CENTRE FOR GLOBAL STUDIES

A Program of Parliamentary Assembly of the Mediterranean

# The Dark Web - Spyware Nexus: Implications for National Security And Human Rights

Report:

# The Dark Web-Spyware Nexus: Implications for National Security And Human Rights

*San Marino, 24 June 2026*

*Disclaimer: This document is prepared by the researchers of the Centre for Global Studies (CGS) of the Parliamentary Assembly of the Mediterranean (PAM) in San Marino in their personal capacity. The opinions expressed in the note are the authors' own and may not reflect the views of PAM. This report underwent AI-assisted linguistic review.*

**Index**

## Executive Summary

This report, The Dark Web-Spyware Nexus: Implications for National Security and Human Rights, is the second study in a strategic research project on the misuse of spyware technologies produced by the Senior Researchers at the Center for Global Studies (PAM-CGS) of the Parliamentary Assembly of the Mediterranean (PAM). It has been prepared in cooperation with the Counter-Terrorism Executive Directorate (CTED) of the United Nations Security Council. The PAM and PAM-CGS research project on the evolution of surveillance technologies, particularly spyware, amidst the ongoing technological revolution, is guided by the core principles and strategic directives of the United Nations. The first report of the PAM-CGS research project, titled Spyware Misuse: Legislative, Governance, and Judicial Considerations, Historical Evolution, and Technical Insights, published on 18 December 2025[1], and peer-reviewed by international experts, asserts that the misuse of increasingly AI-driven spyware significantly impacts the dynamics among institutional powers. In this regard, it is crucial to enhance information ecosystems within social and institutional frameworks by following to the United Nations Global Principles for Information Integrity. Strategic research should be included in the UN Global Digital Compact, part of the Pact for the Future, adopted at the Summit of the Future in New York on 22 September 2024[2]. The OHCHR, UN Special Rapporteur on the Promotion and Protection of Human Rights While Countering Terrorism, and UN Security Council's high-level Arria-formula seminar "Commercial Spyware and the Maintenance of International Peace and Security" on 14 January 2025 are notable in this regard[3].

The analysis, at the base of the present report, examines the growing convergence between the dark web and the spyware industry, an emerging nexus that is reshaping the global digital threat landscape. The dark web no longer functions solely as an illicit marketplace; it now operates as a covert hub where commercial spyware, surveillance tools, and stolen data are traded, tested, and deployed outside state oversight. The symbiosis between anonymity networks and invasive technologies enables both state and non-state actors to conduct intelligence-style operations with unprecedented reach, eroding privacy, sovereignty, and human rights. Within this ecosystem, individuals become both targets and instruments, subjected to psychological

[1] Center for Global Studies (CGS) & Parliamentary Assembly of the Mediterranean (PAM). (18 December 2025). *Spyware misuse report: Implications for national security and human rights*. https://pam.int/wp-content/uploads/2025/12/PAM-CGS-Spyware-Misuse-Report.-10-Dec-2025-1204pm.pdf

[2] United Nations. (2024, 22 September). *Global Digital Compact*. United Nations. https://www.un.org/digital-emerging-technologies/global-digital-compact

[3] United Nations Security Council. (2025, 14 January). *Commercial spyware and the maintenance of international peace and security* [Arria-formula meeting]. UN Web TV. https://webtv.un.org/en/asset/k1j/k1jteho6fm

manipulation, data extraction, or coerced participation in digital espionage. Corrupt intermediaries across sectors, including law enforcement, healthcare, logistics, and trade, facilitate the movement of information, resources, and sometimes even of chemical materials that have the dual-use substances that may be diverted for the production of chemical weapons, as well as pharmaceutical and medical-grade compounds that can be misused in the illicit manufacture of narcotic drugs that sustain these covert operations. Artificial intelligence further compounds these risks by automating reconnaissance, personalizing deception strategies, and accelerating recruitment within hidden online communities. Economically, these mechanisms might destabilize markets, undermine governance, and transform cyber exploitation into a self-sustaining underground economy. To strengthen trust, accountability, and human rights in the digital domain, the report identifies several strategic priorities: (i) the gradual development of a secure global network architecture modelled on adaptive security principles; (ii) voluntary disclosure and protection programs for coerced members; and (iii) the formation of highly vetted international teams for controlled infiltration and intelligence recovery. Together, these measures seek to limit the convergence of spyware and dark-web ecosystems and reinforce the resilience of national and international security frameworks.

## Introduction

1- The senior researchers of the Center for Global Studies (PAM-CGS) of the Parliamentary Assembly of the Mediterranean (PAM) have complied this report in cooperation with the United Nations Security Council Counter Terrorism Executive Directorate (CETD). The report investigates the evolution of the "Dark Web" from a concealed marketplace to a sophisticated and decentralized digital ecosystem. It emphasizes how this evolution has facilitated the emergence of covert communities, psychological manipulation, and the deployment of advanced spyware tools that pose significant threats to national security, individual privacy, and global stability.

2- In the present day, the dark web functions as a parallel intelligence network with its own internal hierarchy and operational reach, which is increasingly intersecting with real-world environments and institutions. These developments call for enhanced action and coordination between international organizations, law enforcement, and policymakers.

## Understanding the Dark Web: Structure, Function, and Security Implication

3- The dark web is a concealed and encrypted layer of the internet, which is accessible only through specialized anonymity networks such as Tor and I2P, creating an environment where identities, locations, and digital pathways remain largely untraceable[4]. While originally designed to safeguard privacy and freedom of expression, the dark web has evolved into a decentralized ecosystem hosting illicit markets, covert fora, and advanced surveillance tools that enable actors to conduct intelligence-relevant activities beyond traditional oversight[5]. Within this hidden sphere, criminal and extremist groups, as well as proxy entities, engage in the acquisition of sensitive data, deployment of sophisticated spyware, challenge-based targeting, psychological manipulation and cross-border coordination. Its architecture facilitates undetectable reconnaissance, anonymized financial transactions[6], and the misuse of everyday digital traces of ordinary individuals, thereby transforming the dark web into a parallel intelligence system with significant implications for national security, public safety, and human rights[7]. A persistent misconception among

[4] Finklea, K. (02 December 2024). *The dark web: An overview* (CRS Report No. IF12172). Congressional Research Service. https://www.congress.gov/crs_external_products/IF/PDF/IF12172/IF12172.3.pdf

[5] Sagrera, E. (03 August 2025). *How national security agencies exploit the dark web*. H25.io. https://www.h25.io/dark-web/how-national-security-agencies-exploit-the-dark-web/

[6] Kumar, R. (19 January 2025). *Dark Web and crypto: Challenges for national security*. IndustryWired. https://industrywired.com/cryptocurrencies/dark-web-and-crypto-challenges-for-national-security-8634495

[7] Jawed, A., & Khan, M. A. (15 June 2025). *Dark Web marketplaces: Monitoring and intervention strategies*. *International Journal of Law Management & Humanities, 8*(3), 2007–2014. https://ijlmh.com/wp-content/uploads/Dark-Web-Marketplaces-Monitoring-and-Intervention-Strategies.pdf

authorities and the wider public is that the dark web is confined to large-scale criminal markets, when in reality its reach extends into the smallest elements of daily life, affecting ordinary individuals through subtle forms of surveillance, manipulation, and exploitation. To contextualize the operational breadth of this environment, the primary service clusters that structure dark-web activity can be outlined as follows:

**Table 1: Dark Web Service Categories and Their Operational Functions**[8]

| **Category** | **Description of Services Provided** | **Relevance to Spyware/ Intelligence Activities** |
|---|---|---|
| Illicit marketplaces | Trade in narcotics, weapons, forged documents, counterfeit pharmaceuticals, stolen data, chemical precursors | Creates supply channels for hostile actors and enables access to sensitive materials used in surveillance or coercion |
| Cybercrime-as-a-service | Hacking-for-hire, malware and exploit kits, botnet rentals, phishing frameworks, SIM-swap services | Allows non-state actors to acquire intrusion capabilities previously available only to state agencies |
| Spyware and surveillance tools | Remote access trojans, mobile spyware, keyloggers, IoT exploitation tools, hijacked cameras and microphones | Directly enables covert monitoring, data extraction, and operational intelligence |
| Human-targeting services | Doxing, stalking-for-hire, harassment missions, challenge-based targeting, deepfake production | Supports psychological manipulation and personal coercion operations |
| Financial anonymity and laundering | Crypto mixers, anonymous wallets, illicit escrow, laundering pipelines | Supports ransomware operations, cross-border payments, and concealment of funding flows |
| Proxy operational support | Smuggling logistics, border facilitation, corrupted port-access services, counterfeit supply-chain networks | Strengthens covert mobility, movement of materials, and deniable operations |
| Extremist and insurgent facilitation | Encrypted forums, propaganda channels, recruitment pipelines, operational manuals | Enables radicalization, coordinated targeting, and cross-border mobilization |
| Disinformation and destabilization operations | Fabricated evidence markets, reputation attacks, coordinated influence campaigns | Used to intimidate targets, manipulate narratives, or weaken institutional trust |

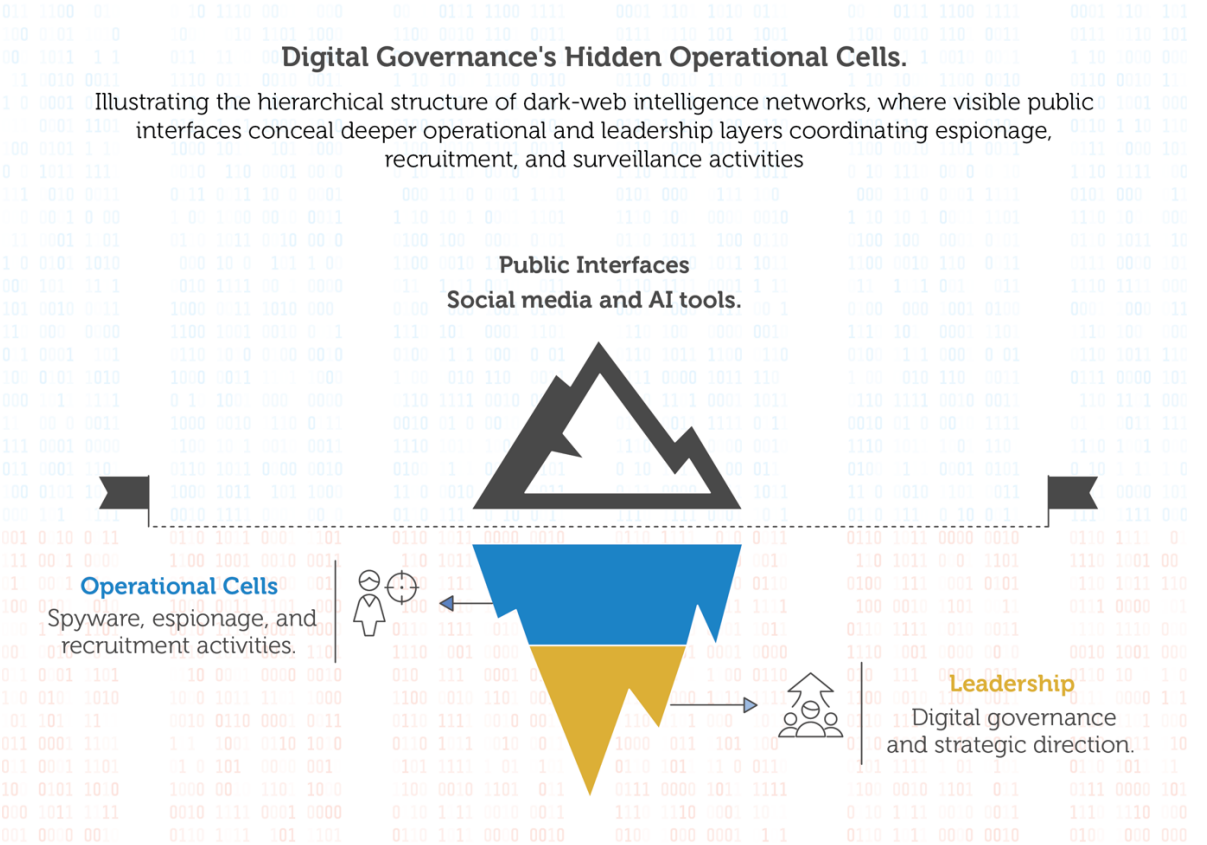
[8] The following chapters examine how these clusters interconnect to sustain covert digital ecosystems.

**Transformation of the Dark Web into a Covert Intelligence Network**

4- The dark web has undergone a significant evolution, transitioning from a decentralized marketplace for illicit goods into a sophisticated ecosystem that facilitates covert intelligence operations. This transformation is marked by the emergence of organized cybercriminal communities, clandestine forums, and encrypted communication channels that enable the coordination of surveillance, espionage, and psychological manipulation.

5- Dark web fora now serve as incubators for threat actor, where knowledge sharing, recruitment, and strategic planning occur beyond the reach of conventional law enforcement agencies and cybersecurity tools. These platforms host discussions on malware development, exploit trading, and operational tactics, effectively functioning as underground intelligence hubs[9].

**Figure 1: Digital Governance's Hidden Operational Cells[10]**




6- The architecture of the dark web, built on anonymizing technologies such as Tor and I2P, provides a secure environment for these activities. The use of multi-layered encryption and

[9] Gowda, M. C. V. (7 June 2025). *Cybersecurity's hidden war: Dark web intelligence*. Ampcus Cyber. https://www.ampcuscyber.com/blogs/cybersecurity-hidden-war-dark-web-intelligence/

[10] Graphic compiled by the CGS research team, based on the analysis presented in this report.

decentralized routing ensures that identities and locations remain concealed, allowing actors to operate with impunity[11].

7- Moreover, intelligence gathering from the dark web has become a strategic priority for cybersecurity and counterterrorism agencies. Monitoring these hidden networks enables early detection of planned cyberattacks, identification of compromised data, and profiling of threat actors[12]. Law enforcement and private-sector analysts increasingly rely on dark web intelligence to anticipate and mitigate threats before they materialize[13].

8- The convergence of anonymity, global reach, and organized structure has led to the formation of what some experts describe as digital governments within the dark web. These entities exhibit hierarchical control, internal governance, and operational discipline, resembling state-like behavior in cyberspace[14].

9- This transformation underscores the urgent need for enhanced international cooperation, advanced monitoring technologies, and robust legal frameworks to counter the growing influence of the dark web as a covert intelligence network.

**Psychological Manipulation and Recruitment Mechanisms**

10- Recruitment into dark web communities frequently involves psychological manipulation, coercion, and the strategic use of fear. These tactics are designed to compromise individuals emotionally and mentally, creating a cycle of dependency that ensures continued participation and loyalty.

11- The individuals drawn into these networks vary widely, including vulnerable youths, ordinary social-media users, persons with emotional or psychological instability, and those seeking belonging or validation. Because of their continued involvement, it becomes difficult to withdraw from it due to the psychological manipulation[15], coercive tasks, dependency mechanisms, and fear of retaliation resulting from shared illicit activity[16]. Once trapped, these individuals are exploited for a range of purposes, including data

---

[11] Check Point Software Technologies. (8 October 2025). *Dark web surveillance*. Check Point Cyber Hub. https://www.checkpoint.com/cyber-hub/cyber-security/dark-web-monitoring/dark-web-surveillance/

[12] SpecialEurasia. (8 April 2025). *OSINT: Practices for deep/dark web intelligence collection*. https://www.specialeurasia.com/2025/04/08/osint-deep-dark-web/

[13] StealthMole. (23 October 2023). *Beneath the surface: Extracting threat intelligence from the dark web*. https://www.stealthmole.com/blog/beneath-the-surface-extracting-threat-intelligence-from-the-dark-web

[14] Lee, S. (25 May 2025). *The dark web's influence on organized crime*. Number Analytics. https://www.numberanalytics.com/blog/dark-web-influence-organized-crime

[15] NeuroLaunch Editorial Team. (14 September 2024). *Fear of retaliation: Psychological impacts and coping strategies*. NeuroLaunch. https://neurolaunch.com/fear-of-retaliation-psychology/

[16] Robinson, T. (15 September 2025). *The hidden pipeline: How dark web extremists exploit America's youth into becoming future killers*. PowerMentor. https://www.powermentor.org/blog/the-hidden-pipeline-how-dark-web-extremists-exploit-americas-youth-into-becoming-future-killers

collection, stalking or surveillance tasks, digital harassment, dissemination of manipulated content, and operational support within broader illicit or intelligence-linked agendas[17].

12- Cybercriminals operating within the dark web often exploit psychological vulnerabilities through social engineering techniques. These include impersonation, emotional appeals, and fabricated scenarios that pressure individuals into reveling sensitive information or performing compromising actions[18]. Once initial trust established, new recruits are subjected to loyalty tests, which may involve illegal or unethical tasks that them to the community through shared culpability[19]. Many individuals, however, do not enter these networks voluntarily. In numerous cases, coercion is initiated by someone within the individual's own social circle who is already involved. This occurs through the deliberate acquisition or exchange of personal data, photographs, messages, or digital interactions that can later be weaponized. Such material is used to exert pressure through threats of exposure, reputational harm, or legal consequences unless specific instructions are followed. In some cases, this material originates from compromised social-media or messaging-platform accounts, where private conversations and personal communications are unlawfully accessed and subsequently used to blackmail, intimidate, or coerce individuals into further involvement. Once an individual complies with even a single request or task, this initial participation itself becomes a source of leverage, as any subsequent interaction can be cited as further evidence for renewed pressure or blackmail. Over time, this process creates a sustained cycle of coercion in which disengagement becomes increasingly risky, effectively trapping individuals in continued compliance within the dark-web environment.

13- To illustrate how individuals become entangled in dark-web ecosystems through coercion and manipulation, it is useful to consider a model like the pyramid-style recruitment strategy known from schemes[20] such as QNet[21]. In such structures, participants are encouraged to "buy one item and bring three," triggering an exponential chain-three become nine, nine, become twenty-seven, and the cycle continues[22]. This is how it often

---

[17] Lerner, D. (16 July 2024). *Coming from inside the building: Dark web recruitment of malicious insiders*. CSO Online. https://www.csoonline.com/article/653481/coming-from-inside-the-building-dark-web-recruitment-of-malicious-insiders.html

[18] Webz.io. (3 April 2024). *Social engineering on the dark web: A hacker's toolkit*. https://webz.io/dwp/social-engineering-on-the-dark-web-a-hackers-toolkit/

[19] Juncker, R. (15 July 2025). *How criminal networks exploit insider vulnerabilities*. Dark Reading. https://www.darkreading.com/vulnerabilities-threats/criminal-networks-exploit-insider-vulnerabilities

[20] Federal Trade Commission. (n.d.). *Multi-level marketing businesses and pyramid schemes*. FTC Consumer Advice. https://consumer.ftc.gov/multi-level-marketing-businesses-pyramid-schemes

[21] QNET. (n.d.). *QNET official website*. https://www.qnet.net/

[22] SowetanLIVE. (30 August 2018). *How to tell a pyramid scheme from a real investment*. SowetanLIVE. https://www.sowetan.co.za/business/money/2018-08-30-how-to-tell-a-pyramid--scheme-from-a-real-investment/

works within the dark web, where those who enter under pressure are drawn into self-perpetuating systems that expand endless, the process relies on psychological conditioning and economic fear, convincing individuals that compliance is the only way to recover loss or avoid exposure. In this way, the dark-web ecosystem grows not merely through technology or spyware but through human recruitment mechanisms that have transformed ordinary users into an untraceable, decentralized network of intelligence assets.

14- AI-Driven Challenge Escalation: Artificial intelligence and automated tooling amplify dark-web recruitment and operational pipelines by personalizing and accelerating challenge-based tactics. Machine learning models enable hostile actors to generate highly convincing deepfakes, tailor social-engineering scripts to an individual's behavioral profile and automate the distribution of mission prompts that progressively demand riskier acts. At the same time, AI lowers the cost and latency of reconnaissance aggregating open-source traces, scraping social feeds, and correlating location or schedule data to produce precise tasking for low-level operatives, while generative tools can synthesize bogus evidence to coerce or discredit targets. Coupled with clandestine surveillance (malware, implanted recorders, compromised IoT), these capabilities convert static data into dynamic, adaptive campaigns that escalate pressure in real time and increase the speed at which a target's exposure can be weaponized[23].

15- On Dark-Web networks, frequently circulate missions and challenges targeting individuals perceived as influential, successful, or obstructive to illicit agendas[24], including diplomatic figures, parliamentary members, government officials, civil servants, journalists, human-rights defenders, and embassy staff[25]. These operations are structured to damage reputations, disrupt personal or professional stability, and apply psychological pressure through coordinated digital harassment or real-world proximity tracking[26]. Such targeting

[23] Center for Global Studies (CGS) & Parliamentary Assembly of the Mediterranean (PAM). (18 November 2024). *The Malicious Use of AI and Emerging Technologies by Terrorist and Criminal Groups: Impact on Security, Legislation, and Governance*. CGS–PAM. https://www.cgspam.org/wp-content/uploads/2024/11/PAM-CGS-Report-on-AI-and-Emerging-Technologies-1.pdf

[24] Oram, N. (16 July 2024). *Executives in the crosshairs: How the dark web is fueling targeted threats*. Cybersecurity Insiders. https://www.cybersecurity-insiders.com/executives-in-the-crosshairs-how-the-dark-web-is-fueling-targeted-threats/

[25] Amnesty International. (09 October 2023). *Global: 'Predator Files' spyware scandal reveals brazen targeting of civil society, politicians and officials*. https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/

[26] SOCRadar. (28 November 2024). *The dark web and cybercrime: How hidden networks operate*. https://socradar.io/the-dark-web-and-cybercrime-hidden-networks-operate/

reflects the network's internal drive to demonstrate power, enforce obedience among members, and reward those who engage in increasingly intrusive or harmful activities[27].

16- Personal data exploitation and real-world surveillance occur when dark web actors repurpose stolen or publicly scraped information to conduct prolonged monitoring of targeted individuals, using leaked financial details, contact numbers, photographs, home surroundings, and daily-movement patterns to create operational missions that enable physical tracking, harassment, intimidation, or infiltration of a victim's social and professional circles; this practice transforms ordinary digital traces into actionable intelligence, allowing hostile actors to observe behavior, identify vulnerabilities, and exert psychological pressure through persistent proximity or repeated digital intrusion[28].

17- Hotels, restaurants, and other accommodation or hospitality venues frequented by diplomats, government officials, parliamentarians, journalists, business leaders, and tourists constitute high-value environments where spyware and covert surveillance devices can be discreetly deployed. Hidden cameras, audio bugs, compromised Wi-Fi access points, and other embedded monitoring tools, technologies frequently discussed in technical spyware analyses, enable the silent collection of personal conversations, private behavior, and sensitive communications, often without leaving visible traces[29]. Once obtained, these recordings can be circulated within dark-web markets or transferred to foreign intelligence intermediaries who weaponize the material for blackmail[30], coercion, reputational pressure, or targeted operational planning[31]. Such practices create a dual-layer threat: they expose diplomats and officials to strategic interception risks while simultaneously placing ordinary visitors at risk of extortion or intimidation campaigns designed to enforce compliance or silence. Restaurants and public venues frequented by political figures, diplomats, parliamentarians, journalists, and other high-profile individuals are also targets for ambient audio capture or proximity-based spyware delivery, enabling the extraction of context-rich intelligence that may later be traded, sold, or exploited on hidden platforms. This intersection between physical-space surveillance and dark-web

---

[27] Shukla, A., & Ahmed, M. B. (02 October 2024). *The role of the dark web in cybercrime: Threats, challenges, and mitigation strategies*. *World Journal of Engineering Research and Technology, 10*(10), 148–154. https://www.wjert.org/admin/assets/article_issue/82092024/1728040774.pdf

[28] Brandefense. (16 October 2024). *Dark Web Diaries: What happens to your data after it's stolen?* https://brandefense.io/blog/dark-web/dark-web-diaries-what-happens-to-your-data/

[29] This source has been previously cited; see Reference No. 1 for full citation details.

[30] Tech Business Fit. (18 September 2024). *Dark web espionage*. Tech Business Fit. https://techbusinessfit.com/dark-web-espionage/

[31] Diverse Daily. (n.d.). *Reconnaissance of political blackmail networks: Mapping the collection and use of kompromat as a tool of intelligence warfare*. Diverse Daily. https://diversedaily.com/reconnaissance-of-political-blackmail-networks-mapping-the-collection-and-use-of-kompromat-as-a-tool-of-intelligence-warfare/

exploitation demonstrates how hospitality environments can serve as covert collection points feeding broader digital-espionage ecosystems.

18- Mental health vulnerabilities are frequently exploited within dark web environments, where actors intentionally target individuals experiencing emotional instability, anxiety, loneliness, or unresolved psychological distress; such individuals are more susceptible to manipulation, coercive messaging, and staged scenarios designed to provoke dependence, obedience, or heightened engagement. By leveraging these emotional weaknesses, hostile networks introduce escalating tasks, reinforce loyalty through psychological pressure, and encourage behavior that individuals would not otherwise consider, ultimately transforming mental-health fragility into an entry point for deeper recruitment, operational involvement, or behavioral control[32].

19- Youth recruitment and radicalization occur when dark web actors identify and target adolescents and/or young adults who display emotional distress, digital overexposure, or a desire for recognition, gradually grooming them through personalized messaging, attention-driven interactions, and staged scenarios designed to create dependency and a sense of belonging. These individuals are then introduced to progressively more manipulative tasks, framed as challenges or opportunities to gain status within the online collective, ultimately exposing them to extremist narratives, coercive demands, and intelligence-like operations that exploit their developmental vulnerabilities and limited awareness of long-term risks[33].

20- Escalation and retention mechanisms, within dark web ecosystems, rely on structured behavioral conditioning, where individuals are gradually introduced to increasingly intrusive tasks framed as challenges, missions, or loyalty tests that reinforce dependency and commitment to the networks[34]. These escalating assignments often involve ethically questionable or unlawful actions, creating shared digital culpability and psychological pressure that makes withdrawal difficult or dangerous. As members progress, the network rewards obedience through elevated status, exclusive access, or perceived empowerment, while punishing hesitation or resistance through humiliation, exposure, intimidation, or

[32] Peremore, K. (02 August 2024). *Mental health data and the dark web*. Paubox. https://www.paubox.com/blog/mental-health-data-and-the-dark-web

[33] Europol. (12 November 2024). *The recruitment of young perpetrators for criminal networks* [Intelligence notification]. Europol. https://www.europol.europa.eu/publications-events/publications/recruitment-of-young-perpetrators-for-criminal-networks

[34] The Dark Psychology Team. (30 September 2025). *Loyalty tests: Proving allegiance on command*. The Dark Psychology. https://thedarkpsychology.com/dark-psychology-tactics/loyalty-tests-manipulation/

targeted harassment, ultimately transforming participation into a cycle of coercion, psychological confinement, and operational exploitation[35].

21- Internal exposure and mutual coercion frequently emerge within dark-web ecosystems when multiple participants become involved in surveillance, harassment, information-gathering, or challenge-based activities directed at the same individual. As actors operate in parallel, they may gradually identify signs of one another's presence, methods, or operational patterns. This often generates suspicion, rivalry, and attempts to uncover the identities of other participants. In such environments, individuals may resort to intimidation, blackmail, or threats of exposure against one another in order to gain influence, avoid personal liability, or secure compliance with their preferred course of action. These dynamics create additional layers of psychological pressure that extend beyond the original mission itself. Over time, participants become trapped not only by fear of the network but also by fear of other members who possess compromising information regarding their involvement. The resulting climate of mistrust, anxiety, and mutual coercion can spill into personal, professional, and social relationships, generating conflicts whose underlying causes remain difficult for families, communities, and authorities to identify.

22- In many cases, these dynamics are intensified by fabricated compliance and false reporting. Participants may claim to have completed assigned tasks, established contact with targeted individuals, or achieved specific operational objectives when, in reality, no such outcome has occurred. Such misrepresentations are often intended to avoid pressure, maintain status within the group, or satisfy escalating demands imposed by other actors. Over time, however, these false claims create additional vulnerabilities, as inconsistencies become visible to other participants who may exploit them for leverage, intimidation, or coercion. The individual then becomes trapped between the fear of external retaliation and the fear of exposure from within the network itself. This cycle of deception, dependency, and mutual pressure frequently leads to escalating demands, increased psychological distress, and a progressive loss of personal autonomy, further reinforcing the individual's inability to disengage from the broader ecosystem. While these dynamics initially affect those directly involved, their consequences often extend far beyond the immediate participants.

[35] Gray, A. (01 October 2024). *The thrill-seekers of the digital underworld: A review of research into the psychological motivations of dark web users and cybercriminals*. Asia Pacific Institute of Information Technology. https://www.researchgate.net/publication/382742239_The_Thrill-Seekers_of_the_Digital_Underworld_A_Review_of_Research_into_the_Psychological_Motivations_of_Dark_Web_Users_and_Cybercriminals

They may generate wider social consequences by fostering mistrust, interpersonal conflicts, family tensions, workplace disputes, and community fragmentation whose underlying causes often remain concealed. When replicated across larger social environments, such mechanisms can gradually undermine social cohesion, weaken confidence in institutions, and contribute to latent patterns of instability that remain difficult for authorities to detect, attribute, and effectively address. Over time, these hidden pressures may evolve into broader societal vulnerabilities capable of affecting community resilience, public trust, and the overall effectiveness of governance structures.

23- These patterns of coercion, deception, dependency, and mutual intimidation are closely aligned with established principles of dark psychology. The manipulation strategies employed are rooted in principles of dark psychology, including gaslighting, emotional blackmail, and deception. These methods are used to destabilize the target's sense of reality and autonomy, making them more susceptible to control[36]. The anonymity of the dark web further amplifies these effects, allowing manipulators to operate without accountability while fostering an environment of secrecy and fear[37].

24- Daily-life harm extends far beyond high-profile individuals, affecting ordinary people and families through sustained online harassment, coercion, stalking, sextortion, reputational sabotage, and coordinated smear campaigns that spill into workplaces, schools, and local communities. Compromised accounts are used for impersonation; financial pressure emerges through credential theft, SIM-swap manipulation, and unauthorized access to banking services; and coercive control is enforced through threats to release private images, audio recordings, or location data harvested from compromised devices or covert surveillance. These pressures generate tangible consequences, job loss, marital disputes, family breakdown, community isolation, and long-term psychological trauma, while cross-border, anonymized nature of dark-web ecosystems prevents victims from identifying perpetrators or seeking timely protection. By converting ordinary digital traces into repeatable "missions," hostile actors sustain cycle of intimidation designed to destabilize victims' personal lives, economic security, and social relationships.

25- Women are increasingly exposed to technology-facilitated coercive control through the misuse of commercial spyware, hidden tracking applications, compromised shared

[36] Waqar. (26 July 2023). *25 psychological manipulation techniques*. PsychologyOrg. https://psychologyorg.com/25-psychological-manipulation-techniques/

[37] Grant, A. (22 May 2025). *Behind the screen: How psychological manipulation fuels cybercrime*. PsyForU. https://psyforu.com/behind-the-screen-how-psychological-manipulation-fuels-cybercrime/

accounts, and covert device-monitoring tools that enable intimate partners, stalkers, or hostile actors to maintain persistent surveillance without consent[38]. International assessments warn that these technologies are frequently used to monitor communications, track real-time movements, access photographs and private messages, observe social interactions, and enforce psychological domination through continuous digital intrusion[39]. In many cases, abusive actors exploit spyware-enabled access to isolate victims socially, manipulate behavior, intimidate them through implicit knowledge of their activities, and create an environment of constant fear, dependency, and self-censorship. AI-driven harassment mechanisms further intensify these dynamics through automated abuse campaigns, synthetic media manipulation, coordinated intimidation, and targeted reputational attacks, particularly against women journalists, public figures, human-rights defenders, and socially visible individuals. The normalization of surveillance-oriented behavior within personal relationships, including location tracking, passcode access, and covert account monitoring, increasingly blurs the distinction between digital monitoring and psychological abuse, transforming everyday technologies into instruments of coercive control capable of undermining personal autonomy, mental well-being, freedom of expression, and human security.

26- Social harm resulting from dark-web exploitation frequently begins inside the household, where victims experience strain, secrecy, and conflict created by coercion, impersonation, or the misuse of private material. Ordinary users who enter dark-web channels, whether through manipulation, curiosity, or pressure from someone they trust, often become trapped in cycle of fear and isolation that erode family stability and undermine natural support systems. This breakdown creates an ideal environment for hostile actors to convert individuals into lo-level operatives, gradually expanding their pool of coerced participants and making it increasingly easy to reach targeted person through people positioned close to them. In this way, domestic vulnerability becomes a direct pipeline into larger intelligence-like networks that rely on dispersed, reluctant, and easily controlled human assets.

27- Corruption and institutional failures significantly enable the expansion of dark web activities, as actors operating within weakened governance environments exploit

[38] Australian Strategic Policy Institute (ASPI). (18 May 2026). Digitally watched without consent: Spyware as a tool of coercive control. The Strategist. https://www.aspistrategist.org.au/digitally-watched-without-consent-spyware-as-a-tool-of-coercive-control/

[39] Dig.watch. (19 May 2026). UNESCO report warns AI-driven abuse threatens women journalists globally. Dig.watch. https://dig.watch/updates/unesco-report-warns-ai-driven-abuse-threatens-women-journalists-globally

compromised officials, inconsistent enforcement, and gaps in regulatory oversight to sustain illicit operations. When individuals within governmental, security, or administrative structures are willing to sell access, overlook violations, or facilitate the movement of prohibited goods or sensitive data, dark web networks gain critical advantages that strengthen their operational resilience[40]. These systemic weaknesses allow hostile entities to bypass detection, manipulate legal processes, secure protection through bribery or intimidation, and maintain cross-border logistical support, ultimately transforming institutional vulnerabilities into core enablers of digital criminality and covert intelligence-like behavior[41].

28- Structural instability created by dark web systems emerges when illicit digital ecosystems undermine social cohesion, weaken institutional trust, and disrupt the operational integrity of national security frameworks[42]. These networks leverage anonymity, decentralized communication tools, and covert financial infrastructures to spread disinformation, intensify social divisions, and erode public confidence in governmental institutions. As operations escalate across borders, they contribute to long-term instability by normalizing illicit behavior, incentivizing cyber-enabled crime, and overwhelming law-enforcement and regulatory capacities, ultimately transforming the digital underground into a persistent source of systemic vulnerability[43].

29- Economic disruption: Dark-web and spyware ecosystems generate far-reaching economic harms that extend beyond individual extortion to systemic disruption of commercial activity and public-sector stability. Compromised corporate devices, leaked executive communications, and threats of reputational exposure are routinely used to extract ransom, manipulate market behavior, or pressure organizations into compliance with illicit demands. Supply-chain infiltration along with the illicit trade of counterfeit goods, chemical precursors, and unregulated medical or cosmetic products, undermines consumer safety, regulatory trust, and national quality-control frameworks. Coordinated disinformation campaigns and fabricated evidence circulating through hidden networks can suppress tourism, destabilize investment climates, and fracture sectoral confidence. When

---

[40] Kumar, V. (09 September 2025). *Unmasking the invisible web: A comprehensive legal study on darknet operations, cybercrime networks, and the challenges of law enforcement in the digital underground*. *International Journal of Multidisciplinary Trends*, 7(10), 99–106. https://www.multisubjectjournal.com/article/812/7-10-32-726.pdf

[41] Stravinsky, A. (11 September 2025). *The dark web supply chain of fraud: How data breaches create global security risks*. Newstrail. https://www.newstrail.com/the-dark-web-supply-chain-of-fraud-how-data-breaches-create-global-security-risks/

[42] Breachsense Team. (06 November 2025). *Top dark web sites every security team needs to monitor*. Breachsense. https://www.breachsense.com/blog/dark-web-sites/

[43] McCarthy-Jones, A., & Turner, M. (06 February 2024). *Dark networks, transnational crime and security: The critical role of brokers*. *Journal of Illicit Economies and Development*, 5(1), 58–69. https://jied.lse.ac.uk/articles/10.31389/jied.226

combined with cross-border laundering channels and covert financial markets, these tactics allow hostile actors to weaponize economic pressure, forcing concessions, weakening institutions, or financing further illicit networks. The anonymity and decentralized architecture of dark-web ecosystems limits accountability, enabling sustained economic disruption that cascades across national and international systems[44].

30- Eliminating dark web influence in theory would require a coordinated transformation of global digital infrastructure, combining enhanced encryption oversight, unified cross-border monitoring protocols, and strengthened international governance mechanisms capable of identifying and disrupting covert digital ecosystems without compromising fundamental rights. Such an approach would necessitate advanced authentication systems, transparent communication standards, and resilient cybersecurity frameworks that prevent the formation of hidden networks while ensuring secure, rights-respecting online environments for the public. Although largely theoretical under current technological and political constraints, this concept highlights the scale of structural reforms required to neutralize the operational space that enables criminal and intelligence-linked activities within the dark web[45].

31- Expanding public awareness and protection mechanisms is critical to reducing vulnerability to dark web exploitation, as individuals often become targets due to limited digital literacy and reliance on unsecured platforms. Effective prevention strategies include accessible awareness campaigns, community-based training programs, and reliable reporting channels that enable users to recognize manipulation attempts and suspicious online behavior. International bodies, such as ENISA[46], emphasize that improving digital literacy and cyber hygiene significantly reduces exposure to online threats, while UNODC[47] and INTERPOL[48] advocate for public education and reporting systems to disrupt recruitment pipelines exploited by hostile actors. Strengthening societal resilience through these measures not only mitigates psychological and financial coercion but also reinforces collective security against cyber-enabled crime.

---

[44] United Nations Office on Drugs and Crime (UNODC). (2023). *Report on cyber-enabled economic crime and operational disruption.* https://www.unodc.org/unodc/en/cybercrime/index_new.html

[45] Warner, C. (12 September 2023). *Law enforcement and digital policing of the dark web: An assessment of the technical, ethical and legal issues*. In *Applications for Artificial Intelligence and Digital Forensics in National Security* (pp. 105–115). Springer. https://link.springer.com/chapter/10.1007/978-3-031-40118-3_7

[46] European Union Agency for Cybersecurity (ENISA) – Threat Landscape 2023, 07 November 2025. CyberEducation Platform. ENISA. https://www.enisa.europa.eu/topics/education-and-career-path/cybereducation-platform

[47] United Nations Office on Drugs and Crime (UNODC) – Cybercrime, 07 November 2025. UNODC. https://www.unodc.org/unodc/en/cybercrime/index_new.html

[48] INTERPOL – National Cybercrime Strategy Guidebook, 01 April 2021. INTERPOL. https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf

32- Enhancing the role of technology companies in device recovery and security support is essential to reducing user exposure to dark-web-linked exploitation, as these companies maintain the technical capacity to detect abnormal activity, identify potential compromises, and assist individuals in restoring device integrity. Dedicated customer-support channels, remote diagnostic tools, and built-in security frameworks enable providers to determine whether a device has been infiltrated, manipulated, or subjected to unauthorized monitoring. International organizations, such as ENISA[49] and the U.S. Federal Trade Commission[50], highlight the timely collaboration between users and service providers significantly reduces the risk of prolonged compromise by improving threat detection and response[51]. Strengthening these support mechanisms and encouraging users to seek verification from trusted manufacturers can prevent hostile actors from sustaining access, thereby reducing the long-term harm associated with digital coercion and spyware-enabled intrusion[52].

33- Cyber-mercenary networks operating across hidden services provide customized intrusion capabilities to a wide range of clients, offering offensive cyber operations that were once limited to state intelligence units. These actors supply tailored services, such as mobile-spyware deployment, targeted phishing and SIM-swap operations, hardware-implantation support, anonymized logistics, and post-compromise persistence, all coordinated through covert marketplaces, encrypted communication channels, and proxy financial, and politically motivated clients to procure professional tradecraft, outsource sensitive digital operations, and scale their activities with a high degree of deniability. This outsourcing model complicates attribution, erodes deterrence, and allows both state-linked and non-state actors to project influence through hired technical intermediaries while insulating themselves from direct exposure, an operational dynamic thoroughly documented in international analyses of proxy cyber-operators and capability-for-hire ecosystems[53].

---

[49] European Union Agency for Cybersecurity (ENISA). (26 June 2025). *Supporting NIS2 implementation through actionable guidance*. ENISA. https://www.enisa.europa.eu/news/supporting-nis2-implementation-through-actionable-guidance

[50] Federal Trade Commission (FTC). (07 November 2025). *Protecting personal information: A guide for business*. FTC. https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

[51] Cybersecurity and Infrastructure Security Agency (CISA). (01 September 2020). *Technical approaches to uncovering and remediating malicious activity* [Joint cybersecurity advisory]. CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a

[52] Blue Cedar Team. (07 November 2025). *Ensure device integrity*. Blue Cedar. https://www.bluecedar.com/ensure-device-integrity-blue-cedar

[53] Saiz Erausquin, G. (28 October 2025). *RUSI Cyber Sanctions Taskforce: Countering state-backed cyber threats*. Royal United Services Institute (RUSI). https://www.rusi.org/explore-our-research/publications/insights-papers/rusi-cyber-sanctions-taskforce-countering-state-backed-cyber-threats

34- The actors operating behind dark-web intelligence and recruitment systems constitute a deep entrenched architecture that fuses translational criminal groups, proxy networks, clandestine intermediaries, and strategically motivated operators whose activities mirror patterns observed in high-risk conflict environments[54]. Growing evidence from international threat assessments confirms that many of the same networks, facilitators, and proxy actors involved in enabling or supporting violent extremist activity in the physical world are simultaneous funds, and direct influence campaigns with near-total deniability[55]. These actors exploit the hidden web to outsources sensitive tasks, test operational methods, and maintain communication channels designed to circumvent oversight, reflecting long-term corruption patterns documented across political, administrative, and security structures[56].

35- Their operational reach is often strengthened by a broad network of corrupt enablers across both the public and private sectors, including compromised state officials and law-enforcement personnel who provide illicit protection, document manipulation, or access to restricted environments, enabling criminal and extremist actors to operate with reduced risk of detection[57]. Hospitals, laboratories, and psychiatric institutions are, likewise, also vulnerable to infiltration by corrupt insiders capable of providing unauthorized access to sensitive medical information, controlled substances, or internal systems behaviors extensive recorded in global health-sector corruption analyses[58]. Parallel risks emerge within illicit supply chains involving corrupt manufacturers and distributors of chemicals, cosmetics, medical products, pesticides, agricultural materials, and perishable goods, whose actions facilitate the covert movement of hazardous substances, counterfeit goods, and precursor chemicals, reinforcing vulnerabilities identified in international anti-corruption and chemical-control frameworks[59]. These fragmented supply chains often converge into a single illicit ecosystem in which drug traffickers, weapons dealers, and

[54] INTERPOL. (19 October 2023). *Global Crime Trend Report 2023*. INTERPOL. https://www.interpol.int/en/How-we-work/Criminal-intelligence-analysis/Our-analysis-reports

[55] United Nations Office on Drugs and Crime (UNODC). (26 June 2023). *World Drug Report 2023*. UNODC. https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2023.html

[56] Organisation for Economic Co-operation and Development (OECD). (20 October 2022). *Foreign bribery report 2022*. OECD. https://www.oecd.org/en/publications/oecd-foreign-bribery-report_9789264226616-en.html

[57] Europol. (12 April 2021). *European Union serious and organised crime threat assessment (SOCTA) 2021: A corrupting influence*. Publications Office of the European Union. https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021

[58] United Nations Office on Drugs and Crime (UNODC). (01 December 2021). *Global report on corruption in the health sector*. UNODC. https://www.unodc.org/unodc/en/frontpage/2021/May/ungass-2021-against-corruption-highlights-importance-of-stolen-asset-recovery-and-addressing-corruption-in-the-health-sector.html

[59] Financial Action Task Force (FATF). (20 July 2023). *Illegal trade in chemical precursors: Assessing the risks and strengthening global responses*. FATF. https://www.fatf-gafi.org/en/publications/Methodsandtrends/illegal-trade-chemical-precursors.html

suppliers of chemical precursors operate through shared channels, using the same intermediaries, smuggling routes, and covert financial networks to move products, exchange services, and sustain cross-sector criminal operations without attracting regulatory scrutiny[60]. Corrupt customs personnel further enable the transit of restricted materials and illicit commodities through weakened border controls, directly contributing to the resilience of these hidden economies[61].

36- Within this cross-sector infiltration, criminal groups, weapons traffickers, drug cartels, and human-smuggling networks exploit the same covert digital infrastructures, as extremist and proxy actors, forming hybrid ecosystems in which logistics, intelligence, money flows, and operational capabilities circulate between factions that would otherwise remain distinct a pattern consistently highlighted across UNODC reporting[62]. Manipulation and recruitment mechanisms deployed by these actors become particularly potent in communities shaped by rigid traditional or religious norms, where heightened sensitivity to stigma and groups pressure significantly increases susceptibility to coercion and psychological conditioning[63]. This dynamic equally extends to individuals operating within modern professional or high-visibility environments, where reputational expectations, competitive pressures, and the need to project stability or credibility can create parallel vulnerabilities. In such contexts, even minor professional lapses or private missteps may be exploited as leverage for coercion or digital entrapment, allowing hostile actors to apply psychological pressure through threats of exposure or reputational disruption. This combined spectrum of traditional and contemporary social pressures demonstrates how divers environments can be weaponized to limit resistance, intensify dependency, and secure long-term control over targeted individuals.

37- In this broader operational landscape, violent extremist organizations constitute one particularly visible manifestation of the threat. Groups inspired by ISIS have demonstrated how dark-web platforms can be weaponized to disseminate indoctrination, rebuild fragmented networks, and assign staged missions designed to escalate psychological

[60] United Nations Office on Drugs and Crime. (2020). *Transnational organized crime threat assessment*. UNODC. https://www.unodc.org/unodc/data-and-analysis/TOC-threat-assessments.html
[61] World Customs Organization (WCO). (30 June 2022). *Annual report 2021–2022*. WCO. https://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/annual-reports/annual-report-2021_2022.pdf
[62] United Nations Office on Drugs and Crime (UNODC). (24 January 2023). *Global report on trafficking in persons 2022*. UNODC. https://www.unodc.org/unodc/en/press/releases/2023/January/global-report-on-trafficking-in-persons-2022.html
[63] United Nations Office on Drugs and Crime (UNODC). (26 June 2023). *World Drug Report 2023*. UNODC. https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2023.html

dependence and operational loyalty tactics consistent with previously documented radicalization cycles and intelligence-style recruitment methods[64].

38- Furthermore, groups that publicly claim to orchestrate political or institutional coups often initiate their destabilization campaigns through social-media ecosystems, where coordinated narrative manipulation serves as their primary operational tool. Research by the Oxford Internet Institute shows that organized networks routinely deploy manufactured narratives, synthetic engagement, and coordinated amplification to simulate widespread public support for disruptive campaigns[65]. Dark-web-linked electronic armies further escalate these operations by deploying bot networks, paid influencers, and covert online cells to fabricate the appearance of mass participation, creating an artificial sense of momentum that can accelerate disorder, undermine institutional cohesion, and provoke real-world unrest. These mechanisms mirror tactics documented by the RAND Corporation, which describes how hostile actors weaponize digital platforms to erode political stability, distort public perception, and engineer destabilizing social pressure[66].

39- At a strategic level, the dark-web ecosystem is shaped and sustained by higher-order networks that operate across ideological, criminal, and geopolitical boundaries. In-depth research has highlighted that while the visible actors include extremist groups, trafficking networks, and corrupt intermediaries, these structures often serve broader agendas driven by entities that benefit from disorder, weakened institutions, and the erosion of public trust[67]. Threat-mapping assessments further indicate that the same transnational facilitators and proxy networks involved in financing or enabling violent extremist activity, organized crime, and destabilization campaigns in the physical domain are also active within dark-web infrastructures, where anonymity allows them to coordinate operations without attribution[68]. These architect-level actors rarely appear directly in recruitment chains or operational exchanges; instead, they influence the strategic environment by providing resources, enabling cross-network cooperation, and ensuring the continuity of illicit markets whose outcomes align with their interests an operational pattern consistent with

---

[64] Ibidem

[65] Bradshaw, S., Bailey, H., & Howard, P. N. (01 February 2021). *Industrialized disinformation: 2020 global inventory of organized social media manipulation*. Oxford Internet Institute. https://www.oii.ox.ac.uk/news-events/reports/industrialized-disinformation-2020-global-inventory-of-organized-social-media-manipulation/

[66] Mazarr, M. J., Casey, A., Demus, A., Harold, S. W., Matthews, L. J., Beauchamp-Mustafaga, N., & Sladden, J. (04 September 2019). *Hostile social manipulation: Present realities and emerging trends*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2713.html

[67] This source has been previously cited; see Reference No. 38 for full citation details.

[68] This source has been previously cited; see Reference No. 46 for full citation details.

findings on proxy behavior and hybrid threat ecosystems[69]. This layered configuration makes the dark web not only a criminal or extremist arena, but a parallel operational space leveraged by actors seeking to shape political, social, or economic conditions in ways that advance their broader objectives while remaining insulated from accountability.

40- Research into psychological profiles of dark web users reveals that many are drawn in by curiosity, ideological motives, or perceived anonymity. However, once inside, the mechanisms of manipulations shift their motivations, often leading to deeper involvement in illicit activities[70]. The structure of these communities reinforces dependency through reputation system, peer validation, and escalating challenges that require increasingly risky behavior.

41- This cycle of psychological manipulation and coercion not only facilitates recruitment but also ensures retention. Individuals become entangled in a system where exit is perceived as dangerous or impossible, and where continued participation is seen as the only viable path to safety or status. Understanding these recruitment mechanisms is essential for developing effective countermeasures. It highlights the need for psychological resilience training, digital literacy, and targeted interventions that address the emotional and cognitive vulnerabilities exploited by dark web actors.

**Advanced Spyware and Surveillance Technologies**

42- The dark web has become a central hub for the development, distribution, and commercialization of advanced spyware and surveillance technologies. These tools are specifically engineered to evade detection by conventional cybersecurity systems, making them particularly dangerous to individuals, organizations, and governments.

43- Spyware available on the dark web includes keyloggers, remote access trojans (RATs), and sophisticated malware capable of real-time tracking, data exfiltration, and device control. These programs are often bundled with exploit kits that target known vulnerabilities in operating systems and applications, allowing attackers to infiltrate systems without user interaction[71].

---

[69] United Nations Security Council Counter-Terrorism Committee Executive Directorate. (1 April 2020). *Trends Alert: Terrorist exploitation of cyber domains*. United Nations. https://www.un.org/securitycouncil/ctc/content/trends-alert-%E2%80%93-april-2020

[70] Gray, A. (8 October 2025). *The thrill-seekers of the digital underworld: A review of research into the psychological motivations of dark web users and cybercriminals*. ResearchGate. https://www.researchgate.net/publication/382742239_The_Thrill-Seekers_of_the_Digital_Underworld_A_Review_of_Research_into_the_Psychological_Motivations_of_Dark_Web_Users_and_Cybercriminals

[71] Webz.io. (6 October 2024). *Top malware types on the dark web in 2024*. https://webz.io/dwp/top-malware-types-on-the-dark-web-2024/

44- The architecture of the dark web facilitates the anonymous exchange of these tools. Fora and marketplaces serve as platforms where malware developers advertise their products with detailed specifications, pricing models, and even customer support[72]. Some platforms offer Ransomware-as-a-Service (Raas), enabling users with minimal technical expertise to deploy powerful spyware and ransomware attacks[73].

45- AI-powered surveillance tools have also emerged, capable of analyzing vast amounts of data from encrypted networks, chat groups, and illicit marketplaces. These tools use machine learning to detect behavioral patterns, identify targets, and automate cyberattacks[74]. The integration of natural language processing (NLP) and predictive analytics further enhances the effectiveness of these spyware systems[75].

46- The anonymity and decentralization of the dark-web systems make it nearly impossible to trace the origin or distribution of these technologies. As a result, even the most advances antivirus and cybersecurity solution struggle to detect or neutralize them[76]. This creates a persistent and evolving threat landscape that requires continuous monitoring and adaptive defense strategies.

47- The proliferation of undetectable spyware tools on the dark web underscores the urgent need for international cooperation, strengthening public-private partnerships, enhanced threat intelligence, and investment in next generation cybersecurity technologies. Without coordinated action, the risks posed by these surveillance tools will continue to escalate, compromising privacy, security, and digital sovereignty.

**AI-Driven Surveillance via Mobile Devices and Photo Recognition**

48- Emerging technologies have enabled the development of AI-powered surveillance tools capable of scanning photo galleries and media content stored on mobile devices. These tools can identify individuals, analyze behavioral patterns, and determine real-time locations based on visual data. Shile such capabilities are often associated with state-level surveillance programs, there is growing concern that similar technologies are being distributed through covert channels, including the dark web.

---

[72] This source has been previously cited; see Reference No. 2 for full citation details.
[73] Paganini, P. (15 January 2018). *Malware in the dark web*. Infosec Institute. https://www.infosecinstitute.com/resources/malware-analysis/malware-dark-web/
[74] SOC CSIRT. (14 February 2025). *AI-powered dark web monitoring: The future of cyber threat detection*. SOC Investigation. https://www.socinvestigation.com/ai-powered-dark-web-monitoring-the-future-of-cyber-threat-detection/
[75] Web Asha Technologies. (7 March 2025). *How AI is being used to monitor the dark web: Enhancing cybersecurity and threat intelligence*. https://www.webasha.com/blog/how-ai-is-being-used-to-monitor-the-dark-web-enhancing-cybersecurity-and-threat-intelligence
[76] CISO Advisory. (30 July 2025). *10 best dark web monitoring tools in 2025*. Cybersecurity News. https://cybersecuritynews.com/dark-web-monitoring-tools/

49- According to cybersecurity research, mobiles spyware applications some marketed as parental control or employee monitoring tools can secretly access photos, track GPS location, and activate microphones and cameras without user consent[77]. These apps are often disguised as legitimate utilities and can be installed remotely or through social engineering tactics[78].

50- This aligns with documented practices in China's Sharp Eyes and Skynet surveillance programs. The Sharp Eyes initiative aims to achieve full coverage of public spaces using AI-enhanced facial recognition and citizen monitoring systems[79]. The Skynet project, with over 600 million surveillance cameras, integrates real-time tracking and facial recognition to monitor individual across China[80].

51- The convergence of AI, mobile technology, and dark web distribution channels presents a serious threat to privacy and civil liberties. These developments underscore the need for stronger data protection policies, public awareness, and international regulation of AI surveillance technologies.

**Irreversible Membership and Hierarchical Structure**

52- Participation in dark web communities is often characterized by a one-way entry process, where exit is either highly restricts or practical impossible. Once an individual becomes involved, the structure and culture of these networks create conditions that discourage or prevent withdrawal.

53- Dark web platform operates on a decentralized and encrypted infrastructure, primarily through anonymizing networks such as Tor and I2P. These systems obscure user identities and locations, making it difficult for external entities to monitor or intervene. Within this framework, communities develop their own internal hierarchies, often resembling organized criminal networks or paramilitary structures[81].

54- Advancement within these communities is typically contingent upon the completion of increasingly risky or illegal tasks, these may include data theft, cyberattacks, or real-world

---

[77] Vigderman, A., & Turner, G. (26 September 2025). *Tracking or stalking? The dark side of tracking apps*. Security.org. https://www.security.org/blog/tracking-or-stalking-the-dark-side-of-tracking-apps/

[78] Bitdefender. (26 June 2025). *How to spot cell phone spy software (and what to do)*. https://www.bitdefender.com/en-us/blog/hotforsecurity/how-to-spot-cell-phone-spy-software-and-what-to-do

[79] Peterson, D. (2 March 2021). *China's 'Sharp Eyes' program aims to surveil 100% of public space*. Center for Security and Emerging Technology. https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/

[80] Chen, S. (4 March 2024). *Skynet 2.0: China plans to bring largest surveillance camera network on Earth to the moon to protect lunar assets*. South China Morning Post. https://www.scmp.com/news/china/science/article/3254054/skynet-20-china-plans-bring-largest-surveillance-camera-network-earth-moon-protect-lunar-assets

[81] SOCRadar. (28 November 2024). *The dark web and cybercrime: How hidden networks operate*. https://socradar.io/the-dark-web-and-cybercrime-hidden-networks-operate/

actions against targeted individuals. The performance of such tasks serves as a form of loyalty verification and status elevation, reinforcing the member's commitment and dependence on the network[82].

55- The psychological and operational mechanisms employes ensure retention. Members are often bound by shared culpability, fear of exposure, and the threat of retaliation. The anonymity of the dark web further complicates exit, as individuals cannot easily sever ties or seek protection without risking identification or reprisal[83].

56- Moreover, the hierarchical nature of these communities fosters a competitive environment where reputation and influence are earned through compliance and contribution. This structure incentivizes continued participation and discourages dissent, creating a closed system that perpetuates itself through coercion and fear[84].

57- Understanding the irreversible nature of dark-web membership and its hierarchical dynamics is essential for developing effective countermeasures. It highlights the need for psychological support, legal protections, and targeted interventions for individuals seeking to disengage from these networks.

**Digital Sovereignty and Emergence of Hidden Government**

58- The dark web has evolved into more than a concealed marketplace for illicit goods and services; it now exhibits characteristics akin to digital governance. Within its encrypted and decentralized architecture, certain communities have developed internal structures, regulatory mechanisms, and operational hierarchies that resemble state-like entities. These formations pose a growing threat to national sovereignty and global stability.

59- The research "From Shadows to Governance: Understanding the Dark Web Parliament[85]," indicates that dark web fora and marketplaces often operate with self-regulatory systems, including reputation scores, dispute resolution protocols, and community moderation, mirroring the administrative functions of formal institutions. These systems foster trust and order within anonymous environments, enabling sustained operations and member retention.

---

[82] Tuhin, M. (7 April 2025). *What is the dark web? Understanding its risks, uses, and mysteries*. Science News Today. https://www.sciencenewstoday.org/what-is-the-dark-web-understanding-its-risks-uses-and-mysteries

[83] Stith, L. (22 October 2023). *Why can't the dark web be shut down?* Robots.net. https://www.robots.net/tech/why-cant-the-dark-web-be-shut-down/

[84] This source has been previously cited; see Reference No. 21 for full citation details.

[85] Slonopas, A., Rutherford, A., Averbeck, R., Beatty, A., & Cooper, H. (2024). From Shadows to Governance: Understanding the Darkweb Parliament. Security and Intelligence, 9(1), 87–109. https://gsis.scholasticahq.com/article/94591.pdf

60- In some cases, these digital entities extend their influence beyond cyberspace. Reports have documented the existence of organized groups within the dark web, that coordinate real-world actions, including cyberattacks, disinformation campaigns, and espionage[86]. The anonymity and lack of oversight inherent to the dark web allow these groups to function with impunity, effectively creating parallel power structures that challenge traditional governance.

61- The concept of digital sovereignty, where states seek control over their digital infrastructure and data has become increasingly relevant in response to these developments. Governments face mounting difficulties in asserting jurisdiction over activities conducted in encrypted networks, especially when those activities originate from decentralized or transnational actors[87]. The emergence of these hidden digital entities complicates effort to regulate cyberspace and protect national interests.

62- Furthermore, the dark web's infrastructure supports the formation of what some researchers describe as "Digital Parliaments" or "Hidden Governments," where decisions are made collectively by anonymous actors with shared objectives[88]. These entities often possess their own enforcement mechanisms, including retaliation and exclusion protocols, reinforcing their autonomy and resilience.

63- The rise of such structures within the dark web underscores the urgent need for international intergovernmental and interparliamentary cooperation, legal innovation, and technological advancement. Addressing the threat posed by these hidden digital governments requires a multifaceted approach that includes enhanced cyber intelligence, cross-border legal frameworks, and proactive digital diplomacy.

**Targeting of Individuals through Public Challenges**

64- The dark web has increasingly become a platform for orchestrating targeted actions against individuals by public challenges. These challenges are often on personal information, such as photographs, financial data, and social media profiles, that has been compromised through data breaches, phishing attacks, or malware infections[89]-[90].

---

[86] Cybernod. (21 April 2025). *The role of the dark web in cyber warfare and nation-state attacks*. https://blog.cybernod.com/2025/04/the-role-of-the-dark-web-in-cyber-warfare-and-nation-state-attacks/

[87] Hwang, J. Y. (25 April 2025). *Digital sovereignty in an era of cyber threats and global connectivity*. *International Journal of Multidisciplinary Research Updates*, *9*(2), 12–23. https://orionjournals.com/ijmru/sites/default/files/IJMRU-2025-0023.pdf

[88] This source has been previously cited; see Reference No. 25 for full citation details.

[89] Neumeier, S. (26 September 2025). *Data breach monitoring: How to protect your personal data from the dark web*. Paessler Blog. https://blog.paessler.com/data-breach-monitoring-how-to-protect-your-personal-data-from-the-dark-web

[90] Key, K. (1 April 2025). *Your info is on the dark web: Use these tips to protect yourself*. PCMag. https://www.pcmag.com/articles/your-info-is-on-the-dark-web-use-these-tips-to-protect-yourself

65- Once personal data is acquired, it is frequently bundled into comprehensive identity packages known as (fullz), which include names, addresses, banking credentials, and biometric data[91]. These packages are then used to create challenges or missions within dark web communities, incentivizing members to engage in real-world actions such as harassment, stalking, or theft[92]. In some cases, these actions escalate into prolonged surveillance, where individuals are persistently followed, photographed, or monitored. To maintain proximity to the target without raising suspicion, perpetrators may attempt to establish a relationship, such as posing as a friend or adopting another socially acceptable role, thereby gaining continued access under false pretenses.

66- A notable example of this practice is doxing, where sensitive personal information is publicly posted with malicious intent. Doxing efforts originating from the dark web can include addresses, phone numbers, and even medical records, and are often accompanied by calls to action encouraging others to act on the information. In some cases, these challenges escalate to coordinated attacks, including Swatting incidents, which involve false emergency reports designed to provoke armed law enforcement responses[93].

67- The anonymity and decentralized nature of the dark web make it difficult to trace the origin of these challenges or hold perpetrators accountable. Fora and marketplaces facilitate the exchange of stolen data and the organization of these activities, often offering rewards or recognition for successful execution[94].

68- This phenomenon represents a significant threat to personal safety and privacy. It underscores the need for enhanced cybersecurity measures, public awareness, and legal frameworks capable of addressing the misuse of personal data in anonymous digital environments.

**Exploitation of Social Media and Online Platforms**

69- Social media platforms and online entertainment channels have become strategic gateways for dark web recruitment and exposure. Popular applications, including children's games, short-form video platforms, and messaging services are increasingly exploited to lure individuals into encrypted networks where illicit activities are conducted.

---

[91] Sharma, A. (4 June 2025). *Dark web threats: How your data is compromised and monetized by cybercriminals*. Cyber Defense Magazine. https://www.cyberdefensemagazine.com/dark-web-threats-how-your-data-is-compromised-and-monetized-by-cybercriminals/

[92] Oram, N. (8 October 2025). *Executives in the crosshairs: How the dark web is fueling targeted threats*. Cybersecurity Insiders. https://www.cybersecurity-insiders.com/executives-in-the-crosshairs-how-the-dark-web-is-fueling-targeted-threats/

[93] Ibidem

[94] Newman, J. (29 September 2025). *The digital black market: How your data is bought, sold, and traded after a breach*. PCMag. https://www.pcmag.com/explainers/the-digital-black-market-how-your-data-is-bought-sold-and-traded-after

70- The dark side of Instagram reels research[95] indicates that platforms such as Instagram, TikTok, and Discord are frequently used to disseminate links disguised as free software, entertainment content, or exclusive access to paid services. These links often redirect users to hidden services accessible only through anonymizing tools like the Tor browser, effectively initiating their entry into dark web[96].

71- Children and teenagers are particularly vulnerable to these tactics. Studies show that online gaming environments and social media reels are used to initiate contact, build trust, and gradually expose young users to dark web content[97]. The anonymity and lack of regulation on these platforms make it difficult for guardians and authorities to monitor or intervene.

72- On many social media platforms, promotional content is circulated under the pretext of raising awareness about cybersecurity or surveillance risks[98]. Influencers and anonymous accounts frequently demonstrate the so-called "best or the most dangerous" spying or monitoring applications, programs capable of recording calls, tracking locations, or accessing photo galleries, while claiming that the purpose is educational. These videos normally end with invitations such as "DM for the link" or "contact for more information," which function as covert recruitment mechanisms leading viewers toward unregulated download channels or restricted networks.[99] In some instances, the same channels promote illicit marketplaces advertising stolen Visa or MasterCard data, often displaying sample card information and prices, reflecting well-documented practices in underground "carding" fora and data trading markets[100].

73- Once contact is established, individuals are often guided to obtain or install such surveillance tools through links associated with hidden or semi-hidden networks. Many engage out of curiosity or personal motives, such as monitoring a partner, without recognizing that these actions create a pathway into interconnected dark-web distribution systems. Technical analyses by cybersecurity institutions, including the University of California, demonstrate that many consumer spyware applications operate covertly,

---

[95] Knutsson, K. (6 December 2023). *The dark side of Instagram Reels: An investigation reveals risqué and disturbing recommendations*. Fox News. https://www.foxnews.com/tech/dark-side-instagram-reels-investigation-reveals-risque-disturbing-recommendations

[96] Key, K. (21 January 2025). *What is the dark web? Here's how to access it safely (and what you'll find)*. PCMag. https://www.pcmag.com/explainers/what-is-the-dark-web-heres-how-to-access-it-safely-and-what-youll-find

[97] The Children's Society. (10 December 2020). *What is the dark web?* https://www.childrenssociety.org.uk/information/professionals/resources/what-is-the-dark-web

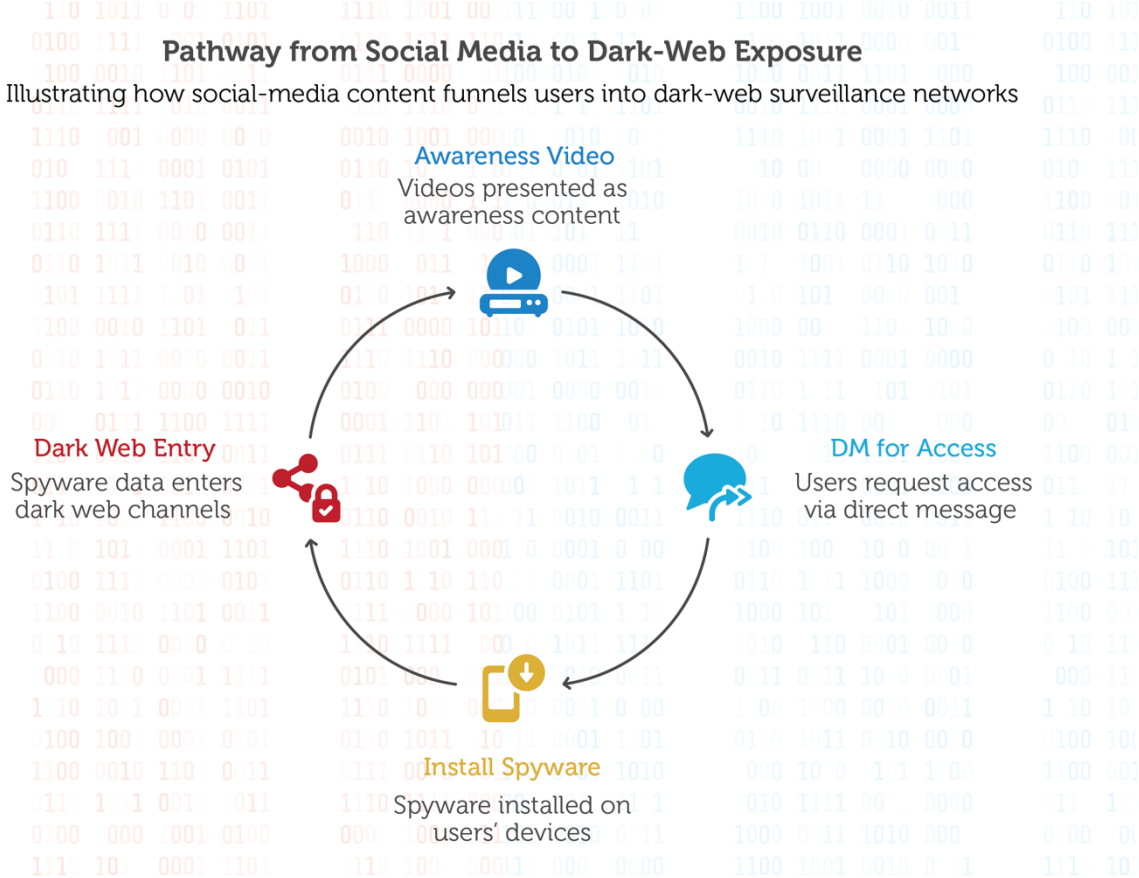
[98] DW Documentary. (9 October 2024). *The dark side of the internet | DW Documentary* [Video]. YouTube. https://www.youtube.com/watch?v=6OP0Oy33zog

[99] Boussiron, C., & Soh, J. (16 September 2024). *Concealed networks: Are dark web syndicates turning to social media for cybercrime?* Group-IB. https://www.group-ib.com/blog/concealed-networks/

[100] Whittaker, J. (1 November 2022). *The online behaviors of Islamic State terrorists in the United States*. *Criminology & Public Policy, 21*(4), 1051–1078. https://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12651

conceal their presence in device systems, and are promoted via social media rather than official app stores[101]. This deceptive content structure transforms awareness campaigns into entry points or illicit networks, reinforcing the need for stronger moderation policies, transparent app store standards, and coordinated international oversight of spyware dissemination.

**Figure 2: Pathway from Social-Media to Dark-Web Exposure[102]**




**Mental Health Vulnerabilities among Participants**

74- Individuals engaged in dark web communities often exhibit signs of psychological instability and unresolved personal issues, which are systematically exploited to maintain control and compliance. The psychological profile of many dark web users includes elevated levels of anxiety, paranoia, emotional instability, and social isolation[103]. These

[101] Patrigenaru, I. (23 March 2023). *This is what happens when your phone is spying on you*. University of California. https://www.universityofcalifornia.edu/news/what-happens-when-your-phone-spying-you

[102] Graphic compiled by the CGS research team, based on the analysis presented in this report.

[103] Deshmukh, A. (16 February 2023). *Are we ready to battle with mental health issues linked with the Darknet?* Times of India. https://timesofindia.indiatimes.com/blogs/darksides/are-we-ready-to-battle-with-mental-health-issues-linked-with-the-darknet/

vulnerabilities are not only byproducts of prolonged exposure to disturbing content but also serve as entry points for manipulation and coercion.

75- Studies have identified a correlation between dark web usage and mental health disorders, including depression, insomnia, and obsessive-compulsive behaviors[104]. The anonymity and lack of accountability within these networks foster environments where individuals with preexisting psychological conditions are down into cycle of dependency and exploitation. The dark web's structure reinforces these conditions through constant exposure to illicit material, peer pressure, and the threat of retaliation for non-compliance[105].

76- Manipulative tactics rooted in dark psychology, such as emotional blackmail, gaslighting, and fear-based conditioning are frequently employed to exploit emotional vulnerabilities[106]. These methods are designed to destabilize the individual's sense of reality and autonomy, making them more susceptible to control. Once compromised, individuals are often coerced into participating in illegal activities or sharing sensitive information, further entrenching their involvement[107].

77- The exploitation of mental health vulnerabilities within the dark web is compounded by the circulation of stolen mental health records. These records, traded anonymously, contain deeply personal information that can be used to blackmail or manipulate individuals[108]. The stigma associated with mental health issues increases the likelihood of compliance, as individuals fear exposure and social repercussions.

78- Youth as intelligence assets: Young people are uniquely vulnerable to recruitment, manipulation, and instrumentalization within dark-web ecosystems, both as direct targets and as unwitting contributors to intelligence-style operations. Recruiters exploit adolescent social needs and digital fluency, offering gamified challenges, peer validation, micro-payment, or promises of status to co-opt minors into information-gathering, location-reporting, or harassment task. In many cases these youths perform reconnaissance, install or test malware on behalf of others, or serve as proximity vectors whose daily movements

---

[104] Sirola, A., Savolainen, I., & Oksanen, A. (1 January 2024). *Who uses the dark web? Cross-national and longitudinal evidence on psychosocial, behavioral, and individual predictors*. *Personality and Individual Differences, 227*, 1–12. https://psycnet.apa.org/record/2024-89976-001

[105] CM Guest Columnist. (17 January 2024). *The psychology of dark web users: Exploring motivations and behaviors*. Cyprus Mail. https://cyprus-mail.com/2024/01/17/the-psychology-of-dark-web-users-exploring-motivations-and-behaviours/

[106] an5s. (11 December 2024). *How manipulators exploit emotional vulnerabilities*. JokerSan. https://jokersan.com/how-manipulators-exploit-emotional-vulnerabilities/

[107] waqar. (26 July 2023). *25 psychological manipulation techniques*. PsychologyOrg. https://psychologyorg.com/25-psychological-manipulation-techniques/

[108] Peremore, K. (2 August 2024). *Mental health data and the dark web*. Paubox. https://www.paubox.com/blog/mental-health-data-and-the-dark-web

and social connections provide granular operational value. Coercion, blackmail, or staged exposure can rapidly convert a curious teenager into a controlled asset, while the legal and ethical complexities surrounding juvenile involvement hinder investigation and remediation. Addressing this trend requires targeted prevention, digital-literacy efforts, and child-safeguarding measures integrated into national cyber-awareness frameworks[109].

79- Economic fragility and labor-market precarity in lower-income countries create a distinct recruitment reservoir for dark-web networks. Individuals facing unemployment, limited social mobility, or dependence on remittances are particularly susceptible to offers of micro-work, quick payments, or remote tasks, opportunities that mask intelligence-relevant assignments such as location reporting, device testing, or logistical support. In some cases, entire local labor pools function as informal service providers to hidden markets, supplying low-risk operational labor that can be scaled rapidly and at low cost. This dynamic not only widens the pool of easily coerced or incentivized participants but also creates geographically distributed human infrastructure that hostile actors can call on for proximity access, local facilitation, or plausible- deniability tasks across multiple jurisdictions[110].

80- This dynamic presents a significant challenge for mental health professionals, law enforcement, and policymakers. Addressing the psychological dimensions of dark web participation requires trauma-informed interventions, digital literacy education, and robust support systems for individuals seeking to disengage from these environments[111].

**Global Threat and Lack of Effective Countermeasures**

81- The dark web represents a persistent and escalating global threat, affecting both direct users and individuals who have never interacted with its platforms. Its encrypted infrastructure and anonymity protocols enable a wide range of illicit activities, including cybercrime, identity theft, financial fraud, and the distribution of malware[112]. These activities transcend borders, making the dark web a transnational challenge that undermines digital security and public safety worldwide.

---

[109] Royal Canadian Mounted Police. (16 December 2024). *Five-Eyes insights – Young people and violent extremism: A call for collective action*. RCMP. https://rcmp.ca/en/corporate-information/publications-and-manuals/five-eyes-insights-young-people-and-violent-extremism-call-collective-action

[110] United Nations Office on Drugs and Crime. (7 February 2023). *Crisis and organized crime: Building resilient responses*. UNODC. https://www.unodc.org/unodc/en/frontpage/2023/February/crisis-and-organized-crime_-building-resilient-responses.html

[111] Pelz, B. (7 May 2025). *Trauma and dark psychology: Therapeutic approaches to manipulation, control, and power abuse*. *Journal of Psychology and Neuroscience, 7*(2), 1–15. https://unisciencepub.com/wp-content/uploads/2025/05/Trauma-and-Dark-Psychology-Therapeutic-Approaches-to-Manipulation-Control-and-Power-Abuse.pdf

[112] Agarwal, S. (3 March 2025). *The dark web dilemma: Can laws keep up with evolving cyber threats?* The Legal Quorum. https://thelegalquorum.com/the-dark-web-dilemma-can-laws-keep-up-with-evolving-cyber-threats/

82- Despite growing awareness, existing cybersecurity and law enforcement mechanisms remain insufficient to dismantle the dark web's infrastructure. The decentralized nature of dark web networks, combined with the use of anonymizing technologies such as Tor and cryptocurrencies like Monero, complicates efforts to trace transactions and identify perpetrators.[113] Law enforcement agencies face significant obstacles, including jurisdictional limitations, lack of technical expertise, and the rapid evolution of cybercriminal tactics[114].

83- Efforts to combat dark web threats have included international operations such as the takedown of marketplaces like Silk Road, AlphaBay, and Hanse. However, these successes are often short-lived, as new platforms quickly emerge to replace those dismantled[115]. The resilience of dark web infrastructure is further reinforced by its adaptive architecture, which is designed to withstand targeted attacks and surveillance efforts[116].

84- Moreover, the dark web's impact extends beyond its immediate users. Data breaches affecting corporations, governments, and individuals frequently result in stolen information being sold on dark web marketplaces. This includes login credentials, financial records, and personal identifiers, which can be used to launch further attacks or exploit victims[117]. As such, even those who have never accessed the dark web may find their data circulating within its hidden fora.

85- The lack of effective countermeasures is compounded by slow legal adaptation and limited international cooperation. Existing laws often fail to address the complexities of dark web operations, and enforcement agencies struggle to keep pace with technological advancements[118]. Experts emphasize the need for dynamic legal reform, cross-border collaboration, and investment in advanced cybersecurity technologies to mitigate risks posed by the dark web[119].

---

[113] Shukla, A., & Ahmed, M. B. (2 October 2024). *The role of the dark web in cybercrime: Threats, challenges, and mitigation strategies*. *World Journal of Engineering Research and Technology, 10*(10), 148–154. https://www.wjert.org/admin/assets/article_issue/82092024/1728040774.pdf

[114] StealthMole. (3 August 2023). *Dark web investigations: Law enforcement's battle against dark web criminals*. StealthMole. https://www.stealthmole.com/blog/dark-web-investigations-law-enforcements-battle-against-dark-web-criminals

[115] Cybernod. (28 April 2025). *Is the dark web getting safer or more dangerous?* Cybernod. https://blog.cybernod.com/2025/04/is-the-dark-web-getting-safer-or-more-dangerous/

[116] De Domenico, M., & Arenas, A. (27 February 2017). *Modeling structure and resilience of the dark network*. *Physical Review E, 95*(2), 022313. https://harvest.aps.org/v2/journals/articles/10.1103/PhysRevE.95.022313/fulltext

[117] Stagner, J. (27 September 2024). *The dark web: An invisible threat to cybersecurity*. Pulsar Security. https://blog.pulsarsecurity.com/the-dark-web-an-invisible-threat-to-cybersecurity

[118] This source has been previously cited; see Reference No. 46 for full citation details.

[119] National Institute of Justice. (15 June 2020). *Taking on the dark web: Law enforcement experts ID investigative needs*. https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs

86- In conclusion, the dark web constitutes a universal and evolving threat that demands a coordinated global response. Strengthening legal frameworks, enhancing digital forensics capabilities, and fostering public-private partnerships are essential steps toward addressing the limitations of current countermeasures and safeguarding digital ecosystems.

**Proposal for New Internet Infrastructure**

87- This proposal outlines the need for a regular upgrading of the existing World Wide Web (WWW) to include modernized coding standards and advanced security protocols. The concept is based on the recognition that the current internet architecture is structurally vulnerable to systemic exploitation by dark-web actors and advanced cyber threats. Although such an initiative would require extensive international cooperation, strict confidentiality throughout its development, and sustained technical commitment, its potential benefits justify serious consideration. A purpose-built digital framework with embedded resilience mechanisms and continuously adaptive security updates could substantially reduce existing vulnerabilities, even though complete immunity from compromise can never be fully achieved.

88- Building on this premise, empirical evidence from the private sector supports the feasibility of this approach. Apple Inc., for example, has demonstrated the effectiveness of continuous system-level reinforcement in its mobile ecosystem. Through an integrated hardware-software security model and strict control over application distribution, Apple has largely eliminated large-scale "jailbreak" exploitation. Industry telemetry indicates that in Q4 2024 only around 6.7% of IOS devices operated on unsupported software versions, compared with over 17% for Android systems[120]. The company's long-standing success in limiting unauthorized modifications illustrates how architectural control and frequent updates can significantly reduce vulnerability surfaces.

89- Although no digital infrastructure can remain permanently invulnerable, a phased transition to a new designed network-maintained through continuous upgrades, much like Apple's model of iterative platform security could meaningfully diminish the risk landscape. Such an evolution would not eradicate the dark web entirely, but it would extend the timeline required for hostile actors to rebuild comparable hidden ecosystem while providing the global community with a far stronger defensive foundation. Moreover, while the proposal would require global consensus and cooperation, resistance to its implementation could

[120] Certo Software. (7 February 2025). *Phone hacking and mobile security stats*. Certo Insights. https://www.certosoftware.com/insights/phone-hacking-and-mobile-security-stats/

raise legitimate questions about vested interests in maintaining the current unregulated structures. A refusal to participate in collective efforts to secure the digital ecosystem may indicate underlying dependencies or advantages derived from the existing vulnerabilities that enable illicit or covert digital activities.

90- In specific cases, limited connectivity models may also be considered to ensure a reinforced and more secure global network. One of the interim measures that may help is to involve maintaining restricted internet functionality in which core communication channels remain operational, such as internet-based voice calls, while access to messaging applications, social platforms, and general web browsing is temporarily disabled. This approach would significantly reduce dark-web activity by limiting the digital environment required for covert coordination, encrypted messaging, and anonymous recruitment. However, the measure carries inherent limitations: certain users, including hostile actors, may still circumvent restrictions through VPN tools, encrypted tunnels, or proxy services. As a result, such a model cannot guarantee complete operational security, and its effectiveness would remain partial unless coupled with broader architectural reforms and cross-border enforcement mechanisms.

91- Building on the concept of structural reinforcement and limited-connectivity models, an additional protective layer may be introduced through the development of AI-governed conditional access architectures for high-risk digital environments. This proposal is grounded in the documented evolution of concealed digital ecosystems into structured networks facilitating coercion, recruitment, blackmail, and intelligence exploitation. As established throughout this report, engagement with dark-web infrastructures is rarely neutral and may lead to progressive and difficult-to-reverse entanglement. A preventive access-control layer therefore represents a proportionate and forward-looking safeguard aimed at reducing exposure before irreversible harm occurs.

92- This model may be extended to establish risk-based access conditioning applicable to all users seeking entry into concealed digital environments, including anonymizing routing networks and dark-web gateways. Rather than restricting general internet access, the framework would introduce adaptive verification thresholds triggered only when attempts are made to access encrypted or flagged high-risk domains. The objective is to distinguish between legitimate digital activity and entry into environments demonstrably associated with exploitation, recruitment pipelines, and covert operational coordination.

93- Operationally, the architecture could incorporate device-level integrity verification mechanisms capable of detecting anonymization-routing activation patterns; AI-driven

link-classification engines assessing risk probability prior to connection establishment; and behavioral anomaly-detection models identifying indicators of coercion, involuntary navigation, or structured targeting. Protective intervention prompts may be activated in cases of accidental exposure, while vulnerability-sensitive safeguards could dynamically adjust access thresholds according to contextual risk indicators.

94- The purpose of such a system would not be indiscriminate surveillance or broad censorship, but calibrated digital risk management. By introducing narrowly tailored, intelligence-informed control layers, states and technology providers could interrupt known pathways that historically lead to systemic exploitation. In practical terms, these systems could reduce recruitment vectors, limit coercive digital conditioning, and create early-intervention mechanisms for individuals who enter concealed environments inadvertently or under pressure.

95- When embedded within transparent legal mandates, judicial authorization procedures, independent oversight mechanisms, and clearly defined accountability standards, this adaptive access-control model would reposition advanced AI capabilities from instruments frequently exploited within hidden networks into tools of structured protection. Implemented responsibly, such an approach would strengthen digital sovereignty, enhance user security, and mitigate structural vulnerabilities while preserving fundamental rights and freedoms.

96- Comparable exploratory initiatives have already emerged in the academic and research domains to eliminate or impact the dark web. There are ongoing discussions among experts and researchers about rebuilding or redesigning the internet to include:

- The RINA project "Recursive InterNetwork Architecture" advocates replacing the outdated TCP/IP protocol with a more secure and scalable model[121].
- The National Science Foundation's FIND and GENI projects in the U.S., and Europe's FIRE initiative, have explored alternative internet architectures to address current limitations[122].
- Mozilla and other digital rights organizations have called for a rethinking of internet design to prioritize data ownership, decentralization, and user control[123].

[121] Tilmont, L. (30 May 2013). *Making the case to rebuild the internet from scratch*. Worldcrunch. https://worldcrunch.com/tech-science/making-the-case-to-rebuild-the-internet-from-scratch/
[122] Ibidem
[123] Robertson, D. (15 March 2023). *How to rebuild the internet*. Politico. https://www.politico.com/newsletters/digital-future-daily/2023/03/15/how-to-rebuild-the-internet-00087254

- The concept of Web3, a decentralized internet built on blockchain, is gaining traction as a way to reduce reliance on centralized platforms and improve security and transparency[124].

97- Complementary to the structural proposal, two additional initiatives are presented in this report to address the human and operational dimensions of dark-web activity. Both approaches require considerable financial resources and extended implementation periods, and neither guarantees outcomes comparable to large-scale structural reforms such as the creation of a new secured internet framework.

a) Voluntary disclosure and protective incentives. This proposal suggests launching a coordinated awareness campaign and an internationally harmonized reward mechanism in countries genuinely committed to combating dark-web exploitation. It would enable individuals to voluntarily disclose their involvement, submit available information, and identify those responsible for coercion or recruitment particularly comparable to existing witness-protection. However, this approach demands long-term outreach, verified confidentiality frameworks, and continuous oversight, with no assurance of rapid or uniform effectiveness. Nevertheless, over time, successful implementation of this strategy could gradually narrow the scope of dark-web involvement, as growing numbers of participants begin to come forward voluntarily to confess and cooperate.

b) Highly vetted operational teams for managed infiltration. A second proposal involves the establishment of specialized, thoroughly vetted teams composed exclusively of individuals with no prior exposure to dark-web environments. These teams would be divided into two sections: one responsible for controlled infiltration and engagement, and another overseeing investigation, analysis, and accountability. While this model represents a more direct operational response, it carries significant financial burden, prolonged preparation timelines, and a high degree of risk because of the unpredictable nature of hidden online ecosystems. Effective implementation would therefore require strict supervision, transparent legal mandates, and robust international coordination to prevent ethical breaches and ensure mission integrity.

98- These proposals focus on evolutionary redesigns. Although no official authority has yet endorsed a total reconstruction of the internet, ongoing debate underscores the depth of global concern surrounding cybercrime, surveillance, and dark-web activity. Such

[124] Kaur, P. (27 February 2023). *The next phase of the internet is coming: Here's what you need to know about Web3*. The Conversation. https://theconversation.com/the-next-phase-of-the-internet-is-coming-heres-what-you-need-to-know-about-web3-192919

deliberations highlight the urgent need for international cooperation and technological innovation to establish a more secure digital environment.

99- Furthermore, such an initiative would not only aim to enhance safety, privacy, and security but would also serve as a second opportunity for numerous individuals who entered the dark web without full awareness of its irreversible nature, a domain from which departure is seldom possible once engaged. The concealed realities behind the dark web extend far beyond the notion of a mere black market, it has evolved into a covert intelligence network, a hidden architecture of operatives functioning in secrecy and anonymity, effectively forming a decentralized army of digital spies, operating in secrecy and anonymity. The precise number of individuals involved remains indeterminate, yet evidence suggests that their presence is considerably greater than commonly perceived.

100- As an initial and straightforward step, efforts should first be intensified to raise awareness and ensure that this information reaches every household in order to protect as many individuals as possible. Secondly, awareness should be complemented by public announcements in police stations declaring that the state stands ready to protect any individual who has become involved into the dark web and faces threats or coercion to perform certain actions, as previously described.

101- In parallel, major technology providers maintain dedicated customer-service and technical-support systems capable of conducting comprehensive diagnostics and remote remediation for users who suspect that their devices have been compromised. These official channels can perform secure scans, remove malicious software, and restore affected systems without the involvement of third-party intermediaries. Integrating such vendor-based assistance into broader cybersecurity response frameworks would significantly reduce remediation time, prevent additional data exposure, and establish a trusted pathway for individuals to regain secure operation. Recognizing and formalizing this capacity within national and international digital-security strategies would strengthen both preventive and reactive measures against cyber intrusions.

**Conclusions**

102- The dark web has evolved into a complex and deeply embedded threat to global security, individual privacy, and digital sovereignty. Its transformation from a hidden marketplace into covert intelligence network complete with hierarchical structures, psychological manipulation, and advanced surveillance tools, demands urgent attention from policymakers, law enforcement, and technology expert.

103- The exploitation of social media platforms, the targeting of individuals through public challenges, and the deployment of AI-powered spyware illustrate how the dark webs increasingly intersect with everyday life. These developments highlight the limitations of current cybersecurity frameworks and the need for coordinated international responses.

104- While some efforts are underway to strengthen digital defenses and regulate emerging technologies, the scale and sophistication of dark web operations may require more radical solutions. Among these is the proposal to rebuild the internet infrastructure from the ground up, a concept that, although unprecedented, reflects the urgency of safeguarding future generations from systemic digital threats.

105- In parallel to large-scale infrastructural redesign, complementary preventive mechanisms rooted in adaptive artificial intelligence may offer a proportionate and operationally feasible layer of protection. Risk-based conditional access architectures, embedded within device ecosystems and governed by transparent legal safeguards, could help interrupt pathways leading to concealed digital environments before irreversible harm occurs. Such calibrated digital safeguards would reinforce structural reform efforts while preserving fundamental rights and strengthening digital sovereignty.

106- This report, prepared by the Center for Global Studies (PAM-CGS) in cooperation with the Counter Terrorism Executive Directorate (CETD) of the United Nation Security Council, addresses the threat represented by the misuse of spyware technologies in the broader context of illegal surveillance activities and cyber intrusions. CGS is a special program of the Parliamentary Assembly of the Mediterranean. This report forms part of the wider research project on the misuse of spyware, which is supported by contributes to the Observatory established at PAM-CGS, serving as a permanent framework for monitoring, analyzing, and fostering international cooperation on the responsible use of surveillance technologies and the protection of human rights in the digital domain.

Prepared by
the Parliamentary Assembly of the Mediterranean (PAM),
Centre for Global Studies (CGS)

Viale Antonio Onofri, 47890 - 103
Città di San Marino, San Marino

PAM

CGS

www.pam.int
www.cgspam.org