SOCIAL REVIEW | Vol. 14 No. 1 2026| ISSN 2695-9755
International Social Sciences Review / Revista Internacional de Ciencias Sociales
https://doi.org/10.62701/revsocial.v14.5565

LA CIBERSEGURIDAD FRENTE A LAS AMENAZAS HÍBRIDAS
Desafíos y soluciones desde la Universidad

Cybersecurity in the Face of Hybrid Threats: Challenges and solutions from the University

MARÍA JOSÉ VICENTE VICENTE (MARIAJOSE.VICENTE@UCLM.ES)[1]
[1]Universidad de Castilla-La Mancha, España

KEYWORDS
Cybersecurity
Disinformation
University education
Hybrid threats
Interdisciplinary training
Psychological manipulation
Cognitive warfare

ABSTRACT
This paper analyzes the growing gap between university cybersecurity education and the demands of hybrid threats, which combine technical attacks with psychological manipulation and disinformation. Through a qualitative-documentary review of academic programs and case studies (Ukraine, Taiwan, Israel), it identifies critical training gaps in social sciences, media literacy, and cognitive defense. The study proposes an integrated educational model that merges technical skills with narrative analysis, political communication, and mass psychology. One effective cybersecurity requires interdisciplinary, hybrid professionals capable of protecting not only systems but also democratic resilience and epistemic trust.

PALABRAS CLAVE
Ciberseguridad
Desinformación
Educación universitaria
Amenazas híbridas
Formación interdisciplinar
Manipulación psicológica
Guerra cognitiva

RESUMEN
Este artículo analiza la creciente brecha entre la formación universitaria en ciberseguridad y las exigencias de las amenazas híbridas, que combinan ataques técnicos con manipulación psicológica y desinformación. Mediante una revisión cualitativo-documental de programas académicos y estudios de caso (Ucrania, Taiwán, Israel), se identifican vacíos críticos en ciencias sociales, alfabetización mediática y defensa cognitiva. Se propone un modelo educativo integrado que combine competencias técnicas con análisis narrativo, comunicación política y psicología de masas. Una ciberseguridad eficaz requiere profesionales interdisciplinares e híbridos, capaces de proteger no solo sistemas, sino también la resiliencia democrática y la confianza epistémica.

Recibido: 19 / 03 / 2026
Aceptado: 23 / 06 / 2026

1. Introducción

El panorama de la ciberseguridad está experimentando una transformación radical. Ya no nos enfrentamos únicamente a ataques técnicos convencionales, sino a un ecosistema complejo donde la tecnología se entrelaza con sofisticadas estrategias de manipulación psicológica y desinformación a gran escala (NATO, 2022). Este fenómeno multidimensional, denominado «amenazas híbridas», representa un punto de inflexión que exige un replanteamiento fundamental de cómo formamos a los profesionales encargados de proteger nuestros sistemas e infraestructuras críticas.

La velocidad a la que evolucionan estas amenazas ha dejado obsoletos muchos enfoques educativos tradicionales, creando una brecha peligrosa entre las competencias que se enseñan en las aulas y las habilidades que realmente se necesitan en el campo profesional. Según el Global Cybersecurity Index (2023), el 65% de las organizaciones a nivel mundial reconocen no contar con personal suficientemente preparado para estos nuevos desafíos híbridos.

La naturaleza cambiante de las amenazas digitales se ha vuelto particularmente evidente en el contexto de los recientes conflictos geopolíticos. La guerra en Ucrania, por ejemplo, ha servido como un laboratorio a escala real donde hemos observado cómo las campañas de desinformación masiva, coordinadas con ciberataques a infraestructuras críticas, pueden tener un impacto devastador en la estabilidad social y política de una nación. Estos eventos han demostrado de manera incontrovertible que ya no es posible separar los aspectos técnicos de los psicológicos y sociales cuando hablamos de seguridad digital.

Sin embargo, al examinar los programas de formación actuales en ciberseguridad, encontramos que la gran mayoría sigue anclada en paradigmas educativos obsoletos, donde los aspectos humanos y cognitivos de la seguridad son tratados como complementos marginales o, en muchos casos, simplemente ignorados. Esta desconexión entre la realidad de las amenazas y los contenidos formativos se ha convertido en uno de los principales factores de vulnerabilidad en el panorama de seguridad global.

El desafío que enfrenta la formación de especialistas es doble y paradójico. Por un lado, debe mantener el ritmo de los avances tecnológicos exponenciales, incorporando conocimientos sobre inteligencia artificial aplicada a la seguridad, análisis de deepfakes y protección contra ciberataques automatizados. Por otro lado, y esto es quizás lo más revolucionario, debe integrar de manera orgánica enfoques multidisciplinarios que permitan a los futuros profesionales comprender y contrarrestar estrategias de influencia maliciosa que operan en la intersección entre tecnología y psicología humana (UNESCO, 2023).

Esta necesidad se hace especialmente evidente al analizar datos como los recogidos por Cybersecurity Ventures (2024), que revela que el 78% de los profesionales en ciberseguridad no han recibido formación específica en identificación de campañas de desinformación, mientras que el 89% de las brechas de seguridad más costosas del último año tuvieron como componente principal la manipulación psicológica de los usuarios (IBM Security, 2023).

La situación se agrava al examinar las certificaciones profesionales más reconocidas. Un análisis del Instituto de Ciberseguridad de España (2023) reveló que menos del 5% de los módulos de certificaciones como CISSP, CEH o CompTIA Security+ abordan temas relacionados con la desinformación o la guerra cognitiva. Esta carencia formativa tiene consecuencias directas: según ENISA (2023), el 63% de las organizaciones afectadas por campañas híbridas reconocieron que sus equipos de seguridad no estaban preparados para identificar y contrarrestar los componentes no técnicos de estos ataques.

El problema trasciende lo académico para convertirse en una cuestión de seguridad nacional. Como señala el Departamento de Seguridad Nacional de Estados Unidos (2023), la escasez de profesionales capacitados para enfrentar amenazas híbridas representa uno de los principales riesgos para la estabilidad democrática en la era digital.

La desconexión entre formación y realidad profesional se manifiesta también en los planes de estudio universitarios. Una investigación reciente de la Asociación Europea de Ciberseguridad (2024) que analizó 120 programas de grado y posgrado en 35 países encontró que solo el 12% incluía asignaturas específicas sobre guerra cognitiva o desinformación. Esta situación contrasta

dramáticamente con las necesidades del sector empresarial: en una encuesta a 500 directores de seguridad informática en Europa y América, el 92% consideró que las habilidades para identificar y mitigar riesgos psicosociales en entornos digitales serán «críticas» en los próximos cinco años (Foro Económico Mundial, 2023).

Esta problemática adquiere dimensiones especialmente preocupantes al considerar el papel creciente de la inteligencia artificial en la generación y amplificación de amenazas híbridas. Los avances en sistemas de generación de lenguaje natural han reducido dramáticamente la barrera de entrada para crear campañas de desinformación sofisticadas. Sin embargo, la formación en técnicas para identificar y contrarrestar este tipo de amenazas basadas en IA brilla por su ausencia en la mayoría de los currículos actuales (MIT Technology Review, 2023).

El presente artículo busca analizar críticamente esta situación desde una perspectiva multidimensional, examinando no solo las deficiencias de los modelos educativos vigentes, sino también proponiendo estrategias innovadoras basadas en las mejores prácticas internacionales. Partimos de la premisa de que formar especialistas capaces de enfrentar los desafíos del entorno digital actual requiere una reimaginación fundamental de lo que significa educar en seguridad de la información.

Los objetivos de esta investigación se centran en abordar de manera integral la crisis formativa que actualmente enfrenta el campo de la ciberseguridad en relación con las amenazas híbridas contemporáneas.

En primer lugar, resulta fundamental evaluar con rigor científico la adecuación real de los programas académicos y certificaciones profesionales existentes para enfrentar los desafíos que plantea este nuevo paradigma de seguridad digital. Este análisis debe extenderse más allá de los contenidos declarados para examinar las metodologías pedagógicas empleadas, los perfiles del profesorado, y la forma en que estas competencias son evaluadas y validadas en los procesos de certificación profesional.

El segundo objetivo busca identificar de manera precisa y documentada las principales brechas formativas que limitan la capacidad de los profesionales de ciberseguridad para enfrentar amenazas híbridas. Esto implica desarrollar un análisis comparativo exhaustivo de planes de estudio de instituciones de educación superior líderes en diferentes regiones del mundo, prestando especial atención a la desconexión entre las necesidades expresadas por las organizaciones y las competencias que realmente desarrollan los programas formativos.

El tercer y más ambicioso objetivo consiste en desarrollar y proponer un modelo educativo integrado que supere las limitaciones de los enfoques actuales. Este modelo debe articularse como un marco coherente donde habilidades tradicionales de ciberseguridad se combinen orgánicamente con conocimientos avanzados en ciencias sociales, comunicación estratégica y análisis político. El desafío es diseñar un enfoque pedagógico que permita a los profesionales entender y anticipar cómo los actores maliciosos explotan la intersección entre vulnerabilidades técnicas y debilidades humanas.

Estos tres objetivos se complementan con una visión transversal que busca sentar las bases para una transformación más amplia en cómo concebimos la formación en seguridad digital. Un resultado clave será proporcionar a instituciones educativas, organismos certificadores y responsables políticos herramientas concretas para rediseñar sus programas formativos. La ambición última es contribuir a formar una nueva generación de profesionales de ciberseguridad que no solo sean expertos en proteger sistemas sino también en defender sociedades frente a las sofisticadas amenazas híbridas del siglo XXI.

2. Metodología

Este estudio adopta un enfoque cualitativo-documental para analizar la formación en ciberseguridad frente a amenazas híbridas. Combina tres estrategias:

Revisión sistemática de 22 programas formativos (grados y posgrados de disciplinas técnicas y también de las ciencias sociales) de Europa, América y Asia (2020-2024), evaluando competencias transversales como alfabetización mediática y gestión de crisis.

Análisis de estudios de caso paradigmáticos: campañas de desinformación en Ucrania (2022-2023) y Taiwán (2024) y el uso del *software* Pegasus, examinados mediante triangulación de informes de inteligencia, académicos y medios.

Integración de hallazgos mediante análisis comparativo constante, contrastando la oferta educativa con las exigencias operativas reales.

Se identificaron vacíos formativos críticos en psicología, sociología y comunicación política, ausentes en la mayoría de los currículos técnicos. La metodología busca no solo diagnosticar brechas, sino también contribuir a un marco formativo flexible que integre capacidades técnicas y humanas para enfrentar amenazas híbridas complejas.

3. Resultados

Israel se ha consolidado como uno de los actores más influyentes en el ámbito de la ciberseguridad y las amenazas híbridas, no solo por su innovación tecnológica, sino por su integración estratégica entre capacidades técnicas y operaciones psicológicas.

Un ejemplo paradigmático es el *software* espía Pegasus, desarrollado por la empresa NSO Group, que ha sido utilizado en múltiples países para espiar a periodistas, defensores de derechos humanos y líderes políticos. Este caso ilustra cómo las herramientas tecnológicas pueden ser empleadas para la manipulación y control social, trascendiendo su función defensiva. Además, Israel cuenta con un ecosistema cibernético fuertemente articulado con su aparato militar e inteligencia, en particular a través de unidades como la 8200, especializada en ciberinteligencia y guerra electrónica. Desde allí, se han impulsado tácticas que combinan vigilancia masiva con desinformación en redes sociales, manipulación de flujos informativos y explotación de vulnerabilidades cognitivas. Estas estrategias han sido documentadas en conflictos como el palestino-israelí, pero también exportadas a través de empresas tecnológicas y servicios de consultoría. El caso israelí, por tanto, no solo ofrece un modelo avanzado de defensa digital, sino también una alerta sobre los riesgos éticos, democráticos y educativos de militarizar la información en contextos civiles y globales.

Por otro lado, Ucrania y Taiwán representan dos escenarios clave para entender cómo evolucionan las amenazas híbridas y la importancia de una formación adecuada en ciberseguridad. En el caso ucraniano, desde 2014 y con especial intensidad desde la invasión rusa de 2022, se ha observado una sofisticada combinación de ciberataques técnicos (como ataques DDoS y malware destructivo) con campañas masivas de desinformación destinadas a desmoralizar a la población y socavar la legitimidad del gobierno. Rusia ha explotado tanto infraestructuras digitales como narrativas culturales, difundiendo noticias falsas, manipulando redes sociales y segmentando mensajes según grupos étnicos y geográficos. Esto ha convertido a Ucrania en un laboratorio geopolítico de guerra cognitiva.

Taiwán, por su parte, enfrenta una presión constante de China mediante campañas digitales que buscan erosionar la confianza ciudadana en las instituciones democráticas. Las operaciones incluyen la difusión de rumores sobre figuras políticas, la generación de contenido falso automatizado y la explotación de conflictos sociales internos. A diferencia de Ucrania, Taiwán ha invertido en alfabetización mediática y ciber-resiliencia ciudadana, promoviendo modelos colaborativos entre Estado, academia y sociedad civil. Ambos casos subrayan que la defensa digital no se limita al plano técnico sino que exige capacidades críticas, éticas y comunicativas que deben incorporarse en la formación universitaria de futuros especialistas.

Los resultados del análisis revelan una desconexión preocupante entre la formación universitaria actual y las competencias necesarias para hacer frente a las amenazas híbridas que caracterizan el entorno digital contemporáneo. En el contexto de carreras como ciencias políticas, sociología, psicología, informática o periodismo, la ciberseguridad continúa siendo abordada desde perspectivas aisladas, con poca integración entre disciplinas y sin una visión integral de las nuevas formas de agresión que enfrentan tanto los Estados como la sociedad civil.

En facultades de informática, por ejemplo, el énfasis sigue estando en aspectos técnicos como redes, criptografía o defensa perimetral, pero rara vez se incluye formación sobre ingeniería social, manipulación algorítmica o desinformación estratégica. A pesar de que estas tácticas

están siendo cada vez más utilizadas en campañas híbridas, las universidades no han actualizado sus planes de estudio con la urgencia que el contexto requiere.

En ciencias sociales y humanidades, como sociología o ciencias políticas, ocurre lo inverso: se abordan teorías sobre poder, conflicto, comunicación política o cohesión social, pero rara vez se introducen herramientas concretas para analizar ciberataques, bots, *deepfakes* o campañas de guerra cognitiva. La psicología, pese a ser fundamental para comprender la manipulación emocional o la vulnerabilidad cognitiva, aún no se articula sistemáticamente con los enfoques técnicos de la ciberseguridad.

En el caso del periodismo, la alfabetización digital ha ganado relevancia en los últimos años, pero sigue centrada en el combate a las fake news de forma superficial, sin profundizar en métodos de detección automatizada, análisis de redes de desinformación o protocolos de verificación avanzados que podrían integrarse desde la ciberseguridad crítica.

Además, el estudio documental reveló que menos del 20% de las universidades analizadas promueven la colaboración interdisciplinaria en sus programas de ciberseguridad. Esta falta de integración refuerza una formación fragmentada que no responde adecuadamente a la naturaleza multifacética de las amenazas híbridas.

Casos como los de Ucrania, Israel y Taiwán demuestran que los ataques más eficaces combinan vulnerabilidades técnicas con estrategias de manipulación narrativa. Las principales consecuencias abordadas muestran que la formación de especialistas debería ser repensada desde un enfoque transversal, donde el código y el discurso se enseñen como dimensiones interconectadas de la seguridad contemporánea.

4. Discusión

La formación de especialistas en ciberseguridad se encuentra en un momento de inflexión crítica. Lo que durante años fue considerado un campo técnico, reservado a ingenieros informáticos y expertos en redes, hoy se revela como una disciplina profundamente interdisciplinaria, que demanda la incorporación urgente de conocimientos provenientes de las ciencias sociales, la psicología, la comunicación y hasta el periodismo. Las amenazas híbridas no pueden enfrentarse únicamente con firewalls y cifrado. Requieren, además, profesionales capaces de leer contextos, analizar discursos, interpretar comportamientos digitales y anticipar las dinámicas narrativas que configuran la opinión pública.

En las universidades, sin embargo, persiste un desfase importante. Facultades como informática o ingeniería en computación siguen centrando su enseñanza en herramientas técnicas como lenguajes de programación, auditoría de sistemas o criptografía, sin integrar contenidos sobre cómo se construyen y diseminan las noticias falsas, cómo operan los bots o qué papel juega el sesgo algorítmico en la radicalización digital. En el otro extremo, carreras como ciencias políticas, periodismo o psicología abordan temas como manipulación mediática, teoría de la propaganda o psicología del miedo, pero sin ningún tipo de articulación con la seguridad digital o los sistemas de detección de ataques informáticos. Esa fragmentación del conocimiento impide la formación de perfiles híbridos, precisamente los más necesarios en un entorno donde la seguridad ya no es sólo técnica, sino también simbólica, perceptiva y política.

Uno de los puntos más débiles es la casi nula colaboración entre facultades. Muy pocas universidades han logrado romper los compartimentos estancos entre departamentos. La ciberseguridad sigue tratándose como una especialidad informática, sin la participación activa de docentes e investigadores en comunicación, sociología, semiótica o ciencia política. Esta separación es especialmente problemática si se considera que las amenazas más efectivas de los últimos años no han sido puramente técnicas sino aquellas que afectaron la percepción colectiva: operaciones de influencia electoral, campañas de odio, manipulación emocional masiva mediante memes, y construcción de narrativas polarizantes que fragmentan la cohesión social (Vargas, 2023: 129). Todos estos fenómenos exigen una mirada crítica, holística y multidimensional, algo que el actual modelo de formación no garantiza.

En este panorama, países como Estonia y Finlandia marcan una diferencia importante. Estonia, con una experiencia histórica directa frente a ciberataques y guerra informativa, ha

integrado desde hace años contenidos de historia política, alfabetización mediática y pensamiento estratégico en sus programas de ciberseguridad. No se trata solamente de enseñar a defenderse de un ataque, sino de entender por qué, cómo y con qué objetivos un actor geopolítico decide manipular una narrativa pública. Finlandia, por su parte, ha impulsado programas conjuntos entre psicología, ciencia política e informática. La Universidad de Jyväskylä, por ejemplo, ofrece módulos interdisciplinares donde se analiza cómo las emociones y los sesgos cognitivos influyen en la propagación de desinformación, combinando este análisis con talleres prácticos de defensa digital.

Estos modelos son mucho más avanzados que otras universidades como las de América Latina, donde la formación en ciberseguridad suele limitarse a cursos técnicos desconectados del contexto social, político o comunicacional. Incluso en países con buena infraestructura académica como Estados Unidos, se observa una «rigidez epistemológica» que impide renovar los programas ante amenazas como el cognitive hacking o el uso de IA para la manipulación masiva. Se enseña a los estudiantes a proteger servidores pero no a detectar un video falso viralizado con fines políticos; se les forma en protocolos de seguridad, pero no en semiótica digital ni en análisis de propaganda. Este déficit académico está dejando al mundo con profesionales altamente capacitados en lo técnico, pero sin recursos en lo narrativo, lo simbólico y lo emocional.

Otro problema detectado es la desconexión entre la academia y el sector productivo. Empresas tecnológicas, bancos, medios de comunicación y hasta organismos del Estado necesitan hoy profesionales que sepan leer el impacto de una campaña de desinformación, analizar patrones de manipulación narrativa o colaborar con áreas de comunicación institucional, pero los graduados de carreras técnicas muchas veces carecen de estas habilidades, mientras que quienes las poseen (por ejemplo, periodistas o sociólogos) no tienen la formación necesaria para operar en contextos de ciberdefensa o seguridad informática. El resultado es un vacío de capacidades que se traduce en respuestas fragmentarias e ineficaces frente a amenazas híbridas.

El reto no está solamente en ampliar los contenidos curriculares sino en repensar completamente cómo se estructura la formación. La ciberseguridad no puede ser una especialización técnica marginal sino una competencia transversal. Así lo ha planteado incluso el Foro Económico Mundial, que propone introducir módulos básicos de seguridad digital y alfabetización mediática en todas las disciplinas universitarias, desde las humanidades hasta la economía. La lógica es simple: vivimos en una sociedad digitalizada, donde cualquier ciudadano, independientemente de su campo profesional, puede ser blanco o canal de una campaña de manipulación. Por tanto, la ciberseguridad debe ser parte del conocimiento general, no exclusivo de unos pocos especialistas.

Además, la dependencia de certificaciones tradicionales como CISSP o CEH también debe revisarse. Estas credenciales, aunque útiles, están orientadas a un paradigma de seguridad centrado en la infraestructura, no en la información ni en la percepción. Sus contenidos rara vez abordan las nuevas formas de ataque centradas en el relato, el miedo o la desinformación emocional. Se requiere crear nuevas certificaciones dinámicas, adaptadas a un entorno donde la frontera entre lo técnico y lo comunicacional se ha difuminado por completo.

También preocupa la falta de formación en pensamiento crítico, ética de los datos y análisis contextual. En muchos casos, los profesionales en ciberseguridad dependen exclusivamente de herramientas automáticas para detectar fake news o discursos tóxicos, sin la capacidad de interpretar adecuadamente los matices culturales, políticos o ideológicos de la información. Esto los hace vulnerables a errores graves, especialmente en contextos multilingües o culturalmente complejos, donde los algoritmos fallan con frecuencia. No se trata sólo de tener herramientas sino de saber cuándo y cómo usarlas, algo que requiere criterio humano, formación filosófica y sensibilidad contextual.

Finalmente, la formación actual adolece también de un grave problema de representación. Las aulas de ciberseguridad siguen estando pobladas mayoritariamente por hombres, blancos y de clase media, dejando fuera a mujeres, personas indígenas, afrodescendientes o LGBTQ+. Esta falta de diversidad no sólo limita la innovación sino que reduce la capacidad de entender y

responder a las distintas formas que puede asumir la violencia digital como el acoso, el discurso de odio o la censura dirigida. Formar profesionales diversos es, por tanto, una cuestión de eficacia tanto como de justicia social.

Así, la discusión sobre la formación en ciberseguridad no puede reducirse a actualizar herramientas técnicas o a agregar un módulo más sobre redes sociales. Se trata de un cambio profundo en cómo entendemos la seguridad digital: como un fenómeno técnico, sí, pero también como uno simbólico, emocional, narrativo y político. Necesitamos aulas que formen a quienes sepan programar firewalls y también leer discursos; que entiendan la criptografía y también la psicología de masas; que puedan colaborar con expertos en redes y también con periodistas o analistas políticos. La formación en ciberseguridad requiere, por tanto, un cambio de paradigma epistemológico. Como afirma Pacheco (2024), «la defensa digital contemporánea no es solo cuestión de proteger dispositivos sino de comprender narrativas, interpretar símbolos y anticipar escenarios». Esta visión implica superar la compartimentalización del conocimiento y adoptar un enfoque sistémico, complejo y orientado a la solución de problemas sociales. Necesitamos profesionales capaces de pensar como ingenieros y como sociólogos, como hackers y como periodistas, como criptógrafos y como antropólogos digitales.

Los modelos de Finlandia y Estonia muestran que este cambio es posible. Y también necesario. Visto lo anterior, si no transformamos nuestros planes de estudio, seguiremos formando profesionales que no comprenden las amenazas que enfrentamos hoy. No hacerlo implica no solo mantener la brecha de capacidades, sino ampliar la vulnerabilidad estructural de nuestras sociedades ante un entorno digital cada vez más hostil y sofisticado.

5. Conclusiones

La transformación del entorno digital global, marcada por la convergencia entre tecnología y manipulación psicológica, exige repensar desde sus cimientos la manera en que se forma a los especialistas en ciberseguridad. Este estudio, en su conjunto, no sólo ha puesto en evidencia una brecha crítica entre la formación existente y las necesidades reales del contexto contemporáneo sino que también ha mostrado que esta deficiencia no es simplemente un problema técnico o curricular. Es, en realidad, una expresión profunda de cómo las instituciones educativas, los marcos de certificación profesional y los sistemas de conocimiento hegemónico continúan operando bajo un modelo analítico inadecuado para una realidad caracterizada por la hibridez, la complejidad y la mutabilidad constante.

El dato de que menos del 20% de los programas académicos incluyan módulos relacionados con la desinformación, la guerra cognitiva o la IA aplicada a la manipulación informativa no es sólo alarmante por lo que significa en términos de contenido sino por lo que revela en términos de prioridades epistémicas. La ciberseguridad sigue anclada en una visión técnica, casi maquinal, de la amenaza. Se enseña a detectar malware, a proteger redes, a asegurar dispositivos, pero no a entender cómo se infiltran ideas, cómo se viralizan los odios, cómo se inoculan narrativas tóxicas que erosionan la confianza social y desestabilizan democracias desde dentro. Es como si formáramos a médicos para diagnosticar síntomas pero no para entender patologías complejas o contextuales.

La guerra híbrida no es sólo un fenómeno bélico. Es un fenómeno político, comunicativo, psicológico, económico y tecnológico a la vez y por tanto, no puede ser abordado con herramientas unidimensionales. En este punto, se vuelve imprescindible un cambio de enfoque. No una asignatura optativa sino una reconceptualización radical de lo que significa hoy formar a un especialista en ciberseguridad. Este especialista no puede ser, ya no, un mero tecnólogo sino también un lector crítico del discurso, un analista del comportamiento colectivo, un observador de los climas emocionales que se incuban en redes sociales y que luego se traducen en decisiones políticas, en rechazos sociales, en odios virales, en estallidos informacionales o incluso en guerras. Tal como apunta Bellingcat, muchos de los conflictos contemporáneos comienzan con memes antes que con misiles, con campañas de hashtags antes que con movimientos de tropas.

Los casos de Ucrania, Israel y Taiwán, así como otros conflictos de menor visibilidad mediática como las campañas de desinformación sobre vacunas en América Latina o las narrativas antiinmigración viralizadas en Europa del Este, han mostrado que el verdadero poder desestabilizador no radica ya en los ataques a infraestructuras físicas sino en la erosión de las infraestructuras cognitivas de las sociedades: confianza, consenso, memoria colectiva, sentido compartido de realidad. Esto redefine completamente la noción misma de «seguridad». Ya no se trata sólo de mantener a salvo servidores o líneas de código sino de proteger ecosistemas epistémicos y esa misión requiere especialistas formados para leer entre líneas, para entender los juegos de poder simbólico que operan detrás de un mensaje aparentemente inofensivo o de una cuenta anónima que lanza desinformación gota a gota, hasta modificar percepciones masivas.

Zuboff ya advertía de que el capitalismo de vigilancia no sólo explota datos sino que modela subjetividades. En ese sentido, la ciberseguridad debe dejar de entenderse como una defensa técnica y empezar a asumirse como un proceso de resistencia cultural y política. Esto implica incluir en los planes de formación lecturas de teoría crítica, análisis del poder mediático, historia de la propaganda, fundamentos de semiótica digital, epistemología algorítmica y teoría de la mente, porque no se puede defender lo que no se comprende y no se puede comprender el ataque híbrido si se lo sigue pensando como una anomalía técnica y no como una estrategia racional y sofisticada de manipulación psico-informacional.

El desfase entre las certificaciones profesionales actuales y las capacidades necesarias también se vuelve cada vez más evidente. Certificaciones como CISSP o CEH, que gozan aún de gran prestigio internacional, se enfocan en contenidos estáticos, como si los entornos de amenaza fueran lineales, predecibles, estandarizados. Las amenazas híbridas mutan en tiempo real, utilizan IA generativa para producir contenido hiperrealista, y se articulan con ciclos de polarización política que las vuelven aún más virales. En este contexto, los profesionales certificados que no hayan sido formados en el análisis crítico de narrativas, en la ética de la IA o en la psicología de masas, simplemente carecen de herramientas cognitivas. La ciberseguridad necesita salir de su zona de confort técnico y empezar a operar en el terreno resbaladizo del conflicto informacional. Aquí es donde la interdisciplinariedad ya no es un ideal académico abstracto sino una necesidad operativa. Necesitamos antropólogos digitales trabajando junto a ingenieros en seguridad de redes. Necesitamos politólogos colaborando con expertos en *machine learning*. Necesitamos psicólogos sociales capaces de diseñar estrategias de resiliencia comunitaria ante campañas de desinformación. Y necesitamos, sobre todo, que las universidades reconozcan que ya no es posible formar profesionales para un mundo compartimentado cuando el mundo real es sistémico, interconectado y altamente no lineal.

Autores como Castells han descrito con claridad cómo las redes de información reconfiguran el poder. Y si el poder se ha desplazado al campo de las redes, entonces la formación en seguridad debe aprender también a leer el poder allí donde se manifiesta: en las imágenes virales, en los discursos emocionales que apelan al miedo, en las cámaras de eco que refuerzan el sesgo, en los algoritmos que jerarquizan qué vemos y qué no. La alfabetización en ciberseguridad debe incluir, por tanto, no sólo el conocimiento de cómo funcionan los ataques sino de por qué funcionan; qué deseos, qué miedos, qué pulsiones colectivas explotan y qué narrativas subterráneas los hacen eficaces.

Otro elemento central es la actualización continua. Las universidades y centros de formación deben abandonar la idea de currículo fijo. La ciberseguridad híbrida es, por definición, volátil. Los contenidos que eran útiles hace dos años hoy pueden ser irrelevantes o incluso contraproducentes. Las tácticas de manipulación informativa se transforman cada semana. Los vectores de ataque se sofistican a medida que se desarrollan nuevas tecnologías de síntesis de voz, animación facial, metadatos falsificados. Si la formación no es adaptable, simplemente no es útil. Y esto también exige una transformación institucional: procesos de evaluación más ágiles, incorporación constante de expertos en activo, alianzas con centros de monitoreo en tiempo real y, especialmente, una pedagogía centrada en la resolución de problemas reales, no en la memorización de protocolos.

La resistencia institucional al cambio también debe ser nombrada. En muchos casos, los currículos se mantienen no por convicción sino por inercia. Detrás de esa inercia hay burocracia, hay acreditaciones, hay miedo al riesgo. También hay una concepción anticuada de la educación como transmisión vertical de conocimientos, en lugar de como espacio de experimentación colaborativa y aprendizaje situado. Formar para la ciberseguridad híbrida requiere entornos de enseñanza abiertos donde se simulen crisis reales, donde los estudiantes debatan dilemas éticos, donde se pongan a prueba soluciones interdisciplinares y donde el error sea parte del proceso formativo.

No se trata sólo de contenidos. Se trata de una pedagogía crítica, activa, comprometida con la realidad. Porque si los profesionales de ciberseguridad no están entrenados para cuestionar el discurso dominante, para reconocer la manipulación, para resistir la presión informativa, no habrá tal conocimiento completo. En la era de la manipulación cognitiva, el profesional de ciberseguridad debe ser también un defensor del pensamiento libre, un garante de la verdad como bien público, un actor consciente de las batallas simbólicas que se libran en el ciberespacio.

La investigación aquí presentada muestra que la importancia de la formación en ciencias sociales para anticipar escenarios de conflicto híbrido, para comprenden mejor los indicadores tempranos de radicalización, saber identificar dinámicas de grupo peligrosas, y poder colaborar más eficazmente con equipos multidisciplinares en la gestión de crisis. Métodos como la etnografía digital, el análisis del discurso o la cartografía narrativa deben ocupar un lugar central en los programas de formación, en un equilibrio entre el conocimiento de cómo se ataca un sistema como de saber por qué se ataca una comunidad, cómo se seleccionan sus símbolos o cómo se infiltra su lenguaje.

En este sentido, la ciberseguridad híbrida no es solo una disciplina técnica sino una praxis política. Es el lugar donde se cruza la protección del dato con la defensa de la democracia. Es, en el fondo, una forma de anticipación estratégica que combina vigilancia tecnológica con sensibilidad social. Formar a quienes ejercerán esta función requiere mucho más que enseñar protocolos. Requiere cultivar pensamiento crítico, visión sistémica, sensibilidad cultural y capacidad de actuar en contextos inciertos.

De no hacerlo, las democracias corren un alto riesgo de debilitarse desde dentro, de ser víctimas de ataques que no se ven pero que funcionan. La polarización se volverá norma, con sistemas educativos que seguirán produciendo profesionales altamente certificados pero profundamente ineficaces para el mundo real. Como advirtió Snowden en una entrevista de 2023: «El mayor riesgo ya no es que hackeen tus sistemas sino que hackeen tu percepción de la realidad».

Las instituciones que deseen formar especialistas verdaderamente útiles para el siglo XXI deben dejar de pensar en planes de estudio como recetas y empezar a concebirlos como laboratorios vivos. Necesitamos formar ciudadanos-tecnólogos, críticos y creativos, capaces de entender el poder tanto en su dimensión técnica como en su dimensión narrativa. La defensa digital ya no puede separarse del debate cultural. Y el especialista en ciberseguridad no puede seguir siendo una figura encerrada en su terminal, ajena a los flujos sociales que dan sentido a las amenazas.

Al final encontramos que la ciberseguridad del futuro será híbrida, o no será. Y para que exista, necesitamos formar personas que piensen como ingenieros, pero también como analistas del discurso, como estrategas sociales, como defensores de lo común. Solo así será posible construir una cultura de seguridad digital que no se limite a resistir ataques sino que promueva una ciudadanía informada, crítica y resiliente frente a las nuevas formas de poder que circulan por los circuitos invisibles de la red.

6. Agradecimientos

El presente texto nace en el marco del primer doctorado defendido en la Universidad Complutense de Madrid en 2016 titulado «El análisis de contenido del proteccionismo en la campaña electoral de Francia de 2012».

Referencias

Bellingcat. (2024). *Digital disinformation in modern conflicts*. https://www.bellingcat.com

Castells, M. (2021). *La sociedad red: Una visión global*. Alianza Editorial.

Departamento de Seguridad Nacional de EE.UU. (2023). *Estrategia nacional contra amenazas híbridas*. https://www.dhs.gov

European Union Agency for Cybersecurity (ENISA). (2023). *Hybrid threats and cybersecurity education: Trends and gaps*. https://www.enisa.europa.eu

Foro Económico Mundial. (2023). *Informe global de riesgos 2023*. https://www.weforum.org

Global Cybersecurity Index. (2023). *Medición de capacidades nacionales en ciberseguridad*. Unión Internacional de Telecomunicaciones.

Goldstein, J. A., DiResta, R., Sastry, G., Musser, M., Gentzel, M., & Sedova, K. (2023). *Generative language models and automated influence operations: Emerging threats and potential mitigations*. Stanford Internet Observatory, OpenAI, & Georgetown University Center for Security and Emerging Technology. https://cyber.fsi.stanford.edu/io/publication/generative-language-models-and-automated-influence-operations-emerging-threats-and

IBM Security. (2023). *Cost of a data breach report 2023*. https://www.ibm.com/security

Instituto de Ciberseguridad de España. (2023). *Estándares para certificaciones profesionales*. https://www.incibe.es

MIT Technology Review. (2023). *Generative AI as a tool for disinformation*. https://www.technologyreview.com

NATO Strategic Communications Centre of Excellence. (2022). *Cognitive security framework*. https://www.stratcomcoe.org

OECD. (2023). *Digital education outlook 2023.* OECD Publishing.

Pacheco, F. (2024). Hacia una ciberseguridad integral: divergencias y puentes entre los enfoques de la academia, la industria y la comunidad hacker. Revis*ta Latinoamericana de Economía y Sociedad Digital, Issue Especial 2*. https://doi.org/10.53857/RLESD.04.2023.03

Vargas, E. S. (2023). El impacto de las Tecnologías de la Información en el reciente auge de las extremas derechas. En M. J. Vicente Vicente (Ed.), L*as nuevas extremas derechas en el mundo* (pp. 129-150). Editorial Tirant Lo Blanch.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.