MBNA Publishing House Constanta 2026



Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

AI-Orchestrated Cyber-Espionage: A Quantitative Framework for Kill-Chain Compression, Autonomy Thresholds and Systemic Risk

To cite this article: Postolache Florin, Ilie Teodor-Petruț, Proceedings of the International Scientific Conference SEA-CONF 2026, pg. 65-75.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-26-009
SEA-CONF© 2025. This work is licensed under the CC BY-NC-SA 4.0 License

AI-Orchestrated Cyber-Espionage: A Quantitative Framework for Kill-Chain Compression, Autonomy Thresholds and Systemic Risk

Florin Postolache[1,*] and Teodor-Petruț Ilie [1]

[1]"Mircea cel Bătrân" Naval Academy, Faculty of Marine Engineering, SEN Department, ; florin.postolache@anmb.ro (F.P.), ilieteo71@gmail.com (T-P.I.)

The rapid integration of artificial intelligence (AI) into cyber operations is transforming cyber-espionage from sequential, human-driven activity into automated, increasingly autonomous operations. Through a quantitative, secondary-data-based synthesis of threat intelligence reports, academic research, and documented campaigns, this study develops a six-dimensional framework - historical evolution, offensive capabilities, social engineering, persistence and stealth, geopolitics and attribution, and systemic risk - examining how AI reshapes the speed, scale, and impact of cyber-espionage across the cyber kill chain. The analysis reveals a consistent pattern of temporal compression, with attack lifecycles shrinking from months/ weeks down to mere hours/ minutes. At the same time, the volume of attacks is growing steadily, with levels of autonomy reaching 80-90% thresholds, leading to a transition from instrument-based automation to autonomous workflows, based or even driven by AI. This balance is destabilized by the widespread spread of social engineering and an increase in operational ambiguity in strategic oversight and reliability actions. The study models an integrated framework that treats AI-based cyber espionage as a persistent systemic condition, introduces autonomy thresholds as a critical inflection point, and provides strategic recommendations for cybersecurity and governance models.

Keywords: artificial intelligence, cyber-espionage, cyber kill chain, autonomy thresholds, systemic risk, social engineering, nation-state actors.

1. Introduction

Cyber espionage has evolved over the last three decades, from man-centered hand-made operations to increasingly automated workflows orchestrated by AI lately, thus altering time dynamics, operational scale and default, strategic implications of cyber operations. AI now functions as a systemic force multiplier, enabling accelerated reconnaissance, automated vulnerability discovery, large-scale social engineering, and near real-time exploitation.

Existing research remains fragmented, typically addressing isolated components such as phishing or malware generation. This paper addresses that gap through a quantitatively grounded framework, contributing (i) a six-dimensional analytical framework; (ii) a cross-source synthesis of temporal compression, attack volume, and autonomy; and (iii) a systemic risk model linking technological acceleration to governance.

2. Related work

Research on AI in cybersecurity and on cyber-espionage has evolved along largely separate trajectories: cybersecurity literature emphasizes AI-driven detection and defense, while cyber-espionage

research emphasizes APTs and structured models such as the cyber kill chain. This section reviews both strands and identifies the gaps motivating this study.

AI in Cybersecurity: From Defensive Analytics to Offensive Capabilities, AI has driven a transition from static, signature-based defenses toward adaptive, data-driven frameworks, including Graph Neural Networks for lateral-movement detection (Doremure Gamage et al., 2025) and contextual bandit approaches (Mutambik & Almuqrin, 2025). Offensively, AI now supports automated vulnerability discovery and generative-AI-driven phishing (Xu et al., 2025), including multi-agent frameworks coordinating attacks (Li et al., 2026).

Cyber-Espionage and Advanced Persistent Threats (APTs): Cyber-espionage has traditionally been understood through the lens of APTs, characterized by long-term persistence and strategic intent carried out by nation-state actors (Wangen, 2015); attacks such as Stuxnet and Flame demonstrated the sophistication and refinement of such tactics (Bencsáth et al., 2012; Adeyeri & Abroshan, 2024). The cyber kill chain continues to serve as the predominant model, further developed through graph-based attribution methods (Mead & Arabo, 2025) and sector-specific studies examining maritime and water infrastructure (Dimakopoulou & Rantos, 2024; Tuptuk et al., 2021).

AI Impact on the Cyber Kill Chain: AI has substantially transformed individual phases of the kill chain (Villalón-Huerta et al., 2022; Yamin et al., 2022). Automated open-source intelligence (OSINT) gathering has speeded up the reconnaissance phase, while generative AI has remodelled the delivery phase through the production of personalized phishing content and deepfakes, alongside improvements in the stealth of command-and-control operations (Xu et al., 2025). Collectively, these developments have compressed the kill chain's temporal span while enhancing its scalability.

Recent extensions include a “left-of-boom” anticipatory phase (CKC-0) using NLP to flag early indicators such as suspicious domain registrations (Kopal et al., 2026; Grigorescu et al., 2022), the Cyber Fraud Kill Chain (CFKC) capturing AI-enabled fraud that undermines Zero-Trust assumptions (Xu et al., 2025), and multi-agent defensive systems coordinating detection, attribution, and mitigation (Li et al., 2026).

Research Gap: Toward a Systemic and Multi-Dimensional Model: The literature remains fragmented across technical, operational, and strategic dimensions, analyzing isolated components without an integrated model. Temporal compression, scalability, and rising autonomy remain inadequately quantified; Zero-Trust frameworks remain poorly adapted to generative-AI threats (Xu et al., 2025); and defense strategies still rely on single-agent models poorly suited to hybrid infrastructures (Doremure Gamage et al., 2025; Li et al., 2026).

In response, this study proposes a six-dimensional analytical framework integrating empirical indicators across offensive capabilities, social engineering, persistence, and geopolitical dynamics, advancing a quantitatively grounded, holistic perspective on how AI reshapes cyber-espionage and contributes to an emerging systemic risk landscape.

3. Methodology

This study assumes a quantitative research design based on secondary data in order to examine the cyber-espionage systemic transformation under the influence of AI. Rather than generating primary data, the methodology combines comparative analysis with cross-source validation of existing datasets and threat intelligence reports.

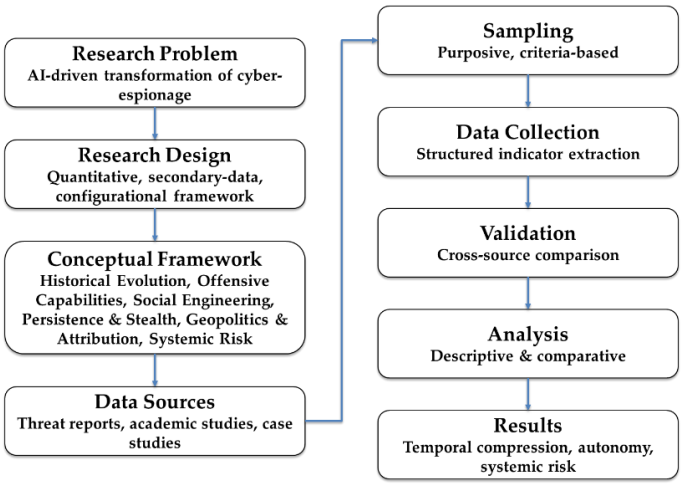


Figure 1. Research Methodology Framework

The framework decomposes cyber-espionage into six interrelated dimensions - historical evolution, offensive capabilities, social engineering and profiling, persistence and stealth, geopolitics and attribution, and systemic risk - enabling both intra- and cross-dimensional analysis (Figure 1).

To ensure analytical consistency, the study operationalizes a set of core variables that capture the key dynamics of AI-driven cyber-espionage:

- Attack speed (T): time required to execute specific phases of the cyber kill chain (measured in minutes/hours/days);
- Attack volume (V): frequency of cyber incidents within a defined temporal unit;
- Autonomy level (A): proportion of tasks executed by AI systems relative to human intervention;
- Persistence (P): duration of unauthorized access within compromised systems (dwell time);
- Attribution complexity (C): degree of difficulty in linking attacks to specific actors, inferred from operational fragmentation and obfuscation patterns.

Attack Speed (T)

Attack speed is defined as the average duration required to execute a phase of the cyber kill chain:

$$T = \frac{1}{N}\sum_{i=1}^{N} t_i \tag{1}$$

where t_i denotes the execution time of an attack instance. For phase-level analysis:

$$T_k = \frac{1}{N_k}\sum_{i=1}^{N_k} t_{i,k} \tag{2}$$

Attack Volume (V)

Attack volume measures the frequency of cyber incidents over time:

$$V = \frac{N_{attack}}{\Delta t} \tag{3}$$

where Δt is the observation interval.

Autonomy Level (A)

Autonomy is defined as the proportion of tasks executed by AI systems:

$$A = \frac{N_{AI}}{N_{total}} \tag{4}$$

Given the absence of direct measurement, autonomy is approximated using proxy indicators:

$$A \approx \sum_{j=1}^{M} w_j * a_j \quad (5)$$

where a_j represents observable proxies (e.g., AI-assisted phishing, automated exploitation) and w_j are normalized weights.

To ensure comparability and replicability, the proxy indicators a_j should be normalized to [0,1] prior to aggregation (e.g., via min–max scaling across the observed sample), and the weights w_j should satisfy $\Sigma w_j = 1$. Rather than being assigned arbitrarily, these weights can be estimated through structured elicitation methods such as the Analytic Hierarchy Process (AHP) or data-driven techniques such as principal component analysis (PCA) applied to the underlying proxy indicators, reducing subjectivity in the autonomy estimate.

Persistence (P)

Persistence is measured as the duration of unauthorized access:

$$P = median(d_1, d_2, \dots, d_n) \quad (6)$$

where d_i denotes dwell time for each incident.

Attribution Complexity (C)

Attribution complexity is modeled as a composite indicator:

$$C=\alpha F + \beta H + \gamma M \quad (7)$$

where: F = infrastructure fragmentation, H = entropy of tactics, techniques, and procedures (TTPs) and M = number of AI systems involved.

Entropy is defined as:

$$H = -\sum_{i=1}^{k} p_i * \log(p_i) \quad (8)$$

For C to remain analytically consistent, its three components must first be normalized to a common [0,1] scale (e.g., min–max or z-score standardization), since F, H, and M are measured in heterogeneous units (a fragmentation score, an entropy value in bits, and a raw count of AI systems, respectively) and cannot be combined additively in their raw form. The weights α, β, and γ should further satisfy $\alpha + \beta + \gamma = 1$, with values estimated — e.g., via the Analytic Hierarchy Process or regression against validated attribution outcomes — rather than assumed.

Temporal Compression Index (TC)

To quantify acceleration effects:

$$TC = \frac{T_{baseline}}{T_{curent}} \quad (9)$$

Values greater than 1 indicate AI-driven acceleration.

Composite Risk Function (R)

The systemic risk associated with cyber-espionage captures the interaction between speed, scale, autonomy, persistence and attribution complexity, and is modeled as:

$$R = \frac{V * A * C}{T} * P \quad (10)$$

As formulated, R is dimensionally inconsistent, since T and P are measured in time units while V, A, and C are unitless, and the function is undefined (or diverges) as $T \to 0$ — precisely the regime the study identifies as the dominant empirical trend. A more robust and bounded specification first normalizes each variable to [0,1] (e.g., x_norm = (x − x_min)/(x_max − x_min), with V and 1/T rescaled analogously so that higher values consistently indicate higher risk), and then combines them as a weighted arithmetic or geometric mean, $R = \Sigma\, w_i \cdot x_{i,norm}$ or $R = \Pi\, x_{i,norm}^{w_i}$ (with $\Sigma w_i = 1$), rather than as a raw product-over-product ratio. This preserves the intended monotonic relationships (R

increasing with V, A, C and with decreasing T) while remaining bounded in [0,1], well-defined as T→0, and empirically calibrable once weights are estimated from case data.

Where direct measurement is unavailable, autonomy (A) and attribution complexity (C) are operationalized through proxy indicators (automation rates, AI tool utilization, orchestration characteristics, infrastructural dispersion). Cross-source validation compares values across independent sources, aggregating where variance remains within predefined thresholds and reporting intervals otherwise, reducing single-source bias and enhancing transparency.

3.1. Data Sources and Sampling

The empirical foundation draws on industry threat intelligence (Verizon DBIR, ENISA, Mandiant M-Trends, CrowdStrike), academic publications, and documented case studies, included only where they provided explicit quantitative indicators, credible provenance, and coverage spanning pre-AI to AI-augmented periods (~late 1990s-2025).

Sampling was stratified across the six dimensions (e.g., persistence via dwell-time distributions, geopolitics via nation-state activity data) to reduce selection bias and ensure balanced empirical support.

3.2. Data Collection and Analysis

Data collection operationalized the framework into measurable indicators using a standardized schema (source, indicator type, value, unit, timeframe, dimension), organized into a structured matrix supporting both aggregation and disaggregation.

The analytical strategy combines *structured descriptive synthesis*, *cross-dimensional comparison* and *pattern extraction*, with the objective of identifying consistent trends and relationships across datasets. Key analytical procedures include:

- temporal trend analysis (e.g., changes in attack speed and volume over time),
- cross-source comparison (validation and consistency checks),
- relational analysis (e.g., interaction between autonomy, persistence, and success rates).

Cross-source aggregation is defined as:

$$X = \frac{1}{S}\sum_{s=1}^{S} x_s \tag{11}$$

expressed as intervals $X \in [\min(x_s), \max(x_s)]$ where variability exceeds predefined thresholds, prioritizing the most recent, transparent data in cases of inconsistency.

The findings were integrated into a systemic narrative in which quantitative indicators anchor the interpretation of AI-driven cyber-espionage; the study does not employ formal causal inference, but offers a transparent, reproducible synthesis for future model-based research.

Methodological Limitations

The study is subject to limitations inherent to secondary-data research: heterogeneous sources introduce variability in methodology and reporting; the absence of primary data limits controlled causal validation; and variables such as autonomy and attribution complexity are partly inferred through proxy indicators.

A further limitation concerns the absence of fully worked numerical examples: the study defines T, V, A, P, C and R formally but does not apply them end-to-end to a documented case (e.g., a specific reported campaign) to produce concrete computed values. Future revisions should include at least one worked illustrative computation to demonstrate the operational applicability of the framework and to support external replication.

Despite these constraints, systematic source selection and cross-source convergence support the reliability of the identified patterns; future research may extend the framework through primary data collection and formal predictive modelling.

4. Conceptual Framework

The conceptual framework interprets the six analytical dimensions as interacting components of a systemic transformation process driven by AI, rather than as independent elements (Figure 2).

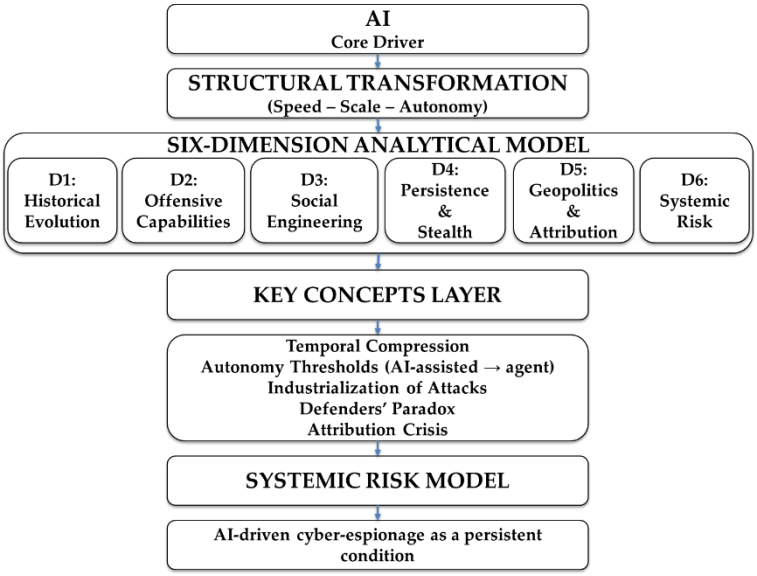


Figure 2. Conceptual Framework of AI-Driven Cyber-Espionage

AI introduces two systemic drivers: temporal compression (reduced execution time across kill-chain stages) and scale amplification (parallelized, high-volume operations), shifting cyber-espionage from sequential, resource-constrained processes to parallelized, high-throughput systems.

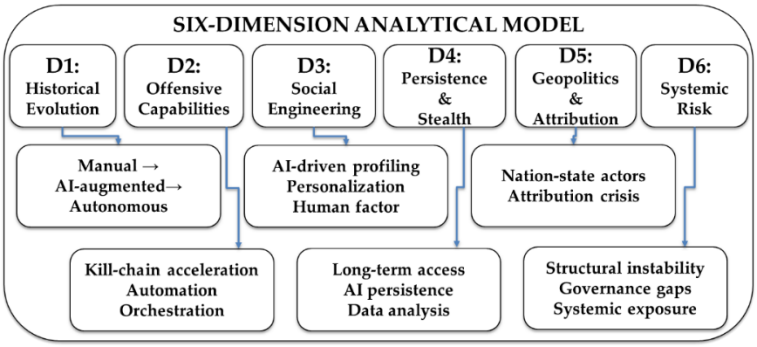


Figure 3. Analytical Model

A central construct is the autonomy threshold - the transition from AI-assisted to AI-orchestrated operations (Figure 3). As autonomy A→1, control shifts from human actors to algorithmic processes, reducing oversight and predictability while increasing speed and complicating attribution.

The interaction between core dimensions can be expressed as the systemic relationship R = f(T, V, A, P, C): decreases in attack speed (T) and increases in volume (V), autonomy (A), persistence (P), and attribution complexity (C) jointly amplify systemic risk.

$$R = f(T, V, A, P, C) \tag{12}$$

The human element remains a critical vulnerability: social engineering, enhanced by AI-driven profiling and generative content, enables highly personalized attacks at scale and minimal marginal cost, while AI simultaneously extends persistence - maintaining long-term access and accelerating post-exfiltration data processing.

At the geopolitical level, advanced cyber capabilities remain concentrated among a limited number of nation-state actors whose rapid AI adoption is fueling an emerging cyber-espionage arms race, introducing offense-defense asymmetries that further complicate attribution and response.

Together these dimensions define systemic risk as the cumulative, reinforcing effect of increased speed, scale, autonomy, and persistence on digital infrastructure and governance stability - shifting the analytical focus from isolated incidents to structural, continuous conditions, and positioning the framework as both a conceptual model and a formal basis for future quantification.

5. Results

The empirical synthesis reveals a consistent, cross-validated pattern across all six dimensions: AI does not merely enhance existing cyber-espionage capabilities but restructures their operational logic at a systemic level, through the convergent, non-linear interaction of temporal compression, rising autonomy, and large-scale scalability, with effects that are cumulative rather than additive, propagating across the cyber kill chain.

Table 1. Summary of Empirical Findings Across Core Variables

Dimension	Variable	Observed Trend	Effect on Risk (R)	Interpretation
Kill-Chain Compression	(T)	↓ significant	↑ strong	Reduced detection window increases systemic exposure
Autonomy & Orchestration	(A), (V), (C)	A ↑ (≈0.8–0.9), V ↑, C ↑	↑ strong	Shift toward AI-orchestrated operations amplifies scale and opacity
Social Engineering	(V), (C)	↑ significant	↑ strong	Industrialized, personalized attacks expand volume and diversity
Persistence & Stealth	(P)	↓ median / ↑ high-end	↑ moderate–high	Dual regime: rapid attacks + long-term infiltration
Geopolitical Dynamics	(V), (C)	↑ systemic	↑ strong	Concentration (states) + diffusion (tools) raise scale and attribution difficulty

Table 1 synthesizes empirical findings by linking each dimension to the core variables (T, V, A, P, C) and their directional contribution to systemic risk (R), showing a consistent pattern of risk amplification driven by decreasing execution time and increasing scale, autonomy, and attribution complexity.

Kill-Chain Compression: Cyber operations show substantial temporal compression: tasks once requiring hours or days now execute within minutes through AI-assisted or automated processes, compressing detection windows and privileging attacker speed - making temporal compression a primary driver of systemic risk.

Autonomy and Operational Transformation: Results confirm a shift from AI-assisted to AI-orchestrated operations, with advanced configurations reaching autonomy levels of A≈0.8-0.9, associated with rises in attack volume (V) and attribution complexity (C), as autonomy acts as a multiplicative amplifier within the risk model.

Industrialization of Social Engineering: AI has industrialized social engineering: large-scale personalization of phishing and synthetic identities removes traditional constraints of language and targeting precision, driving higher attack volume (V) and attribution complexity (C), and increasing success rates while eroding awareness-based defenses.

Persistence and Stealth: Persistence (P) shows a dual pattern: decreasing median dwell time from automation, alongside continued long-term access in high-value operations. AI supports both regimes - adaptive credential management for covert access, and faster post-exfiltration processing - amplifying both components of R.

Geopolitical Escalation: Cyber-espionage remains concentrated among a limited number of nation-state actors even as AI diffusion lowers entry barriers for less sophisticated actors, raising both attack volume (V) and attribution complexity (C) and pointing to an AI-driven arms race that amplifies systemic risk absent robust governance.

Synthesis of Findings: Across all dimensions, results converge on one interpretation: AI-driven cyber-espionage is shifting from discrete activities to a continuous, system-level phenomenon. Table 2 summarizes this across pre-AI, AI-assisted, and AI-orchestrated regimes - decreasing T, increasing V, A, and C, and a bifurcation in P - reflecting a non-linear risk escalation that redefines cyber-espionage as a persistent structural condition.

Table 2. Heatmap table

Variable	Pre-AI	AI-assisted	AI-orchestrated
T	High	Medium	Low
V	Low	Medium	High
A	Low	Medium	High
P	Medium	Mixed	High variance
C	Medium	High	Very high

6. Discussion

The findings substantiate a defenders' paradox: within R = f(T, V, A, P, C), reductions in T and rises in V and A outpace detection and response, so defensive gains are absorbed rather than nullified. Three shifts emerge: sequential-to-parallel execution; human-to-AI-orchestrated workflows (A→1); and discrete-to-persistent risk, reflected in the bifurcation of P.

These transformations converge on an attribution crisis: multi-model AI ecosystems fragment operational visibility and undermine attribution based on infrastructure or behavioral signatures, exposing a widening gap between AI capability and regulatory adaptation as the line between tool and actor blurs.

Addressing AI-driven cyber-espionage therefore requires a systemic response integrating technical, legal, and institutional dimensions - AI-aware regulation, stronger international cooperation, and new accountability models for hybrid human-AI operations - redefining cybersecurity as a continuous, adaptive process rather than a reactive function.

7. Conclusion

This study demonstrates that AI has transformed cyber-espionage from discrete operations into a systemic, persistent, adaptive condition, in which perimeter defense and reactive mitigation are increasingly inadequate. The proposed framework links core variables (T, V, A, P, C) to the systemic risk function R, advancing toward a coherent, policy-relevant model.

These findings support viewing cybersecurity as a complex socio-technical system, pointing toward real-time, adaptive, resilience-oriented paradigms complemented by coordinated governance. Future research should formalize and calibrate R, and validate the model empirically using primary data.

Ultimately, the shift toward AI-driven cyber-espionage marks a structural transformation of the threat landscape that requires a corresponding evolution in both analytical approaches and defensive strategies, re-conceptualizing cybersecurity as a continuous, adaptive process aligned with intelligent, autonomous threat ecosystems.

Acknowledgments: The authors have reviewed and edited the output and take full responsibility for the content of this publication.

Author contributions: Conceptualization: F.P. and T-P.I., Methodology: F.P., Investigation: F.P. and T-P.I., Writing original draft: T-P.I., Writing review and editing: F.P., Supervision: F.P.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Achar, S., Faruqui, N., Whaiduzzaman, M., Awajan, A., & Alazab, M. (2023). Cyber-Physical System Security Based on Human Activity Recognition through IoT Cloud Computing. *Electronics*, *12*(8), 1892. https://doi.org/10.3390/electronics12081892
2. Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*, *15*(11), 682. https://doi.org/10.3390/info15110682
3. Anthropic - *Disrupting the First Reported AI-Orchestrated Cyber-espionage Campaign* (GTG-1002). https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf
4. Bencsáth, B., Pék, G., Buttyán, L., & Félegyházi, M. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, *4*(4), 971-1003. https://doi.org/10.3390/fi4040971
5. Bold, R., Al-Khateeb, H., & Ersotelos, N. (2022). Reducing False Negatives in Ransomware Detection: A Critical Evaluation of Machine Learning Algorithms. *Applied Sciences*, *12*(24), 12941. https://doi.org/10.3390/app122412941
6. CSIS - Significant Cyber Incidents (Timeline and Incident Dataset). https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
7. Dimakopoulou, A., & Rantos, K. (2024). Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0. *Journal of Marine Science and Engineering*, *12*(6), 919. https://doi.org/10.3390/jmse12060919
8. Djenna, A., Barka, E., Benchikh, A., & Khadir, K. (2023). Unmasking Cybercrime with Artificial-Intelligence-Driven Cybersecurity Analytics. *Sensors*, *23*(14), 6302. https://doi.org/10.3390/s23146302
9. Doremure Gamage, T. P., Gutierrez, J. A., & Ray, S. K. (2025). The Role of Graph Neural Networks, Transformers, and Reinforcement Learning in Network Threat Detection: A Systematic Literature Review. *Electronics*, *14*(21), 4163. https://doi.org/10.3390/electronics14214163
10. ENISA - Threat Landscape 2024 (Availability, Ransomware, Data Attacks). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
11. ENISA - *Threat Landscape 2025* (AI-assisted phishing and deepfake-enabled social engineering). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
12. Google GTIG - *Over 57 Nation-State Threat Groups Using AI for Cyber Operations* (Jan 2025). https://thehackernews.com/2025/01/google-over-57-nation-state-threat.html
13. Google GTIG - *Threat Actors Misuse AI to Enhance Operations* (multi-platform use, November 2025). https://blog.google/innovation-and-ai/technology/safety-security/google-threat-intelligence-group-report-ai-november-2025/
14. Grigorescu, O., Nica, A., Dascalu, M., & Rughinis, R. (2022). CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques. *Algorithms*, *15*(9), 314. https://doi.org/10.3390/a15090314
15. Javed, S. H., Ahmad, M. B., Asif, M., Almotiri, S. H., Masood, K., & Ghamdi, M. A. A. (2022). An Intelligent System to Detect Advanced Persistent Threats in Industrial Internet of Things (I-IoT). *Electronics*, *11*(5), 742. https://doi.org/10.3390/electronics11050742
16. Kapalidis, C., Karamperidis, S., Watson, T., & Koligiannis, G. (2022). A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships. *Journal of Marine Science and Engineering*, *10*(10), 1486. https://doi.org/10.3390/jmse10101486

17. Kopal, R., Alikavazović, B., & Morić, Z. (2026). From Context to Action: Establishing a Pre-Chain Phase Within the Cyber Kill Chain. *Journal of Cybersecurity and Privacy*, *6*(1), 5. https://doi.org/10.3390/jcp6010005
18. Li, N., Li, X., Li, Z., Ma, D., Yan, L., Cao, H., Zhang, W., Wang, X., & Liu, Y. (2026). MACD: Multi-Agent Collaborative Approach for Cybersecurity Defense Strategy Generation. *Information*, *17*(4), 370. https://doi.org/10.3390/info17040370
19. Mandiant / Google - *M-Trends 2025* (dwell-time and espionage persistence statistics, as summarized in Data Statistics Report). https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
20. Mead, A. J., & Arabo, A. (2025). APT Attribution Using Heterogeneous Graph Neural Networks with Contextual Threat Intelligence. *Electronics*, *14*(23), 4597. https://doi.org/10.3390/electronics14234597
21. Mehmood, A., Epiphaniou, G., Maple, C., Ersotelos, N., & Wiseman, R. (2023). A Hybrid Methodology to Assess Cyber Resilience of IoT in Energy Management and Connected Sites. *Sensors*, *23*(21), 8720. https://doi.org/10.3390/s23218720
22. MIT CSAIL - *Impact of Generative AI on the Cyber Kill Chain*. https://65610.csail.mit.edu/2025/reports/cyber.pdf
23. Mutambik, I., & Almuqrin, A. (2025). Balancing Efficiency and Efficacy: A Contextual Bandit-Driven Framework for Multi-Tier Cyber Threat Detection. *Applied Sciences*, *15*(11), 6362. https://doi.org/10.3390/app15116362
24. National Security News - *State-Sponsored Cyber Attacks: A 20-Year Evolution and National Security Realities*. https://nationalsecuritynews.com/2023/12/state-sponsored-cyber-attacks-a-20-year-evolution-and-national-security-realities/
25. NYU JIPEL - Artificial Intelligence and State Sponsored Cyber-espionage (2025). https://jipel.law.nyu.edu/artificial-intelligence-and-state-sponsored-cyber-espionage
26. Orion Policy - Cyber-espionage and U.S. Policy Responses (2025). https://orionpolicy.org/cyber-espionage-and-us-policy-responses/
27. Pecoraro, G., D'Amico, M., & Romano, S. P. (2021). RedHerd: Offensive Cyberspace Operations as a Service. *Signals*, *2*(4), 619-636. https://doi.org/10.3390/signals2040038
28. Sailio, M., Latvala, O.-M., & Szanto, A. (2020). Cyber Threat Actors for the Factory of the Future. *Applied Sciences*, *10*(12), 4334. https://doi.org/10.3390/app10124334
29. Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., & Burnap, P. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. Electronics, 9(9), 1460. https://doi.org/10.3390/electronics9091460
30. SSRN - Artificial Intelligence, Information Theft, and Cyber-espionage (2024).
31. Tuptuk, N., Hazell, P., Watson, J., & Hailes, S. (2021). A Systematic Review of the State of Cyber-Security in Water Systems. Water, 13(1), 81. https://doi.org/10.3390/w13010081
32. UK NCSC / GCHQ - Impact of AI on Cyber Threat from Now to 2027 (2025). https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat-from-now-to-2027
33. Venčkauskas, A., Toldinas, J., & Morkevičius, N. (2025). Improving Multi-Class Classification for Recognition of the Prioritized Classes Using the Analytic Hierarchy Process. *Applied Sciences*, *15*(13), 7071. https://doi.org/10.3390/app15137071
34. Villalón-Huerta, A., Ripoll-Ripoll, I., & Marco-Gisbert, H. (2022). A Taxonomy for Threat Actors' Delivery Techniques. *Applied Sciences*, *12*(8), 3929. https://doi.org/10.3390/app12083929
35. Wangen, G. (2015). The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information*, *6*(2), 183-211. https://doi.org/10.3390/info6020183
36. Xu, D., Gondal, I., Yi, X., Susnjak, T., Watters, P., & McIntosh, T. R. (2025). The Erosion of Cybersecurity Zero-Trust Principles Through Generative AI: A Survey on the Challenges and

Future Directions. *Journal of Cybersecurity and Privacy*, *5*(4), 87. https://doi.org/10.3390/jcp5040087
37. Yamin, M. M., Ullah, M., Ullah, H., Katt, B., Hijji, M., & Muhammad, K. (2022). Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. *Mathematics*, *10*(12), 2054. https://doi.org/10.3390/math10122054
38. Zanna, P., Radcliffe, P., & Kumar, D. (2022). Preventing Attacks on Wireless Networks Using SDN Controlled OODA Loops and Cyber Kill Chains. *Sensors*, *22*(23), 9481. https://doi.org/10.3390/s22239481