Preparación de Artículos revista Vínculos: Ciencia, Tecnología y Sociedad
Fecha de envío: 11/08/2025
Fecha de recepción: 17/10/2025
Fecha de aceptación: 10/11/2025

REEVALUACIÓN DEL MODELO CYBER KILL CHAIN EN LA ERA DE AMENAZAS NO LINEALES Y DOMINIOS EMERGENTES

REASSESSING THE CYBER KILL CHAIN MODEL IN THE ERA OF NONLINEAR THREATS AND EMERGING DOMAINS

Robinson Stiven Inagan Ochoa, Sergio Daniel Mejía Carvajal, Juan Esteban Sáenz Lara, Johan Orduz Esteban Gutierrez.

Resumen:

Este artículo presenta una revisión crítica y multidimensional del modelo Cyber Kill Chain (CKC) en el contexto actual de amenazas cibernéticas no lineales y multidominio. Se analizan sus limitaciones estructurales frente a ataques modernos, su integración con marcos como MITRE ATT&CK y teoría de juegos, y se propone su evolución hacia arquitecturas adaptativas e interoperables. El estudio se apoya en evidencia empírica y conceptual, considerando además implicaciones éticas, normativas y operativas relacionadas con la inteligencia artificial y el uso de OSINT. Como resultado, se demuestra que el CKC, aunque insuficiente por sí solo, conserva valor analítico cuando se enriquece con herramientas contemporáneas. Se identifican líneas de investigación orientadas a su automatización, formalización y adecuación a escenarios emergentes como UAVs, IoT y guerra cognitiva. Esta evaluación busca contribuir a una ciberdefensa técnica, ética y resiliente.

Palabras clave: Cyber Kill Chain, ciberseguridad, inteligencia artificial, OSINT, ATT&CK, ética algorítmica.

Abstract:

This article presents a critical and multidimensional reassessment of the Cyber Kill Chain (CKC) model within the current landscape of nonlinear, multidomain cyber threats. The paper

analyzes its structural limitations against modern attacks, explores its integration with frameworks such as MITRE ATT&CK and game theory, and proposes its evolution toward adaptive and interoperable architectures. The study is grounded in empirical and theoretical evidence, also addressing ethical, regulatory, and operational implications associated with artificial intelligence and OSINT. Findings demonstrate that while CKC is insufficient as a standalone model, it retains analytical value when augmented with contemporary tools. Future research directions include automation, formalization, and adaptation of the model for emerging contexts such as UAVs, IoT, and cognitive warfare. This evaluation aims to contribute to a technically sound, ethically guided, and resilient approach to cyber defense.

Keywords: Cyber Kill Chain, cybersecurity, artificial intelligence, OSINT, ATT&CK, algorithmic ethics.

1. Introducción

El modelo Cyber Kill Chain (CKC), propuesto por Lockheed Martin en 2011 [1], constituye una de las bases doctrinales más ampliamente aceptadas en ciberseguridad para el análisis y detección de ataques. Diseñado originalmente para estructurar las fases de un ciberataque desde una perspectiva ofensiva-defensiva, el CKC descompone la intrusión en siete fases: Reconocimiento, Armamento, Entrega, Explotación, Instalación, Comando y Control (C2), y Acciones sobre el Objetivo. Esta representación secuencial ha servido como pilar para diseñar estrategias defensivas proactivas, priorizar alertas en sistemas SIEM, y desarrollar respuestas incidentales coordinadas. De hecho, revisiones sistemáticas recientes confirman su eficacia y continua aplicación como una herramienta estratégica para la defensa empresarial, lo que justifica una reevaluación de sus capacidades en lugar de su descarte [24]. Sin embargo, la aparición de actores con capacidades de inteligencia artificial, el uso de arquitecturas de ataque no lineales, y la inclusión de nuevos dominios operacionales como el espacio ultraterrestre, los

enjambres de UAVs y el ecosistema IoT, ponen en cuestión la suficiencia del CKC como único modelo operativo. En esta revisión técnica se propone una reevaluación de su aplicabilidad, incorporando análisis desde marcos emergentes como ATT&CK, teoría de juegos, y modelos probabilísticos adaptativos, con el fin de mejorar su capacidad predictiva y su resiliencia en entornos dinámicos y multidominio.

2. Fundamentos Teóricos y Estado del Arte

2.1 Orígenes del Modelo Cyber Kill Chain

La concepción del Cyber Kill Chain (CKC) está directamente inspirada en doctrinas de combate militar estadounidenses, específicamente en el concepto de "kill chain" desarrollado para operaciones cinéticas, donde la identificación, localización, seguimiento y destrucción del objetivo constituyen fases secuenciales de una operación bélica [1]. Lockheed Martin, al extrapolar esta lógica al dominio cibernético, estructuró el CKC como una herramienta metodológica que permitiera a los analistas identificar, interrumpir o mitigar un ciberataque en curso. En el ámbito doctrinal, el CKC fue rápidamente acogido por organismos como el Departamento de Defensa (DoD), la NSA y el NIST, incorporándose a guías y marcos normativos sobre ciberdefensa táctica y operativa.

A nivel técnico, cada una de las siete fases del modelo CKC representa un punto potencial de intervención y contención. La fase de Reconocimiento implica la recopilación pasiva o activa de información sobre el objetivo, lo cual puede incluir técnicas OSINT, fingerprinting de red, y análisis de vulnerabilidades públicas. El Armamento se refiere a la construcción del vector de ataque, como malware, exploits personalizados o scripts automatizados. La Entrega marca el momento de inserción del artefacto, mediante phishing, enlaces maliciosos o acceso físico. La Explotación busca ejecutar código en el sistema objetivo, seguido por la Instalación del

malware que garantice persistencia. Luego, en C2, se establece un canal de comunicación remoto que habilita el control adversario, y finalmente se llevan a cabo las Acciones sobre el Objetivo, tales como extracción de datos, sabotaje o propagación lateral. Cabe destacar que el modelo sigue siendo un pilar fundamental no solo para la defensa, sino también para las prácticas ofensivas modernas como el pentesting, donde se adapta para estructurar y ejecutar ataques simulados de manera metódica [25].

2.2 Críticas al Modelo Lineal y Perspectivas Alternativas

Diversas investigaciones han señalado que el modelo CKC, si bien útil en contextos estructurados, no refleja adecuadamente las dinámicas actuales de amenazas persistentes avanzadas (APT), ataques multi-vectoriales o campañas asincrónicas [2][3]. La crítica más común es su carácter excesivamente lineal, el cual asume que un ataque progresa necesariamente de una fase a la siguiente, cuando en la práctica muchos adversarios operan en ciclos iterativos, fases paralelas o incluso retroalimentadas. En respuesta a estas limitaciones, han surgido enfoques más comprensivos como la Unified Kill Chain (UKC), la cual expande el modelo a 18 fases para integrar de forma nativa la granularidad de ATT&CK y cubrir todo el ciclo de vida del adversario de manera más completa [26]. Adicionalmente, se han desarrollado modelos explícitamente defensivos, como el "SOC Critical Path", que reinterpreta la cadena de ataque desde la perspectiva de un Centro de Operaciones de Seguridad (SOC) para priorizar acciones de defensa y contención de manera más eficaz [23].

En contextos modernos, los ataques pueden omitir fases enteras (por ejemplo, saltar de reconocimiento a acciones directas gracias al uso de credenciales filtradas), o adaptarse dinámicamente según la respuesta del entorno defensivo. Esta flexibilidad táctica no está adecuadamente modelada en el CKC tradicional. De igual forma, marcos como MITRE ATT&CK permiten mapear comportamientos en múltiples plataformas, fases de persistencia o

movimiento lateral con un alto nivel de especificidad, lo cual ha llevado a muchas organizaciones a utilizar ambos marcos de forma complementaria [4].

2.3 Aplicaciones del CKC en Nuevos Dominios

Pese a las limitaciones mencionadas, el CKC ha sido extendido a dominios operativos emergentes con resultados prometedores. En el ámbito aeroespacial, el SDA TAP Lab ha desarrollado aplicaciones basadas en CKC para cerrar brechas en la detección de amenazas anti-satélite y optimizar respuestas automatizadas a eventos de riesgo orbital [5]. En escenarios militares, el CKC se ha usado para modelar ataques coordinados de enjambres de UAVs, mediante árboles de comportamiento que permiten reducir el tiempo de cierre de la cadena y aumentar la letalidad táctica [6]. En el ecosistema IoT, se ha propuesto el IoT Kill Chain (IoTKC), una variante que contempla vectores de ataque propios de dispositivos embebidos, conectividad inestable y autenticación débil [7].

Cada una de estas aplicaciones ha requerido adaptar las fases tradicionales del CKC a sus particularidades. Por ejemplo, en IoT, el armamento puede implicar firmware modificado, la entrega puede aprovechar protocolos como MQTT, y el comando y control puede establecerse mediante botnets distribuidas. Esta capacidad de adaptación sugiere que, si bien el CKC no es suficiente por sí solo, sí representa un marco base útil cuando es integrado con modelos dinámicos y tecnologías emergentes.

3. Inteligencia Artificial y Asimetría Operativa en el CKC

3.1 Potenciación de la Ofensiva mediante Inteligencia Artificial

En el contexto contemporáneo de ciberseguridad, la inteligencia artificial (IA) ha alterado significativamente la balanza de poder entre atacantes y defensores, generando una marcada asimetría operativa a favor de los primeros. Herramientas de automatización y aprendizaje

supervisado y no supervisado han permitido a los actores maliciosos optimizar las fases iniciales del CKC, especialmente Reconocimiento, Armamento y Entrega [8][9]. Ejemplos emblemáticos incluyen la utilización de GyoiThon, que automatiza la identificación de tecnologías y vulnerabilidades en servidores web, y DeepExploit, un framework basado en reinforcement learning que permite seleccionar y ejecutar exploits de manera autónoma.

Las redes generativas antagónicas (GANs) también han sido instrumentalizadas en la generación de dominios de comando y control (C2), evadiendo blacklistings convencionales mediante Domain Generation Algorithms (DGAs) dinámicos [10]. Asimismo, el concepto de Smart Delivery Malware ha introducido cargas maliciosas que no se activan hasta identificar condiciones óptimas de ejecución, como intervalos de inactividad del usuario o patrones específicos de tráfico de red, simulando conductas benignas ante mecanismos de detección superficial.

3.2 Limitaciones de la Defensa Tradicional Frente a la IA Ofensiva

A pesar de los avances en tecnologías defensivas, la brecha de efectividad entre ofensiva y defensa cibernética permanece amplia. Kazimierczak et al. [8] estiman una desventaja de 2.1:1 para los mecanismos defensivos actuales frente a herramientas de ataque potenciadas por IA. Esta desventaja se evidencia en la limitada eficacia de herramientas como PhishSpy, que aunque alcanza una precisión del 95 % en entornos de prueba, disminuye su rendimiento ante ataques adversariales que utilizan adversarial training para evadir clasificadores.

Otra limitación crítica es la dependencia de firmas estáticas o detecciones por comportamiento no contextualizadas, lo cual se traduce en una alta tasa de falsos negativos frente a ataques novedosos o altamente adaptativos. Soluciones emergentes como el Autonomous Response Controller (ARC), basado en cadenas de Markov competitivas, han demostrado mayor

capacidad para responder a amenazas en tiempo real, pero su adopción en entornos productivos aún es incipiente.

3.3 Perspectivas de la IA Defensiva: Hacia una Resiliencia Multicapas

Diversos estudios sugieren que la superación de esta asimetría requiere un enfoque defensivo multicapa basado en aprendizaje híbrido, detección colaborativa y entrenamiento adversarial [8][11]. El uso combinado de técnicas supervisadas, no supervisadas y de aprendizaje por refuerzo en arquitecturas de detección permite identificar comportamientos anómalos en fases tempranas de la CKC. Por ejemplo, la integración de Random Forest, SVM y redes neuronales convolucionales ha demostrado mejorar la precisión en la detección de malware polimórfico en entornos Android [8]. Enfoques innovadores proponen la aplicación de técnicas de forensia digital en tiempo real para la detección temprana de ataques en curso, permitiendo a los defensores identificar artefactos maliciosos mientras el ataque aún se está desarrollando [21].

Asimismo, la protección de los datos de entrenamiento mediante cifrado homomórfico y el uso de estrategias de federated learning permiten reducir el riesgo de ataques de inferencia o model stealing en sistemas de defensa basados en IA. Estos enfoques deben acompañarse de auditorías algorítmicas y métricas de equidad para evitar sesgos inadvertidos que puedan excluir falsos positivos o legitimar comportamientos no maliciosos como amenazas.

3.4 Implicaciones Estratégicas

La IA no sólo transforma las tácticas individuales dentro del CKC, sino que modifica la lógica operacional completa del conflicto cibernético. La velocidad de toma de decisiones, la adaptabilidad de los ataques y la evasión dinámica de controles defensivos configuran un entorno donde la latencia humana se convierte en un punto de vulnerabilidad. En este sentido, el desarrollo de sistemas autónomos de detección y respuesta debe estar alineado con principios

éticos, regulaciones internacionales y capacidades de interpretación humana, para evitar respuestas automatizadas desproporcionadas o inadecuadas.

4. Integración del CKC con Marcos Complementarios y Arquitecturas Emergentes

4.1 Complementariedad entre CKC y MITRE ATT&CK

El modelo CKC, si bien proporciona una estructura narrativa útil para la trazabilidad de ataques, carece de la granularidad técnica necesaria para mapear TTPs específicos (Tactics, Techniques and Procedures). En contraste, el marco MITRE ATT&CK ha emergido como una taxonomía extensiva de comportamientos adversarios organizada por plataformas, fases y objetivos. A diferencia del CKC, ATT&CK permite representar técnicas específicas (por ejemplo, "Credential Dumping" o "Timestomping") que pueden estar presentes en múltiples fases del CKC, disolviendo la estructura lineal a favor de una matriz multidimensional [4].

La integración práctica de ambos modelos puede realizarse mediante una correlación cruzada, donde ATT&CK actúe como módulo de enriquecimiento de inteligencia dentro de cada fase del CKC. Por ejemplo, durante la fase de Explotación, ATT&CK permite discriminar entre vulnerabilidades explotadas localmente (T1203) versus remotamente (T1210), brindando mayor especificidad para acciones de respuesta. Herramientas como ATT&CK Navigator y CALDERA han permitido implementar esta integración en plataformas de detección y orquestación automatizada. Esta integración es la base de las prácticas modernas de emulación de adversarios, donde los equipos de seguridad (Purple Teams) utilizan la inteligencia de amenazas mapeada en ATT&CK para simular ataques realistas y validar proactivamente la eficacia de sus controles defensivos [27].

4.2 Aplicación de Teoría de Juegos al Modelado de Ataques

Desde una perspectiva estratégica, los ataques cibernéticos pueden modelarse como juegos de Stackelberg o juegos diferenciales, donde el atacante y el defensor optimizan sus acciones en función de las decisiones del oponente. El CKC puede ser reinterpretado como una secuencia de estados dentro de un juego secuencial imperfecto, donde cada fase representa una decisión binaria (intervenir o no) sujeta a costos, beneficios y observabilidad parcial [12].

Investigaciones como la de Kour et al. [12] proponen formalizaciones matemáticas del CKC utilizando matrices de transición, recompensas asociadas y estados absorbentes. Estas aproximaciones permiten identificar equilibrios de Nash y estrategias dominantes para cada parte, optimizando la asignación de recursos defensivos en fases críticas. La aplicación de este enfoque también facilita el diseño de honeypots estratégicos y respuestas diferidas (delayed response) que modulan el comportamiento del adversario. Esto se alinea con estrategias defensivas más amplias, como el "cyber threat hunting" inducido por tecnologías de engaño, que actúan como una última línea de defensa para frustrar a los atacantes y recopilar inteligencia sobre sus métodos, especialmente en entornos críticos como las redes SCADA [22].

4.3 Arquitecturas Blackboard para Coordinación Dinámica

Una arquitectura blackboard se compone de un espacio compartido de conocimiento (blackboard) donde agentes expertos especializados (conocidos como knowledge sources) depositan hipótesis, inferencias y resultados parciales. En el contexto del CKC, este tipo de arquitectura puede ser utilizada para coordinar múltiples sensores, motores de inferencia, y módulos de respuesta ante incidentes en tiempo real [13].

Straub [13] demuestra la eficacia de combinar CKC y ATT&CK dentro de una arquitectura blackboard, donde cada fase del CKC corresponde a un subsistema especializado. Esta distribución modular mejora la escalabilidad, la resiliencia frente a fallos de componentes, y la

adaptabilidad ante amenazas nuevas. Además, permite implementar mecanismos de razonamiento basado en evidencia, donde las decisiones se actualizan en función de datos contextuales provenientes de múltiples fuentes (tráfico, logs, alertas de EDR).

4.4 Limitaciones de la Interoperabilidad Semántica

Uno de los retos persistentes en la integración de modelos como CKC y ATT&CK es la divergencia semántica en la representación de eventos. Mientras CKC se enfoca en el flujo lógico de ataque, ATT&CK categoriza acciones individuales sin una dependencia explícita entre ellas. Esto genera dificultades para traducir detecciones específicas en acciones correlacionadas dentro de la cadena de ataque. Para resolver este obstáculo, se ha propuesto la estandarización de taxonomías mediante STIX 2.1 y el uso de lenguajes de orquestación como OpenC2.

En conclusión, la interoperabilidad entre modelos requiere no sólo integración técnica, sino también convergencia semántica y operacional. La armonización de estos enfoques constituye un paso esencial hacia una defensa cibernética basada en conocimiento, adaptativa y explicable.

5. Implicaciones Éticas, Epistemológicas y Normativas del CKC

5.1 El CKC como Marco Epistémico: Modelando la Amenaza

Desde una perspectiva epistemológica, el CKC no solo constituye una herramienta para describir ataques, sino también un marco que moldea la manera en que las amenazas son conceptualizadas, priorizadas y combatidas [14]. Según Muller [14], el modelo encarna una lógica vigilante que traduce dinámicas sociotécnicas complejas en narrativas lineales, simplificadas y operativamente viables. Esta traducción es necesaria para articular respuestas institucionales, pero también puede generar sesgos en la atribución de riesgo, delimitando

artificialmente lo que se considera una amenaza legítima frente a lo que se excluye por no encajar en la cadena.

Al promover una visión estructurada de la agresión, el CKC puede inadvertidamente favorecer estrategias defensivas centradas en el vector técnico, dejando de lado factores contextuales, sociales y organizacionales. En este sentido, su uso indiscriminado en ambientes automatizados puede cristalizar supuestos culturales sobre quién representa una amenaza y cómo deben priorizarse los incidentes, particularmente en contextos geopolíticos o de inteligencia militar.

5.2 Sesgo Algorítmico y Automatización de Decisiones

La implementación automatizada del CKC en sistemas de detección y respuesta basados en inteligencia artificial conlleva riesgos significativos en términos de equidad, transparencia y responsabilidad. Los algoritmos entrenados para identificar amenazas a partir de datos históricos corren el riesgo de replicar sesgos estructurales, amplificando patrones discriminatorios sobre determinadas geografías, comportamientos o tecnologías [15]. Por ejemplo, la excesiva representación de tráfico proveniente de ciertas regiones en bases de datos de amenazas puede inducir modelos de clasificación que sobredimensionan el riesgo asociado a dichas ubicaciones.

Este fenómeno es particularmente crítico en sistemas de respuesta autónoma que operan con latencia mínima, donde las decisiones son tomadas sin supervisión humana directa. La ausencia de mecanismos de auditoría algorítmica y explicación causal en estos modelos puede derivar en consecuencias operativas adversas, incluyendo falsas alarmas sistemáticas, bloqueos indebidos o escaladas innecesarias de respuesta.

5.3 OSINT, Vigilancia Digital y Protección de la Privacidad

La fase de reconocimiento del CKC ha evolucionado hacia una sofisticación sin precedentes gracias al uso masivo de técnicas de Open Source Intelligence (OSINT). Plataformas automatizadas pueden recolectar, correlacionar y explotar datos públicos y semipúblicos a una escala que bordea la vigilancia masiva [16]. Esta capacidad, aunque útil desde la perspectiva de la defensa, plantea tensiones éticas y jurídicas relacionadas con el consentimiento, la transparencia y la protección de datos personales.

Normativas como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea establecen principios estrictos sobre la minimización, legitimidad y proporcionalidad del tratamiento de datos, los cuales pueden entrar en conflicto con prácticas OSINT agresivas. En particular, el principio de propósito limitado entra en tensión con el uso de datos recolectados para fines indefinidos o cambiantes como la seguridad nacional o la ciberinteligencia. Estas tensiones se agravan cuando los datos utilizados han sido generados por usuarios sin conciencia clara de su exposición, como metadatos en redes sociales, nombres de dominio o contenidos indexados.

5.4 Hacia una Ciberdefensa Ética y Responsable

Ante estos desafíos, diversos autores y organismos han abogado por el desarrollo de marcos de gobernanza algorítmica y ciberética que regulen la implementación del CKC y modelos similares en entornos operacionales. Se ha propuesto la adopción de principios de diseño responsables, que incluyan auditoría continua, documentación explícita de supuestos, y participación multidisciplinaria en la evaluación de riesgos sociotécnicos [15][17].

En síntesis, la eficacia operativa del CKC debe equilibrarse con su impacto normativo y cultural, evitando que la automatización de la defensa conlleve una deshumanización de la seguridad. Las futuras aplicaciones del CKC en entornos de alta autonomía deben incluir

salvaguardas que garanticen la rendición de cuentas, la protección de los derechos fundamentales y la interpretación humana de las decisiones críticas.

6. Conclusiones y Perspectivas Futuras

El Cyber Kill Chain, concebido como un modelo lineal para representar la progresión táctica de un ataque cibernético, ha demostrado una utilidad duradera en entornos operativos, institucionales y de formación. No obstante, la evolución del panorama de amenazas exige una revisión crítica y expansiva de sus postulados fundamentales. Este trabajo ha argumentado que, si bien el CKC mantiene valor como esquema de referencia, debe ser complementado con enfoques más dinámicos, modulares y éticamente responsables.

Desde una perspectiva técnica, se ha evidenciado que la inteligencia artificial ha profundizado la asimetría entre atacantes y defensores, demandando soluciones defensivas basadas en IA híbrida, federated learning, y cifrado homomórfico. Asimismo, la combinación del CKC con marcos como MITRE ATT&CK, teoría de juegos y arquitecturas blackboard permite dotarlo de una mayor adaptabilidad y granularidad operativa, facilitando la detección de APTs y ataques no secuenciales.

En el plano estratégico, se han propuesto mecanismos para armonizar modelos de ciberseguridad con principios normativos y éticos. Las problemáticas derivadas del sesgo algorítmico, la automatización de decisiones sin interpretación humana, y el uso masivo de OSINT exigen la formulación de una ciberdefensa que combine eficacia operativa con rendición de cuentas, protección de derechos y gobernanza transparente.

Las líneas futuras de investigación deben incluir:

- Desarrollo de CKC adaptativos mediante redes bayesianas dinámicas y procesos de Markov ocultos.

- Automatización de la simulación de cadenas de ataque completas mediante IA, utilizando LLMs para interpretar inteligencia de amenazas y planificar escenarios de prueba dinámicos, tal como demuestran sistemas emergentes [28].
- Implementación de auditorías algorítmicas explicables en entornos SOC autónomos.
- Evaluación empírica del CKC extendido en dominios emergentes como guerra cognitiva, operaciones satelitales y vehículos autónomos conectados.

En conclusión, el CKC no debe ser descartado, sino repensado y expandido. Su evolución debe orientarse hacia una arquitectura interoperable, automatizada y humanamente interpretable que responda a las complejidades de un entorno de amenazas post-lineal y multidominio.

7. Referencias

[1] Lockheed Martin Corporation. (2011). Cyber Kill Chain®.

[2] Avast. (2023). What Is the Cyber Kill Chain and How Does It Work?

[3] Kazimierczak, M., et al. (2024). Impact of AI on the Cyber Kill Chain: A Systematic Review. Heliyon.

[4] Elhoseny, A., et al. (2024). Enhancing CKC Detection Using ML and Network Behavior. IEEE SMC.

[5] Furlich, G., et al. (2024). Automated, Collaborative Applications to Close Kill Chain Gaps. AMOS Conference.

[6] Cai, L., et al. (2025). Research on the Kill Chain of UAV Swarm Coordinated Attack. Scientific Journal of Technology.

[7] Haseeb, J., et al. (2020). A Measurement Study of IoT-Based Attacks Using IoT Kill Chain. IEEE TrustCom.

[8] Shehu, A., et al. (2023). Cyber Kill Chain Analysis Using Artificial Intelligence. Asian Journal of Research in Computer Science.

[9] Cho, S., et al. (2020). Threat Taxonomy and its Application on Cyber COP. IEEE SmartCloud.

[10] Yamin, M. M., et al. (2022). Mapping OSINT Tools with CKC. Mathematics.

[11] Ahmed, Y., et al. (2021). Detecting Advanced Persistent Threats. Computers, Materials & Continua.

[12] Kour, R., et al. (2025). Modelling cybersecurity strategies with game theory and CKC.

[13] Straub, J. (2020). Modeling CKC and ATT&CK with Blackboard Architectures. IEEE SmartCloud.

[14] Muller, L. P. (2024). The vigilant logic of kill chains. European Journal of International Security.

[15] Pijnenburg Muller, L. (2024). On fairness and adversarial learning.

[16] Yamin, M., et al. (2022). Mapping OSINT Tools with Cyber Kill Chain. Mathematics.

[17] PhishDetector and PhishSpy .

[18] Vijayan, J. (2021). The Cyber Kill Chain: A Flawed Model. Dark Reading.

[19] Deep Exploit and GyoiThon .

[20] GDPR compliance issues with OSINT.

[21] Dimitriadis, A., et al. (2023). Fronesis: Digital Forensics-Based Early Detection of Ongoing Cyber-Attacks. *IEEE Access*, 11, 728-742.

[22] Ajmal, A. B., et al. (2021). Last Line of Defense: Reliability Through Inducing Cyber Threat Hunting With Deception in SCADA Networks. *IEEE Access*, 9, 126791-126800.

[23] Villalón-Huerta, A., Gisbert, H. M., & Ripoll-Ripoll, I. (2022). SOC Critical Path: A Defensive Kill Chain Model. *IEEE Access*, 10, 13572–13578.

[24] Dávila-Huayhuapuma, J. E., Vílchez-Roncal, E., & Alvarado-Silva, C. A. (2025). The Cyber Kill Chain Methodology as a Business Defense Tool: A Systematic Review of Its Application and Efficacy. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(12), 160–179.

[25] Zhao, L. (2023). Navigating the Cyber Kill Chain: A modern approach to pentesting. *Applied and Computational Engineering*, 38, 170-175.

[26] Pols, P. (2022). *The Unified Kill Chain*. Unifiedkillchain.com.

[27] Selmanaj, D. (2024). *Adversary Emulation with MITRE ATT&CK*. O'Reilly Media.

[28] Ni, T., et al. (2024). *From Sands to Mansions: Simulating Full Attack Chain with LLM-Organized Knowledge*. arXiv preprint arXiv:2407.16928.

[29] Mitra, S., Chakraborty, T., Neupane, S., Piplai, A., & Mittal, S. (2024). Use of graph neural networks in aiding defensive cyber operations. arXiv. https://arxiv.org/abs/2401.05680

[30] Rodriguez, M., Popa, R. A., Flynn, F., Liang, L., Dafoe, A., & Wang, A. (2025). A framework for evaluating emerging cyberattack capabilities of AI. ArXiv. https://arxiv.org/abs/2503.11917