De Rueda Hernanz

Paula M. Núñez-Guerra

Adrián Nicolás Marchal González

Jeimy J. Cano M.

ÍNDICE

PANEL NUEVAS TECNOLOGÍAS

Desarrollos Recientes de Armas Estratégicas Avanzadas Rusas y su Aplicación en los Conflictos Internacionales

Luis V. Pérez Gil

Desarrollo Tecnológico como Vector de Amenaza del Sur Global

Fulvio Queirolo Perellano

Amenazas Híbridas, Tecnologías Disruptivas y Crimen Organizado Transnacional: Desafíos para el Hemisferio Occidental

Jonnathan Jiménez Reina

La Inteligencia Artificial como Arma

Francisco José Oliva

De la Ciencia Ficción a la Realidad: Implicaciones Éticas y de Género de la IA en Seguridad y Defensa

Lucía Otero López

Militarización de la IA: El Uso de la IA en los Conflictos Armados, Caso del Líbano

Soukaina Messou

Inteligencia Artificial, Disuasión Nuclear y Toma de Decisiones

David García Cantalapiedra

PANEL CIBERSEGURIDAD

La Dinámica del Dominio Cibernético en la OTAN: Desafíos y Estrategias para la Seguridad Colectiva

Mercedes De Rueda Hernanz

La Ciberseguridad en la Lucha contra el Ciberterrorismo en la UE y la OTAN: ¿Intereses Compartidos?

Paula María Núñez-Guerra

El Factor Humano en Ciberseguridad: el Eslabón Más Importante y su Explotación a Través de la Ingeniería

Adrián Nicolás Marchal González

Agencias Nacionales de Seguridad Digital. Un Marco de Trabajo en Perspectiva Ecosistémica

Jeimy J. Cano M.

PONENCIAS DEL PANEL NUEVAS TECNOLOGÍAS

DESARROLLOS RECIENTES DE ARMAS ESTRATÉGICAS AVANZADAS RUSAS Y SU APLICACIÓN EN LOS CONFLICTOS INTERNACIONALES

RECENT DEVELOPMENTS OF RUSSIAN ADVANCED STRATEGIC WEAPONS, AND THEIR APPLICATION IN INTERNATIONAL CONFLICTS

Luis V. Pérez Gil ¹

RESUMEN

En un sistema internacional cada vez más complejo e inestable, las grandes potencias recurren de forma creciente al poder duro (*hard power*) frente a otras etapas después del final de la Guerra Fría, donde dominaron a través de la cooperación y la paz (*soft power*). Pero este cambio no es reciente; no comenzó con el estallido de la guerra en Ucrania en febrero de 2022, sino que se activó mucho antes cuando los dirigentes de la política exterior americana decidieron romper aquellos equilibrios de la Posguerra Fría e iniciaron el desmantelamiento del régimen de control de armamentos. En ese momento, tanto Rusia como China aumentaron el ritmo de sus programas de armas estratégicas avanzadas para dotarse de las capacidades necesarias para disuadir y, en caso de no tener éxito, poder combatir y ganar guerras. La Rusia de Putin ha recurrido a estas nuevas armas en su guerra contra Ucrania.

PALABRAS CLAVE: Armas estratégicas, Desarrollo Tecnológico, Conflictos Internacionales, Rusia, Guerra en Ucrania.

ABSTRACT

In a complex and unstable international system, great powers are increasingly turning to hard power, compared to previous eras after the end of the Cold War, when they dominated through cooperation and peace (*soft power*). But this change is not recent; it did not begin with the outbreak of the war in Ukraine in February 2022, but it was triggered long before when American foreign policy leaders decided to break those post-Cold War balances and began dismantling the arms control regime. At that time, both Russia and China increased the pace of their advanced strategic weapons programs to

¹ Luis V. Pérez Gil es doctor en Derecho con Premio Extraordinario por la Universidad de La Laguna, profesor de Derecho Internacional y Ciencia Política en varias universidades nacionales y extranjeras. Sus líneas de investigación principales son la teoría del conflicto y la guerra nuclear. Es autor de cuatro libros y más de cien artículos y ensayos en revistas nacionales y extranjeras. Actualmente se desempeña como analista en el Instituto Español de Estudios Estratégicos (IEEE) en Madrid.

Luis V. Pérez Gil holds a PhD in Law with an Extraordinary Award from the University of La Laguna, and is professor of Constitutional and International Law at several national and international universities, with main lines of research in conflict theory and nuclear war. He is author of four books and more than one hundred articles and essays in national and international journals. He currently works as analyst at the Instituto Español de Estudios Estratégicos (IEEE) in Madrid.

prepare themselves with the necessary capabilities to deter and, if unsuccessful, to be able to fight and win wars. Putin's Russia has resorted to these new weapons in its war against Ukraine.

KEYWORDS: Strategic Weapons, Technological Development, International Conflicts, Russia, War in Ukraine.

DESARROLLO TECNOLÓGICO COMO VECTOR DE AMENAZA DEL SUR GLOBAL

TECHNOLOGICAL DEVELOPMENT AS A VECTOR OF THREAT TO THE GLOBAL SOUTH

Fulvio Queirolo Pellerano ²

RESUMEN

Convengamos que el Sur Global se ha instalado como una plataforma de coordinación de países emergentes. Un foro perfilado para debatir problemas que, en condición de comunes y pendientes, podrían encontrar espacio de solución. La instancia procura dar respuesta a temas largamente arraigados como el crecimiento y desarrollo económico, recursos para salud, educación y alimentación, la seguridad global y efectos del cambio climático. Pero por sobre todo ello intentar modificar el orden establecido que rige en el ámbito del sistema internacional. Sus detractores sostienen que es justamente su diversidad y heterogeneidad la mayor debilidad para lograr buenos resultados. Discusión que se encuentra abierta y objeto de debate. Pese a la resistencia de poderosos actores internacionales sobre la viabilidad e impacto de esta plataforma en el sistema internacional, el Sur Global, continúa consolidando y ampliando su nomenclatura. En el entorno del Sur Global se puede identificar ciertos liderazgos. Sin duda que China, India y la República Islámica de Irán presentan una musculatura que permite reconocerles como tales, sin desconocer la existencia de más de alguna pugna y tensión al interior de dicha tribuna. Entre ellas, las disímiles y contradictorias posturas, de apoyo o rechazo, a sanciones impuestas por la comunidad internacional. Asumiendo que el Sur Global no se posicionaría en reemplazo de organizaciones internacionales, cuyo fin es velar por la paz y seguridad internacional, sí se podría asentir una condición complementaria. Entonces, si se admite que este foro abraza principios universales de paz y seguridad, el trabajo postula a demostrar que el desarrollo tecnológico, utilizado como instrumento de poder de actores del Sur Global, converge en amenaza a la inestabilidad internacional.

PALABRAS CLAVE: Sur Global, Países Emergentes, Desarrollo Tecnológico, Amenazas

ABSTRACT

Let us agree that the Global South has established itself as a coordination platform for emerging countries. A forum designed to discuss problems that, as shared and pending, could find room for resolution. This forum seeks to address long-standing issues such as economic growth and development, resources for health, education, and food, global security, and the effects of climate change. But above all, it seeks to change the established order that governs the international system. Its detractors argue that its diversity and heterogeneity are precisely the greatest weaknesses in achieving good results. This discussion is open and subject to debate. Despite resistance from powerful international actors regarding the viability and impact of this platform on the international

² Magíster en Ciencia Política, Seguridad y Defensa (ANEPE). Doctorando en Seguridad Internacional (UNED, programa internacional, IUGGM, España). Investigador asociado Universidad UBO, Chile.

system, the Global South continues to consolidate and expand its nomenclature. Within the Global South, certain leaderships can be identified. Undoubtedly, China, India, and the Islamic Republic of Iran have the muscle to recognize them as such, without ignoring the existence of more than a few struggles and tensions within that forum. Among them are the diverse and contradictory positions, of support or rejection, of sanctions imposed by the international community. Assuming that the Global South would not position itself as a replacement for international organizations, whose purpose is to ensure international peace and security, a complementary condition could be established. Thus, if it is accepted that this forum embraces universal principles of peace and security, the paper aims to demonstrate that technological development, used as an instrument of power by actors in the Global South, constitutes a threat to international instability.

KEYWORDS: Global South, Emerging Countries, Technological Development, Threats

AMENAZAS HÍBRIDAS, TECNOLOGÍAS DISRUPTIVAS Y CRIMEN ORGANIZADO TRANSNACIONAL: DESAFÍOS PARA EL HEMISFERIO OCCIDENTAL

HYBRID THREATS, DISRUPTIVE TECHNOLOGIES AND TRANSNATIONAL ORGANIZED CRIME: CHALLENGES FOR THE WESTERN HEMISPHERE

Jonnathan Jiménez-Reina³

RESUMEN

La presente comunicación analiza el impacto de las tecnologías disruptivas —criptomonedas, inteligencia artificial y drones— en los sistemas de seguridad y defensa frente al crimen organizado transnacional en América, desde Alaska hasta la Patagonia. La originalidad radica en abordar cómo estas tecnologías, utilizadas por actores ilegales como cárteles mexicanos, disidencias de las FARC y el ELN, reconfiguran las dinámicas delictivas y desafían las capacidades estatales. La metodología empleada combina un enfoque cualitativo basado en el análisis documental de fuentes académicas indexadas, informes estratégicos y casos de estudio representativos. Esto permitió identificar patrones de uso criminal y su impacto en la seguridad regional. Entre las principales conclusiones, se destaca que estas tecnologías potencian tanto las capacidades del crimen organizado transnacional como las respuestas estatales, generando una carrera tecnológica asimétrica que exige cooperación internacional, regulación ágil y fortalecimiento de capacidades en ciberseguridad e inteligencia artificial para mitigar riesgos emergentes.

PALABRAS CLAVE: Amenazas híbridas, Cooperación, Crimen Organizado Transnacional, Hemisferio occidental, Tecnologías disruptivas.

ABSTRACT

This communication analyzes the impact of disruptive technologies —cryptocurrencies, artificial intelligence and drones— on security and defense systems against transnational organized crime in the Americas, from Alaska to Patagonia. The originality lies in addressing how these technologies, used by illegal actors such as Mexican cartels, FARC and ELN dissidents, reconfigure criminal dynamics and challenge state capacities. The methodology employed combines a qualitative approach based on documentary analysis of indexed academic sources, strategic reports and representative case studies. This made it possible to identify patterns of criminal use and their impact on regional security.

³ Estudiante de doctorado en Seguridad Internacional, Universidad de Educación a Distancia-UNED, España. Magíster en Seguridad y Defensa Nacionales, y en Derechos Humanos y DICA, Escuela Superior de Guerra “General Rafael Reyes Prieto”-ESDEG, Colombia. Profesional en Política y Relaciones Internacionales, Universidad Sergio Arboleda, Colombia. Docente Ocasional, Tiempo Completo en Categoría Asociado, ESDEG, Colombia. Investigador Asociado reconocido por MinCiencias, Colombia. Código ORCID: <https://orcid.org/0000-0001-9042-834X> – Contacto: jjimenez1956@alumno.uned.es

Among the main conclusions, it is emphasized that these technologies enhance both the capabilities of transnational organized crime and state responses, generating an asymmetric technological race that demands international cooperation, agile regulation and capacity building in cybersecurity and artificial intelligence to mitigate emerging risks.

KEYWORDS: Disruptive Technologies, Hybrid Threats, International Cooperation, Organized Transnational Crime, Western Hemisphere.

LA INTELIGENCIA ARTIFICIAL COMO ARMA

ARTIFICIAL INTELLIGENCE AS WEAPON

Francisco José Oliva Bermejo ⁴

RESUMEN

En un escenario de competencia geopolítica creciente se están identificando indicios de cómo la tecnología está afectando a las características de las sociedades occidentales haciéndolas más vulnerables y potenciando las capacidades disponibles para imponer la voluntad política, ya sea mediante la coerción y la subversión, sin llegar a la guerra o llegando a la confrontación directa. En este escenario es la Inteligencia Artificial la gran protagonista y es el elemento catalizador de una revolución de los asuntos militares que afectará a la seguridad y la defensa.

PALABRAS CLAVE: Inteligencia Artificial, Zona Gris, Guerra Híbrida, Revolución Asuntos Militares

ABSTRACT

In a scenario of growing geopolitical competition, there are signs identifying how technology affect the characteristics of Western societies, making them more vulnerable and enhancing the capacities available to impose political will, through both coercion and subversion, without reaching war, or reaching a direct confrontation. In this scenario, Artificial Intelligence is the main protagonist and is the catalyst for a revolution in military affairs and security and defense.

KEYWORDS: Artificial Intelligence, Grey Zone, Hybrid War, Revolution Military Affairs

⁴ Doctorando en Seguridad Internacional. Coronel Jefe de la Sección de Ciberespacio y Operaciones Electromagnéticas de Ejército de Tierra.
PhD student in International Security. Colonel Chief of the Cyberspace and Electromagnetic Operations Section of the Army.

DE LA CIENCIA FICCIÓN A LA REALIDAD: IMPLICACIONES ÉTICAS Y DE GÉNERO DE LA IA EN SEGURIDAD Y DEFENSA

FROM SCIENCE FICTION TO REALITY: ETHICAL AND GENDER IMPLICATIONS OF AI IN SECURITY AND DEFENSE

Lucía Otero López ⁵

RESUMEN

La presente comunicación explora las implicaciones éticas y de género del uso de la Inteligencia Artificial (IA) en seguridad y defensa. La IA, aunque eficiente en el procesamiento de datos y con una gran capacidad de aprender mediante algoritmos, no está exenta de cuestionamientos morales que es necesario considerar. La falta de representatividad de mujeres en los datos históricos, así como en los sectores de seguridad y defensa, tecnología y ciencia y en roles de liderazgo, contribuye a que la IA perpetue las desigualdades de género. Además, la IA carece de compasión genuina, lo que limita su capacidad para tomar decisiones éticas; a pesar de esto, también serían cuestionables ciertas decisiones humanas en conflictos. La responsabilidad legal en este campo es compleja y requiere transparencia y supervisión humana. Es crucial desarrollar normativas que aseguren la ética y la inclusión de diversas perspectivas en el uso de la IA.

PALABRAS CLAVE: Inteligencia Artificial (IA), seguridad y defensa, ética, moralidad, género

ABSTRACT

This communication explores the ethical and gender implications of the use of Artificial Intelligence (AI) in security and defense. AI, although efficient in data processing and with a great capacity to learn through algorithms, is not exempt from moral questions that need to be considered. The lack of representation of women in historical data, as well as in the sectors of security and defense, technology, and science, and in leadership roles, contributes to AI perpetuating existing gender inequalities. Furthermore, AI lacks genuine compassion, which limits its ability to make ethical decisions; despite all of this, certain human decisions in conflicts would also be questionable. Legal responsibility in this field is complex and requires transparency and human oversight. It is crucial to develop regulations that ensure ethics and the inclusion of diverse perspectives in the use of AI.

KEYWORDS: Artificial Intelligence (AI), security and defense, ethics, morality, gender

⁵ Psicóloga especialista en gerontología social, igualdad y no discriminación. Técnica de la Unidad de Emergencias de Cruz Roja en Galicia.

Psychologist specializing in social gerontology, equality and non-discrimination. Technician of the Emergency Response Unit at Galician Red Cross.

MILITARIZACIÓN DE LA IA: EL USO DE LA IA EN LOS CONFLICTOS ARMADOS, CASO DEL LÍBANO

MILITARIZATION OF AI : THE USE OF AI IN ARMED CONFLICTS, CASE OF LEBANON

Soukaina Messou⁶

RESUMEN

El conflicto entre Israel y el Líbano muestra signos claros de transformación impulsada por la inteligencia artificial en el ámbito militar. Israel ha integrado sistemas de IA en sus operaciones para mejorar la precisión de sus ataques, utilizando drones autónomos y misiles guiados capaces de identificar y destruir objetivos con gran exactitud. Por su parte, Hezbolá ha demostrado una notable adaptabilidad, recurriendo a tácticas como la interferencia en las comunicaciones y el uso de drones en incursiones sorpresivas. Esta comunicación examina cómo estas tecnologías están modificando la manera en que se desarrolla el combate, planteando complejas cuestiones éticas y legales. La posibilidad de que sistemas autónomos tomen decisiones letales sin intervención humana representa uno de los grandes desafíos regulatorios de nuestro tiempo, que exige un marco legal internacional. La tecnología está alterando no solo la naturaleza de la guerra, sino también su percepción, organización, gestión y sus consecuencias humanitarias y geopolíticas.

PALABRAS CLAVE: Inteligencia Artificial, Defensa, Seguridad, Conflictos Armados, Ética.

ABSTRACT

The conflict between Israel and Lebanon shows clear signs of an artificial intelligence-driven transformation in the military sphere. Israel has integrated AI systems into its operations to improve the precision of its attacks, using autonomous drones and guided missiles capable of identifying and destroying targets with great accuracy. For its part, Hezbollah has demonstrated remarkable adaptability, resorting to tactics such as communications jamming and the use of drones in surprise raids. This communication examines how these technologies are changing the way combat is conducted, raising complex ethical and legal questions. The possibility of autonomous systems making lethal decisions without human intervention represents one of the great regulatory challenges of our time, demanding an international legal framework. Technology is altering not only the nature of warfare but also its perception, organization, management, and its humanitarian and geopolitical consequences.

KEYWORDS: Artificial Intelligence, Defense, Security, Armed Conflicts, Ethics.

⁶ Doctoranda en Seguridad Internacional en el Instituto Universitario General Gutiérrez Mellado (IUGM-UNED) en Madrid. Profesora asistente de francés.

PhD candidate in International Security at Instituto Universitario General Gutiérrez Mellado (IUGM-UNED) in Madrid, Spain. Assistant professor of French.

INTELIGENCIA ARTIFICIAL, DISUASIÓN NUCLEAR Y TOMA DE DECISIONES.

ARTIFICIAL INTELLIGENCE, NUCLEAR DETERRENCE AND DECISION-MAKING

David García Cantalapiedra⁷

RESUMEN

La inteligencia artificial (IA) se ha convertido ahora en una parte importante del nuevo sistema de armas, que tiene tanto un impacto tanto negativo como positivo en la disuasión nuclear y en su papel en la toma de decisiones en crisis. Existe una amplia bibliografía y de expertos dedicados a este ámbito que en España no se ha estudiado en profundidad aún. La importancia de la IA es trans-dominio y en este artículo se plantearán algunos de los temas que parecen más urgentes desde el punto de vista estratégico: estabilidad estratégica, escalada (*escalation dominance and management*), vulnerabilidad mutua (*mutual vulnerability*) y capacidad de represalia (*second strike capability*)

PALABRAS CLAVE: IA, Disuasión Nuclear, Armas Nucleares, EEUU, China, Toma de Decisiones

ABSTRACT

Artificial intelligence (AI) has become an important part of the new weapons system, which has both a negative and positive impact on nuclear deterrence and its role in decision-making in crises. There is an extensive bibliography and expertise dedicated to this field which in Spain has not yet been studied in depth. The importance of AI is already transdomain and in this article we will raise some of the issues that seem most urgent from a strategic point of view: strategic stability, escalation (*Escalation dominance and management*), Mutual Vulnerability and second-strike capability.

KEYWORDS: AI, Nuclear Deterrence, Nuclear Weapons, USA, China, Decision-making

⁷ David García Cantalapiedra, Profesor Titular de Universidad. UCM. Director del Grupo Complutense de Estudios Internacionales y Estratégicos.

David García Cantalapiedra, Associate Professor. UCM. Director of the Complutense Group of International and Strategic Studies.

PONENCIAS DEL PANEL NUEVAS TECNOLOGÍAS

LA DINÁMICA DEL DOMINIO CIBERNÉTICO EN LA OTAN: DESAFÍOS Y ESTRATEGIAS PARA LA SEGURIDAD COLECTIVA

THE DYNAMICS OF THE CYBER DOMAIN IN NATO: CHALLENGES AND STRATEGIES FOR COLLECTIVE SECURITY

Mercedes De Rueda Hernanz⁸

RESUMEN

En el contexto de la transformación digital global, la OTAN se enfrenta a desafíos sin precedentes que exigen una revisión constante de sus tácticas y estrategias en el dominio cibernético. Reconocido oficialmente como el quinto dominio operativo, junto con los tradicionales ámbitos terrestre, marítimo, aéreo y espacial, el ciberespacio se ha consolidado como un componente esencial para la seguridad colectiva y la defensa mutua entre los Estados miembros. El presente estudio analiza el proceso de adaptación de las políticas y operaciones de la Alianza ante la creciente sofisticación de las amenazas cibernéticas, con el fin de preservar su capacidad disuasoria y operativa en un entorno cada vez más interconectado y vulnerable.

PALABRAS CLAVE: OTAN, Ciberespacio, Seguridad Colectiva, Defensa Cibernética, Operaciones Cibernéticas.

ABSTRACT

In the context of global digital transformation, NATO faces unprecedented challenges that require the continuous reassessment of its tactics and strategies in the cyber domain. Officially recognized as the fifth operational domain, alongside the traditional land, maritime, air, and space domains, cyberspace has become a critical component of collective security and mutual defense among member states. This study examines NATO's ongoing efforts to adapt its policies and operations in response to the increasing sophistication of cyber threats, with the aim of preserving its deterrence and operational capabilities in an increasingly interconnected and vulnerable environment.

KEYWORDS: NATO, Cyberspace, Collective Security, Cyber Defense, Cyber Operations.

⁸ Estudiante de doctorado en Seguridad Internacional. Actualmente trabaja en la OTAN, en la Agencia de Comunicación e Información, en el área de ciberseguridad.
PhD candidate in International Security. Currently working at NATO's Communication and Information Agency in the field of cybersecurity.

LA CIBERSEGURIDAD EN LA LUCHA CONTRA EL CIBERTERRORISMO EN LA UE Y LA OTAN: ¿INTERESES COMPARTIDOS?

CYBERSECURITY IN THE FIGHT AGAINST CYBERTERRORISM IN THE EU AND NATO: SHARED INTERESTS?

Paula M. Núñez-Guerra ⁹

RESUMEN

La mayor parte de las amenazas actuales se caracterizan por tener un denominador común: no entienden de fronteras. Además de ello, los fenómenos como el terrorismo, evolucionan de manera exponencial y son cada vez más latentes. Actualmente, los instrumentos que utilizan los terroristas en la Red pasan de ser armas convencionales a ser ciberarmas. El ciberespacio permite que la actividad se ejecute a una velocidad excepcional donde los *hackers* actúan al servicio de las organizaciones terroristas, tratándose así de ciber-mercenarios encargados de cometer actos delictivos. Grandes organismos internacionales como la UE y la OTAN han diseñado líneas de actuación para luchar contra el ciberterrorismo a través de la ciberseguridad. Sin embargo, ¿comparten ambos organismos internacionales los mismos intereses en materia de ciberseguridad?

PALABRAS CLAVE: ciberseguridad, ciberterrorismo, UE, OTAN, políticas

ABSTRACT

Most of today's threats are characterized by a common denominator: they do not understand borders. Moreover, phenomena such as terrorism are evolving exponentially and are becoming increasingly latent. Today, the tools used by terrorists on the Internet have evolved from conventional weapons to cyber weapons. Cyberspace allows activity to be carried out at exceptional speed, where hackers act in the service of terrorist organizations, thus becoming cyber-mercenaries in charge of committing criminal acts. Major international organizations such as the EU and NATO have designed courses of action to combat cyberterrorism through cybersecurity. However, do both international organizations share the same cybersecurity interests?

KEYWORDS: cybersecurity, cyberterrorism, EU, NATO, politics

⁹ Periodista por la Universidad de Málaga. Máster en Relaciones Internacionales y Comunicación por la Universidad Camilo José Cela y, actualmente doctoranda en el Programa de Doctorado en Ciencias Políticas y de la Administración y Relaciones Internacionales en la Universidad Complutense de Madrid *Journalist from the University of Malaga. Master's degree in International Relations and Communication from the Camilo José Cela University and currently a PhD candidate in the Doctorate Program in Political and Administration Sciences and International Relations at the Complutense University of Madrid.*

EL FACTOR HUMANO EN CIBERSEGURIDAD: EL ESLABON MÁS IMPORTANTE Y SU EXPLOTACIÓN A TRAVÉS DE LA INGENIERÍA

THE HUMAN FACTOR IN CYBERSECURITY: THE MOST IMPORTANTE LINK AND ITS EXPLOITATION THROUGH SOCIAL ENGINEERING

Adrián Nicolás Marchal González¹⁰

RESUMEN

La dimensión humana constituye actualmente el componente más vulnerable en la estructura defensiva de las organizaciones frente a ciberamenazas. Los perpetradores implementan metodologías diversificadas de ingeniería social para explotar predisposiciones psicológicas y patrones conductuales que facilitan compromisos de seguridad. Esta comunicación examina la instrumentalización sistemática de factores psicosociales como vía preferente de acceso ilegítimo a sistemas protegidos. El análisis abarca diversas manifestaciones técnicas como *phishing*, *spear phishing* y *ransomware*, entre otras variantes emergentes, que configuran un ecosistema complejo de amenazas fundamentado en la manipulación cognitiva y emocional. La caracterización técnica de estos vectores de ataque revela una sofisticación progresiva y capacidad adaptativa que supera frecuentemente las medidas defensivas convencionales. La tendencia evolutiva sugiere una correlación directa entre efectividad de ataques y explotación de vulnerabilidades humanas. La gestión eficaz de este vector crítico requiere una aproximación integral que trascienda soluciones meramente tecnológicas, incorporando dimensiones formativas, organizacionales y procedimentales en la configuración de estrategias defensivas.

PALABRAS CLAVE: Ciberseguridad, hacking ético, ingeniería social, factor humano, concienciación.

ABSTRACT

The human dimension currently constitutes the most vulnerable component in the defensive structure of organizations against cyber threats. Perpetrators implement diversified social engineering methodologies to exploit psychological predispositions and behavioral patterns that facilitate security compromises. This communication examines the systematic instrumentalization of psychosocial factors as the preferred pathway for illegitimate access to protected systems. The analysis encompasses various technical manifestations such as *phishing*, *spear phishing*, and *ransomware*, among other emerging variants, which configure a complex ecosystem of threats founded on cognitive and emotional manipulation. The technical characterization of these attack vectors reveals a progressive sophistication and adaptive capacity that frequently surpasses conventional

¹⁰ Doctor en Derecho. Director Departamento de Seguridad y Defensa Universidad Nebrija.
P.h.D. of Law. Director of the Department of Security and Defense at Nebrija University.

defensive measures. The evolutionary trend suggests a direct correlation between attack effectiveness and the exploitation of human vulnerabilities. The effective management of this critical vector requires a comprehensive approach that transcends merely technological solutions, incorporating formative, organizational, and procedural dimensions in the configuration of defensive strategies.

KEYWORDS: Cybersecurity, Ethical hacking, Social Engineering, Human Factor, Awareness

**AGENCIAS NACIONALES DE SEGURIDAD
DIGITAL. UN MARCO DE TRABAJO EN
PERSPECTIVA ECOSISTÉMICA**

***NATIONAL DIGITAL SECURITY AGENCIES. A
FRAMEWORK IN AN ECOSYSTEM PERSPECTIVE***

Jeimy J. Cano M. ¹¹

RESUMEN

Las Agencias Nacionales de Seguridad Digital (ANSD) son parte del eje articulador de la estrategia de ciberseguridad y elemento clave de la postura de ciberdefensa de un país. En este sentido, las ANSD se presentan como un foco natural de tensiones, de tal forma que es necesario usar los recursos propios de la ciberdiplomacia para motivar consensos entre los diferentes actores del ecosistema digital. Tomando los fundamentos de ciberdiplomacia de París 2018 y los elementos de dichos ecosistemas, se propone un marco de trabajo que permita a las ANSD diseñar una agenda de seguridad digital situada tanto en la dinámica de la geopolítica global, como en los retos de cada país. Basado en lo anterior, se detalla una aplicación práctica del uso de este marco para Colombia, concluyendo con algunas reflexiones sobre los retos de la aplicación del marco frente a los desafíos de las políticas públicas en los países.

PALABRAS CLAVE: Ciberseguridad, Ciberdefensa, Ecosistema Digital, Ciberdiplomacia, Políticas Públicas

ABSTRACT

National Digital Security Agencies (NDSAs) are part of the backbone of the cybersecurity strategy and a key element of a country's cyberdefense posture. In this sense, the NDSAs are a natural focus of tensions, so it is necessary to use the resources of cyber diplomacy to motivate consensus among the different actors of the digital ecosystem. Based on the Paris 2018 cyberdiplomacy fundamentals and the elements of such ecosystems, a framework is proposed that allows the NDSAs to design a digital security agenda situated both in the dynamics of global geopolitics, as well as in the challenges of each country. Based on the above, a practical application of the use of this framework for Colombia is detailed, concluding with some reflections on the challenges of the application of the framework in the context of the challenges of public policies in the countries.

KEYWORDS: Cybersecurity, Cyberdefense, Digital Ecosystem, Cyberdiplomacy, Public Policies

¹¹ Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes, Colombia. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Administración de Negocios por Newport University, USA y Ph.D en Educación por la Universidad Santo Tomás, Colombia. Profesor universitario y asesor internacional en ciberseguridad y ciber defensa. *B.Sc. and M.Sc. in Computer and Systems Engineering from Universidad de los Andes, Colombia. Specialist in Disciplinary Law, Universidad Externado de Colombia. Ph.D in Business Administration from Newport University, USA and Ph.D in Education from Universidad Santo Tomás, Colombia. Professor and international advisor in cybersecurity and cyber defense.*

