Investigating AI Enabled Attacks and Malware Within Dark Web Ecosystems: An Updated Assessment

Chuck Easttom and William Butler
Vanderbilt University and Georgetown University; Washington, USA

chuckeasttom@gmail.com
whbutler@captechu.edu

Abstract: This paper provides a technically grounded assessment of how Dark Web ecosystems are intersecting with AI-enabled offensive cyber capabilities to compress time-to-effect across the cyber kill chain. Hidden-service marketplaces and broker forums have matured into resilient, quasi-industrial supply chains for initial access vectors (credential dumps, VPN/RDP footholds), exploit artifacts, malware loaders, and operational services (bulletproof hosting, cryptomixers, DDoS booter capacity). Generative AI and machine-learning–assisted tooling increases attacker throughput by automating target enumeration, vulnerability triage, exploit parameterization, and social-engineering content generation, thereby reducing the marginal cost of tailored intrusion campaigns. We synthesize research on anonymity architectures, dark-market economics, and emerging autonomous cyber systems to characterize an operational model in which AI agents execute multi-step workflows: (i) harvesting and fusing threat-intelligence signals from forum discourse and market telemetry; (ii) selecting targets via probabilistic scoring informed by asset criticality and exploitability; (iii) generating polymorphic payload variants and adversarial phishing lures; and (iv) iterating tactics in response to defensive controls through reinforcement-learning–style feedback. This convergence enables hybrid state–criminal collaboration and proxy operations by decoupling capability acquisition from attribution and by supporting deniable command-and-control (C2) staging within onion-routed infrastructures. Quantitative telemetry underscores the strategic relevance of this shift: the FBI's IC3 reported losses exceeding US$16 billion in 2024, with cyber-enabled fraud comprising approximately US$13.7 billion and 'cyberthreats' (including ransomware and data breaches) contributing more than US$1.5 billion, illustrating the scale of the economic attack surface. In parallel, breach forensics continue to show that initial access is frequently achieved through stolen credentials, vulnerability exploitation and social engineering, which are precisely the phases most susceptible to AI-driven acceleration. We conclude that AI-augmented Dark Web ecosystems materially increase campaign scalability, complicate attribution via supply-chain opacity and pseudonymity, and elevate escalation risk by enabling rapid re-tooling and persistent access. The paper closes with engineering-oriented defensive implications, including telemetry-driven detection, graph-analytic threat-hunting, and governance controls for AI-enabled offensive automation.

Keywords: Dark web, TOR, Cyber warfare, Cyber operations

1. Introduction

Cyber warfare continues to evolve as states and non-state actors exploit anonymity, deniability, and persistent access. The Dark Web sits at the center of this environment, functioning as both an illicit marketplace and an operational layer for covert activity. Foundational work on onion routing and anonymity architectures (Goldschlag, Reed, & Syverson, 1999; Reed, Syverson, & Goldschlag, 1998; Syverson, Goldschlag, & Reed, 1997) established the technical basis for the hidden-service ecosystems that now support cyber operations. Subsequent research has documented how Dark Web markets facilitate illicit trade, criminal collaboration, and the diffusion of offensive capabilities (Meehan & Farmer, 2023; Broséus et al., 2016; Buxton & Bingham, 2015; Kruithof et al., 2016). These ecosystems have also been repeatedly linked to child exploitation networks, access-broker activity, and large-scale takedowns such as AlphaBay and Playpen (Cimpanu, 2016; FBI, 2017; McGoogan, 2017; Popper & Ruiz, 2017). As cyber conflict has matured into a recognized operational domain (Nichols, 2024), the Dark Web has become a strategic substrate for procurement, coordination, and covert communication.

Concurrently, the operational environment surrounding offensive cyber activity is shifting as generative AI becomes embedded in the tooling and tradecraft of modern threat actors. Research on AI-enabled cyber operations shows that these systems amplify existing offensive techniques by accelerating reconnaissance, refining target selection, and automating technically demanding tasks (Gabrian, 2024; Saade & Ng, 2024). RAND's analysis of autonomy, reasoning, and tool-integration suggests that emerging AI systems may increasingly support multi-step cyber activities and adapt to defensive measures in real time (Hodgson, Horton, & Malone, 2025). When paired with the anonymity, resilience, and illicit economies of the Dark Web, these AI-driven capabilities create a more fluid and adaptive threat landscape to one where state and non-state actors can blend, outsource, and obscure their operations with unprecedented ease. This convergence is becoming a defining feature of contemporary cyber conflict and a critical factor in understanding how offensive capabilities are acquired, deployed, and sustained.

2. Cryptographic Foundations: Onion Routing and Anonymity Architecture

The following sections provide a technical overview of onion routing and associated technologies.

2.1 Onion Routing Protocol Design

Onion routing is a layered cryptographic forwarding architecture designed to decouple message origin, routing state, and destination information across multiple independently operated network relays. In this model, a client encapsulates application traffic inside a sequence of encrypted protocol layers, where each layer corresponds to a specific relay in a selected path, conceptually resembling the nested structure of an onion (Reed, Syverson, & Goldschlag, 1998). In Tor, this path is instantiated as a circuit, usually consisting of an entry guard, one or more middle relays, and an exit relay. Before user traffic is transmitted, the Tor client performs circuit construction by incrementally extending the circuit one hop at a time. For each hop, the client negotiates a distinct ephemeral session key, historically using telescoping key agreement protocols based on public-key cryptography and, in modern Tor deployments, authenticated key exchange mechanisms that provide forward secrecy. These per-hop session keys are then used with symmetric cryptographic primitives to encrypt fixed-size Tor cells in multiple layers.

At the protocol level, the client does not simply send an IP packet through the relay chain. Instead, it fragments traffic into Tor cells, each of which contains circuit identifiers, relay commands, stream identifiers, integrity checks, and encrypted payload data (Döpmann, 2025). When the client sends a cell into the circuit, it applies layered encryption in reverse path order: first encrypting the payload for the exit relay, then wrapping that ciphertext for the middle relay, and finally encrypting the outermost layer for the entry relay. As the cell traverses the circuit, each relay uses only its own negotiated symmetric key to remove one cryptographic layer, verify the relevant integrity material, and determine the next hop. Crucially, a relay learns only the routing information necessary for local forwarding. It does not possess the cryptographic keys required to decrypt layers intended for other relays, nor does it receive a complete source-to-destination route.

This design produces strict compartmentalization of network visibility (Dutta et al., 2021). The entry guard observes the client's network address and the next relay in the circuit, but it cannot determine the final destination or inspect application-layer plaintext. The middle relay functions as a cryptographic and routing intermediary, observing only its predecessor and successor within the circuit (Döpmann, 2025). The exit relay removes the final Tor encryption layer and forwards traffic to the destination service, meaning it can observe the destination address and, unless end-to-end encryption such as TLS is used, potentially the application payload; however, it does not know the client's original IP address. Thus, anonymity is not derived from any single trusted server, but from distributing trust across relays and ensuring that no individual relay has sufficient information to correlate both communication endpoints.

The security properties of onion routing rely on the interaction between layered symmetric encryption, ephemeral key establishment, circuit isolation, and probabilistic relay selection (Döpmann, 2025). Public-key cryptography is used primarily during circuit setup to authenticate or establish shared secrets, while high-throughput data forwarding is handled by efficient symmetric encryption because relays must process large volumes of traffic with low latency (Camenisch, J., & Lysyanskaya, 2005). Ephemeral session keys provide forward secrecy: compromise of a relay's long-term identity key should not automatically reveal previously transmitted circuit traffic. Tor's use of fixed-size cells also reduces certain packet-size leakage, although it does not eliminate timing correlation attacks. Because low-latency anonymity systems must preserve interactivity, Tor cannot fully randomize packet timing or introduce large delays in the way high-latency mix networks do.

Path selection further contributes to anonymity by drawing relays from a distributed consensus of available nodes, weighted by relay capacity, policy constraints, and role suitability. Entry guards are typically reused for extended periods to reduce exposure to malicious first-hop relays, while middle and exit relays may vary across circuits. Exit relay selection is constrained by exit policies, since not all relays permit outbound connections to all ports or destinations (Camenisch, J., & Lysyanskaya, 2005). The resulting anonymity set depends on the number of users, the diversity of relay operators, relay bandwidth distribution, and the adversary's ability to observe or operate relays. If a global passive adversary can monitor both the client-to-entry link and the exit-to-destination link, traffic timing and volume correlation may still weaken anonymity despite the cryptographic protections.

Recent analyses of AI-enabled cyber operations highlight how adversaries increasingly pair traditional anonymity architectures with AI-driven reconnaissance and automation tools to streamline circuit construction, evade detection, and optimize routing behavior (Gabrian, 2024). RAND's assessment of autonomy and tool-integration

further suggests that future AI systems may assume more active roles in route selection, traffic shaping, and relay-level evasion, enhancing the operational resilience of onion-routed communications (Hodgson, Horton, & Malone, 2025). These developments indicate that while the core cryptographic design remains stable, the operational use of onion routing is evolving alongside AI-enabled offensive tradecraft

2.2 Traffic Analysis and Limitations

While onion routing provides strong resistance to single-point compromise, it is not invulnerable. Adversaries capable of large-scale traffic correlation monitoring both entry and exit nodes can conduct timing analysis to probabilistically deanonymize users (McCoy et al., 2008; Nurmi & Niemelä, 2017). Intelligence agencies have historically bypassed Tor's cryptographic protections through network investigative techniques (NITs), browser exploits, and endpoint compromise, demonstrating that anonymity networks protect routing metadata but not the security posture of the device itself (Paganini, 2015; Schneier, 2013). AI-enabled tooling is intensifying these risks. Gabrian (2024) notes that machine-learning models now accelerate traffic-pattern recognition and automate correlation attacks, identifying subtle timing or volume anomalies that human analysts might overlook.

RAND's assessment reinforces this trajectory, emphasizing that as AI systems gain more advanced reasoning and tool-integration capabilities, they may increasingly support multi-step offensive actions including reconnaissance, exploitation, and traffic analysis—within anonymized environments (Hodgson, Horton, & Malone, 2025). These developments suggest that the threat surface surrounding onion-routed traffic is evolving not because the cryptographic design has weakened, but because adversaries now possess more capable analytical tools. Despite these vulnerabilities, Tor's architecture remains sufficiently robust to provide operational-grade anonymity for actors who combine it with disciplined OPSEC practices such as compartmentalization, cryptocurrency obfuscation, and endpoint hardening.

3. How the Dark Web is Used in Cyber Warfare

Style and Maglaras (2020) define cyber warfare as the use of digital operations to target states or non-governmental entities, noting that virtual actions can produce tangible physical effects. Boyte et al. (2020) demonstrate this reality through cyberattacks on Ukraine from 2013–2015 that disrupted power grids, satellite communications, and weapons systems. Recent analyses further show that generative AI is accelerating offensive capability development by enhancing reconnaissance, vulnerability discovery, and malware adaptation, expanding the operational reach of cyber actors (Gabrian, 2024; Hodgson, Horton, & Malone, 2025).

Dark web marketplaces operate as semi-structured ecosystems for acquiring malware, zero-day exploits, and access credentials outside formal state channels (Hasanti et al., 2024). Reputation systems and escrow mechanisms help sustain trust in an anonymous environment, lowering the technical and economic barriers to sophisticated cyber tools. This commodification accelerates the proliferation of offensive capabilities once limited to nation-states, enabling both state and non-state actors to adopt advanced techniques more rapidly (Pavlovskaia & Belousov, 2024). The dark web also supports recruitment and coordination through anonymity-preserving architectures and global accessibility. State-linked groups and independent contractors advertise services, solicit collaborators, and form loosely organized collectives oriented toward political or financial objectives. This decentralized model complicates attribution, distributing operational tasks across actors with diverse motivations and producing hybrid campaigns that blur the line between state operations and criminal entrepreneurship.

Adversaries further leverage Dark Web hidden services to establish resilient command-and-control infrastructures (Gaber & Ahmed, 2026). Layered encryption and pseudonymous routing obscure server locations and operator identities, enhancing operational survivability. By decoupling C2 infrastructure from conventional hosting, Dark Web based architectures reduce the effectiveness of takedown efforts and complicate forensic analysis, contributing to the persistence and stealth of modern malware campaigns.

The Dark Web also serves as a repository of illicit data and cyber-threat intelligence (Kühn, Wittorf, & Reuter, 2024). Actors obtain compromised credentials, network access, and proprietary information that facilitate initial intrusion or accelerate reconnaissance. Monitoring dark web forums reveals emerging vulnerabilities, criminal collaborations, and evolving attack methodologies, complementing traditional intelligence collection and supporting long-term infiltration strategies used by state-sponsored APT groups. In information warfare, the Dark Web functions as a staging ground for disinformation and psychological operations. Its anonymous infrastructure enables the distribution of leaked or fabricated materials, coordination of influence networks, and propagation of ideologically charged narratives without clear attribution. Because these activities often migrate

to mainstream platforms, Dark Web operations can exert disproportionate influence, illustrating the convergence of cyber and cognitive warfare.

Cryptocurrency based financial systems embedded within the Dark Web provide the economic substrate for illicit cyber operations (Jung et al., 2022). Anonymous payments support malware procurement, infrastructure leasing, and contractor labor, while laundering mechanisms obscure transactional provenance. This financial opacity enhances the strategic autonomy of state and non-state actors engaged in cyber warfare and frustrates counter-financial intelligence efforts. The Dark Web mediates complex interactions between state actors and criminal organizations, fostering hybrid ecosystems where capabilities, intelligence, and operational services are exchanged with minimal visibility. States may outsource cyber activities to criminal proxies to achieve plausible deniability, while criminal groups may receive protection or technical support in exchange for aligning their operations with state interests. Cyber terrorism encompasses terrorist activity conducted through digital networks, including system attacks, online propaganda, psychological operations, fundraising, recruitment, and operational coordination (Lucas, 2020).

4. The Nexus of AI, Dark Web, and Cyber Warfare

The integration of Artificial Intelligence (AI) into Dark Web ecosystems has reshaped the operational landscape of cyber warfare by enabling autonomous, adaptive, and scalable capabilities under conditions of strong anonymity and reduced attribution (Kela, 2025). Within Tor and mix-net infrastructures, AI-driven systems support automated reconnaissance, threat-intelligence generation, and offensive cyber operations. Machine-learning model, ranging from supervised classifiers to deep neural networks, analyze Dark Web traffic, forum communications, and marketplace telemetry to identify vulnerabilities, zero-day opportunities, and adversarial behavioral patterns. Transformer-based NLP enables automated extraction of intent, ideological alignment, and operational indicators from unstructured extremist discourse, supporting cyber-enabled psychological operations and coordinated attack planning. These capabilities allow state and non-state actors to execute AI-augmented campaigns that dynamically adapt malware payloads, C2 structures, and attack vectors in response to defensive countermeasures, compressing the cyber kill chain. Gabrian (2024) underscores this shift, noting the widespread availability of AI-driven hacking tools on the Dark Web, while RAND's assessment of autonomy, reasoning, and tool-integration suggests that emerging AI systems may soon assume more complex operational functions within anonymized environments (Hodgson, Horton, & Malone, 2025).

From an offensive cyber-warfare perspective, the Dark Web operates as a distributed marketplace for AI-enabled cyber weapons and services, accelerating capability diffusion through models such as Malware-as-a-Service (MaaS), Phishing-as-a-Service (PhaaS), and Disinformation-as-a-Service (DaaS) (Ciancaglini et al., 2025). Reinforcement learning algorithms optimize attack strategies including lateral movement, privilege escalation, and IDS/SIEM evasion, while generative AI produces polymorphic malware, adversarial phishing content, and synthetic media for hybrid information operations. Defensive and intelligence organizations counter with AI-based monitoring frameworks that combine graph analytics, anomaly detection, and behavioural fingerprinting to infer adversarial networks, trace illicit financial flows, and anticipate cyber terrorist activity despite encrypted and pseudonymous conditions. This dual-use dynamic reinforces Gabrian's (2024) warning that AI-enabled cyber capabilities materially elevate national-security risk and highlights the need for governance mechanisms capable of addressing AI-driven escalation(Kela, 2025).

The convergence of AI and the Dark Web also accelerates the commodification of cyber capabilities. AI-powered tools for malware automation, phishing, and disinformation are increasingly traded in Dark Web markets, lowering the technical threshold for sophisticated attacks. Defensive actors employ AI-enabled analytics to detect weak signals of emerging threats and attribute malicious activity through behavioral and network-based inference rather than identity-centric methods. This adversarial co-evolution positions the Dark Web as a contested battlespace where AI simultaneously enables asymmetric warfare and supports counter-terrorism and cyber-intelligence operations. The absence of unified international legal frameworks governing AI-enabled cyber conflict further amplifies these challenges.

AI-enabled exploitation of Dark Web infrastructures aligns with NATO cyberspace-operations doctrine, functioning as an enabler of Cyberspace Intelligence, Surveillance, and Reconnaissance (C-ISR) and effects generation within joint operations. NATO's AJP-3.20 maps naturally onto AI-supported pipelines for indexing hidden services, inferring entities under pseudonymity, and conducting operational preparation of the environment (NATO, 2020). Graph learning, representation learning, transformer-based NLP, and anomaly detection accelerate indicator-to-warning conversion by extracting operational signals such as capability acquisition, malware diffusion, and recruitment surges from adversary-controlled ecosystems. In contexts

where the Dark Web facilitates terrorist coordination, propaganda, and fundraising, AI-driven automation enables monitoring and triage at scale, shifting analysis from identity-based attribution toward behavioural and infrastructural attribution.

From a U.S. DoD perspective, AI + Dark Web integration aligns with joint cyberspace-operations doctrine and the 2023 DoD Cyber Strategy's emphasis on defending forward and persistent engagement (DoD, 2023). Technically, this manifests as AI-accelerated kill-chain compression: automated reconnaissance, ML-assisted vulnerability discovery, and adaptive C2 and payload delivery leveraging Dark Web anonymity for staging and logistics. Defensive applications mirror this with AI-enabled hunt-forward analytics—graph embeddings to infer operational cells, clustering to detect emergent TTPs, NLP to identify operational intent, and blockchain analytics to map illicit finance pathways. These outputs feed joint targeting and campaign assessment, enabling disruption to be measured not only by takedowns but by changes in adversary access, resiliency, and TTP substitution under persistent engagement.

5. Operational Telemetry and Risk Quantification

Quantifying risk and assessing operational telemetry is key to understanding the nexus between the Dark Web, AI, and cyber warfare.

5.1 Macro-level Loss and Breach Telemetry

Operational risk modeling for Dark Web–mediated, AI-enabled intrusion must be anchored in empirical telemetry. At the macro level, incident-reporting data provides coarse but decision-useful bounds for expected loss. The FBI's Internet Crime Complaint Center (IC3) reported aggregate victim losses exceeding US$16 billion in 2024, a 33% increase relative to 2023, and indicates that cyber-enabled fraud accounts for the dominant share of losses. These macro-signals are not directly attributable to Dark Web activity; however, they contextualize the economic scale available to access brokers, malware operators, and monetization crews operating within anonymized ecosystems (FBI, 2025).

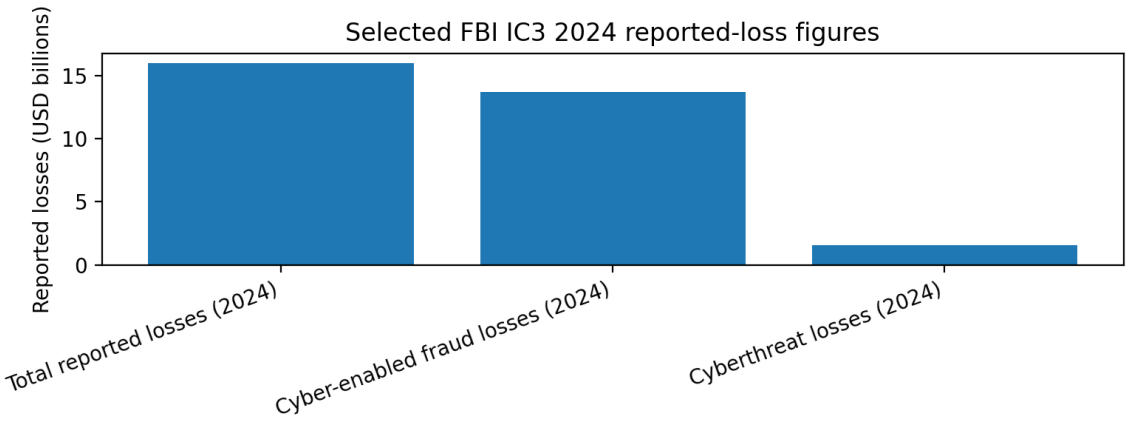

Figure 1: Selected FBI IC3 2024 reported-loss figures (values in USD billions) (FBI, 2025).

5.2 Capability Taxonomy Observed in Dark Web Markets

Dark Web markets commoditize discrete capability primitives that can be composed into full-spectrum campaigns. Table 1 provides an engineering taxonomy that maps common marketplace offerings to kill-chain phases and to representative defensive control families (e.g., identity hardening, vulnerability management, egress filtering).

Table 1: Engineering taxonomy of Dark Web capability primitives

Capability class	Typical market artefact/service	Kill-chain impact	Defensive control mapping
Initial access brokerage	Compromised VPN/RDP accounts; stealer logs; session cookies	Recon → Initial access	MFA, conditional access, credential hygiene, UEBA
Exploit enablement	N-day exploit chains; PoCs; exploit kits	Exploit	Patch SLAs, virtual patching, WAF/IPS signatures

Capability class	Typical market artefact/service	Kill-chain impact	Defensive control mapping
Payload delivery	Malware loaders; droppers; macro builders; email templates	Delivery/Install	Secure email gateway, sandboxing, attachment detonation
C2 resilience	Onion service C2; bulletproof hosting; fast-flux DNS	C2	Egress allowlists, TLS/JA3 fingerprinting, sinkholing
Monetization	Ransomware affiliates; crypto laundering; mule recruitment	Actions on objectives	Immutable backups, fraud analytics, blockchain tracing

5.3 Indicative Kill-chain Compression Under AI Augmentation

AI-assisted automation disproportionately accelerates early kill-chain phases by reducing human-in-the-loop latency for reconnaissance, target selection, content generation, and exploit parameterization. Figure 2 presents an illustrative (non-empirical) compression model intended to communicate the directionality of the effect: procurement and automation decrease cycle time per stage, increasing the number of parallelized intrusion attempts an actor can execute under a fixed resource budget (Hodgson, Horton, & Malone, 2025).

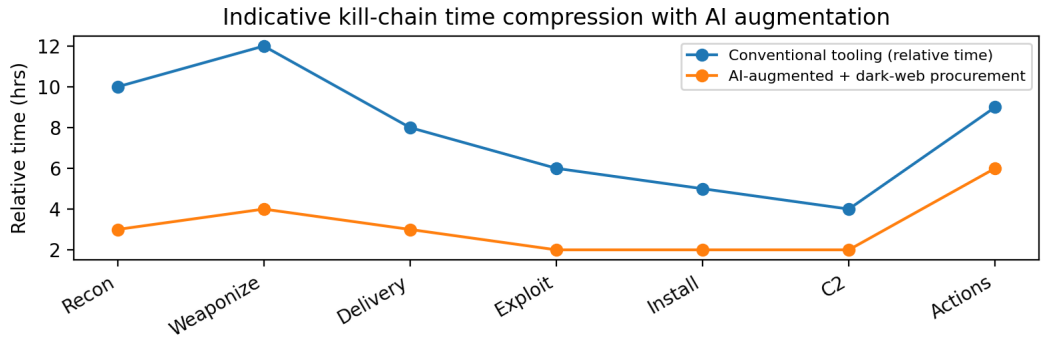

Figure 2: Indicative kill-chain time compression with AI augmentation (conceptual model) (Hodgson, Horton, & Malone, 2025)

5.4 Breach Telemetry Relevant to Initial-access Vectors

Independent breach investigations provide higher-fidelity indicators about prevailing initial-access vectors. Verizon's 2025 DBIR reports a 34% year-over-year increase in attackers exploiting vulnerabilities for initial access, finds that only 54% of perimeter-device vulnerabilities were fully remediated over the past year, and notes that ransomware was present in 44% of analyzed breaches (Verizon, 2025). These findings are operationally aligned with Dark Web market dynamics: access brokers monetize unpatched edge devices and compromised identities, while ransomware ecosystems externalize capability development through affiliate models.

Table 2: Selected cyber-risk telemetry informing Dark Web threat models

Telemetry indicator	Reported value	Engineering implication
Reported victim losses (IC3, 2024)	US$16B+	Macro-scale economic incentive for illicit capability markets
Cyber-enabled fraud losses (IC3, 2024)	US$13.7B	Monetization pressure favors credential theft and social engineering
Cyberthreat losses (IC3, 2024)	US$1.571B	Ransomware/data-breach ecosystems continue to scale
Perimeter vulns fully remediated (DBIR 2025)	54%	Patch latency creates durable exploit windows for access brokers
Ransomware presence in breaches (DBIR 2025)	44%	Affiliates profit from commoditized access and tooling
YoY increase in vulnerability exploitation (DBIR 2025)	34% increase	Prioritize attack-surface reduction for edge assets

6. Conclusions

The Dark Web has evolved from a privacy-enhancing communication layer into a strategic substrate for contemporary cyber warfare, mirroring the argument established in the introduction. Its anonymity architecture, marketplace economies, hidden-service infrastructures, and cryptocurrency systems collectively enable the procurement, coordination, and sustainment of offensive and defensive cyber operations. The integration of Artificial Intelligence amplifies these dynamics by accelerating reconnaissance, automating vulnerability discovery, and enabling adaptive adversarial behaviors that compress the cyber kill chain. As Gabrian (2024) observes, AI-driven hacking tools and automated malware kits are increasingly accessible within Dark Web ecosystems, while RAND's assessment of autonomy, reasoning, and tool-integration suggests that emerging AI systems may soon assume more complex operational functions within anonymized environments (Hodgson, Horton, & Malone, 2025). Together, these developments reinforce the introduction's central claim: the Dark Web is no longer a peripheral criminal enclave but a core operational environment within modern cyber conflict.

Within NATO and U.S. doctrinal frameworks, the Dark Web must therefore be conceptualized as a contested battlespace embedded within persistent cyberspace competition. Its infrastructures enable hybrid operations that blend espionage, information warfare, and cyber-enabled coercion under conditions of reduced attribution precisely the convergence highlighted in the introduction. As AI-enabled automation continues to reshape offensive and defensive tradecraft, doctrinal approaches must integrate intelligence fusion, rapid decision advantage, and persistent engagement to counter adversaries who leverage anonymity-preserving ecosystems for strategic effect. Future research must address the governance of AI-enabled cyber capabilities, the development of attribution methodologies capable of operating under pseudonymity, and the establishment of international norms regulating cyber-enabled hybrid warfare conducted through anonymity-preserving infrastructures. Advancing these areas is essential to ensure that emerging AI-driven capabilities do not outpace the legal, ethical, and strategic frameworks required to manage them.

Ethics declaration: This research did not involve human subjects and thus no ethical clearance was required.

AI declaration: This research did not use any AI.

References

Akhgar, B., 2021. Case Study: Dark Web Markets. *Dark Web Investigation*, p.237.

Camenisch, J., & Lysyanskaya, A. 2005, 'A formal treatment of onion routing' In Annual International Cryptology Conference, pp. 169-187.

Chawki, M., 2022. The Dark Web and the future of illicit drug markets. *Journal of Transportation Security*, *15*(3), pp.173-191.

Ciancaglini, V., & Sancho, D. 2025. The State of Criminal AI: Market Consolidation and Operational Reality. Trend Micro Research. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-criminal-ai>

DoD, 2023. 2023 Department of Défense Cyber Strategy <https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf>

Döpmann, C., 2025. *On the Evolution of Onion Routing Networks*. Technische Universitaet Berlin (Germany).

Dutta, N., Jadav, N., Tanwar, S., Sarma, H.K.D. and Pricop, E., 2021. Tor—the onion router. In Cyber security: Issues and current trends (pp. 37-55). Singapore: Springer Singapore.

El-Kady, R., 2025. Decoding the dark: AI and ML in the dark web cybercrime and cryptocurrency forensics. International Cybersecurity Law Review, 6(2), pp.107-143.

FBI 2017. 'Playpen' Creator Sentenced to 30 Years', <https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years>.

FBI 2025, 'FBI Releases Annual Internet Crime Report', Federal Bureau of Investigation, viewed 2026-03-02, <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>.

FBI Internet Crime Complaint Center (IC3) 2024, Internet Crime Report 2024, IC3, viewed 2026-03-02, <https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf>.

Gaber, M. and Ahmed, M., 2026. The Underbelly of Cyber Espionage. In *Cyber Espionage and National Security Challenges: Cyber Wargaming for Critical Infrastructures* (pp. 65-91). Cham: Springer Nature Switzerland.

Gabrian, C. A. (2024). Unveiling the Dark Side: How Hackers Exploit Artificial Intelligence for Cyber Warfare. Euro-Atlantic Resilience Journal, 2(3).

Hasanti, F., Osman, M.Z., Rahman, M.H., Darus, M.Z.A. and Mohd, N.B., 2024, December. A Comprehensive Study on Emerging Trends of Dark Web Marketplaces and Forums. In 2024 IEEE International Conference on Computing (ICOCO) (pp. 356-361). IEEE.

Hodgson, Q. E., Horton, K., & Malone, M. J. (2025). Facing the artificial intelligence–cyber nexus: A structured approach to government decisionmaking to address emerging artificial intelligence capabilities for cyber attacks (RR-A4250-1). RAND Corporation. https://www.rand.org/t/RRA4250-1

Ireland, L. and Jardine, E., 2024. Drug transactions and the dark web: Public perceptions of the locational setting of offenders and support for drug policy outcomes. *International Journal of Drug Policy*, *123*, p.104286

Jiang, S., Chen, G. and Wang, T., 2025, July. Governance of Dark Web Crimes from the Perspective of a Holistic Approach to National Security. In *2025 11th International Conference on Humanities and Social Science Research (ICHSSR 2025)* (pp. 1405-1418). Atlantis Press.

Jin, P., Kim, N., Lee, S. and Jeong, D., 2024. Forensic investigation of the dark web on the Tor network: pathway toward the surface web. *International Journal of Information Security*, *23*(1).

Jung, B.R., Choi, K.S. and Lee, C.S., 2022. Dynamics of dark web financial marketplaces: An exploratory study of underground fraud and scam business. Dynamics, 8, pp.22-2022.

KELA. 2025 AI Threat Report: How Cybercriminals Are Weaponizing AI Technology. KELA Cyber Threat Intelligence. <https://info.ke-la.com/hubfs/Reports/KELA%20Report%20-%202025%20AI%20Threat%20Report.pdf>

Kruithof, K., Aldridge, J., Hétu, D. D., Sim, M., Dujso, E., & Hoorens, S. 2016, 'The role of the dark web in the trade of illicit drugs' Rand publication. Viewed April 12, 2018 <https://www.rand.org/pubs/research_briefs/RB9925.html>.

Kühn, P., Wittorf, K. and Reuter, C., 2024. Navigating the shadows: Manual and semi-automated evaluation of the dark web for cyber threat intelligence. *IEEE Access*, *12*, pp.118903-118922.

Lucas, G. (2020). Cybersecurity and Cyber Warfare: The Ethical Paradox of 'Universal Diffidence'. In The Ethics of Cybersecurity (pp. 245-258). Cham: Springer International Publishing.

Meehan, B. and Farmer, N., 2023. Dark web drug markets and cartel crime. Review of Law & Economics, 19(3), pp.317-350

Moggridge, E. and Montasari, R., 2022. A critical analysis of the dark web challenges to digital policing. In *Artificial intelligence and national security* (pp. 157-167). Cham: Springer International Publishing.

NATO 2020, AJP-3.20 Allied Joint Doctrine for Cyberspace Operations (Edition A, Version 1), UK Government (hosting), viewed 2026-03-02, <https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf>.

Nichols, R. A. (2024, December). Cyber Progression of the Domains of Warfare. In International Conference on Computational Science and Computational Intelligence (pp. 64-76). Cham: Springer Nature Switzerland.

Nurmi, J., & Niemelä, M. S. 2017, 'Tor De-anonymization Techniques'. In International Conference on Network and System Security, pp. 657-671.

Paganini, P. 2015, 'A look to the "NIT Forensic and Reverse Engineering Report, Continued from January 2015". NIT code was used by the FBI to deanonymize Tor users.' Security Affairs. Viewed May 2, 2018 <http://securityaffairs.co/wordpress/38213/cyber-crime/nit-fbi-deanonymize-tor.html>.

Pavlovskaia, A., and Belousov, V., 2024. Dark Deals: Unveiling the Underground

Market of Exploits. <https://www.virusbulletin.com/uploads/pdf/conference/vb2024/papers/Dark-deals-unveiling-the-underground-market-of-exploits.pdf>

Popper, N, Ruiz, R. 2017, '2 Leading Online Black Markets Are Shut Down by Authorities' New York Times. Viewed May 2, 2018 <https://www.nytimes.com/2017/07/20/business/dealbook/alphabay-dark-web-opioids.html>.

Saade, T., & Ng, A. A. (2024). Generative artificial intelligence and offensive cyber-operations: A literature review [Manuscript]. Stanford University; CrowdStrike.

Style, M. P., & Maglaras, L. (2020). The Current Posture of Cyber Warfare and Cyber Terrorism. Global Foundation for Cyber Studies and Research, 3.

Tor Project 2026, Tor Metrics, Tor Project, viewed 2026-03-02, <https://metrics.torproject.org/>.

Verizon 2025, 2025 Data Breach Investigations Report (DBIR) resource page, Verizon Business, viewed 2026-03-02, <https://www.verizon.com/business/resources/reports/dbir/>.