Bitdefender® Global Leader In Cybersecurity

Exploring THE DARKNET

The Subculture of Cybercriminals

Table of contents

Bitdefender Global Leader In Cybersecurity

Introduction

The darknet is a distinct and hidden part of the internet, intentionally inaccessible through standard browsers and invisible to conventional search engines, unlike the deep web, which includes all parts of the internet not indexed by search engines but still accessible with proper authorization. The darknet requires specific software, configurations, or authorization to access, setting it apart from the surface web, which is open to the general public.

Understanding the darknet is crucial for navigating its complexities and comprehending the subcultures that flourish within this anonymity-protected environment. These subcultures, which range from cybercriminal hubs to forums for political dissidents, influence the evolution of internet privacy measures and the landscape of cyber threats, which businesses must contend with in their operations.

Historical Context

The darknet began as a military communications tool designed for secure, anonymous exchanges during the Cold War, utilizing advanced encryption to safeguard messages. Encryption paved the way for further technological advancements that expanded the darknet's capabilities and accessibility. The development of the TOR Network (The Onion Router) significantly enhanced user anonymity by encrypting and rerouting internet traffic through a global relay network, protecting individuals' identities and locations. This was complemented by the rise of cryptocurrencies like Bitcoin, which facilitated anonymous transactions, making the darknet an attractive platform for various activities beyond its initial governmental and military purposes.

Over time, the darknet has attracted a diverse user base, from political activists and whistleblowers to cybercriminals, each drawn by the promise of privacy. This demographic shift has led to a complex subculture rich in unique norms and values. Combined with technological evolutions, it gave birth to various marketplaces, such as the infamous Silk Road, which used the anonymity afforded by TOR and the financial obscurity of cryptocurrencies to trade in illicit goods and services.

These marketplaces were long thought to be untouchable due to their anonymity. However, the FBI's takedown of the Silk Road was a turning point in darknet history, showing that even the darknet is vulnerable to law enforcement.

Common Misconceptions

While it’s undeniable that the darknet provides a haven for various forms of cybercrime, it also offers a critical platform for **whistleblowers** to share sensitive information anonymously, supports individuals in oppressive regimes seeking free speech avenues, and facilitates journalists and researchers who need to access or share censored data securely.

The darknet is often misconstrued as a shadowy underworld used exclusively for illicit activities, yet this perspective overlooks its multifaceted nature and legitimate uses. While it’s undeniable that the darknet provides a haven for various forms of cybercrime, it also offers a critical platform for whistleblowers to share sensitive information anonymously, supports individuals in oppressive regimes seeking free speech avenues, and facilitates journalists and researchers who need to access or share censored data securely. These functions prove indispensable in places where conventional media is heavily controlled nations or where maintaining anonymity is crucial to personal safety and freedom, such as Russia.

The darknet is not as easily accessible as popular myths suggest. It requires specific technical knowledge and tools to navigate, so the average internet user cannot simply hop in and access illicit content. Those who do will find that the darknet is not nearly as vast as the media portrays. It is far smaller in scale than the vast expanse of the surface web, accounting for only 5% of the volume. While it hosts a range of illegal content, a significant portion is dedicated to legitimate activities.

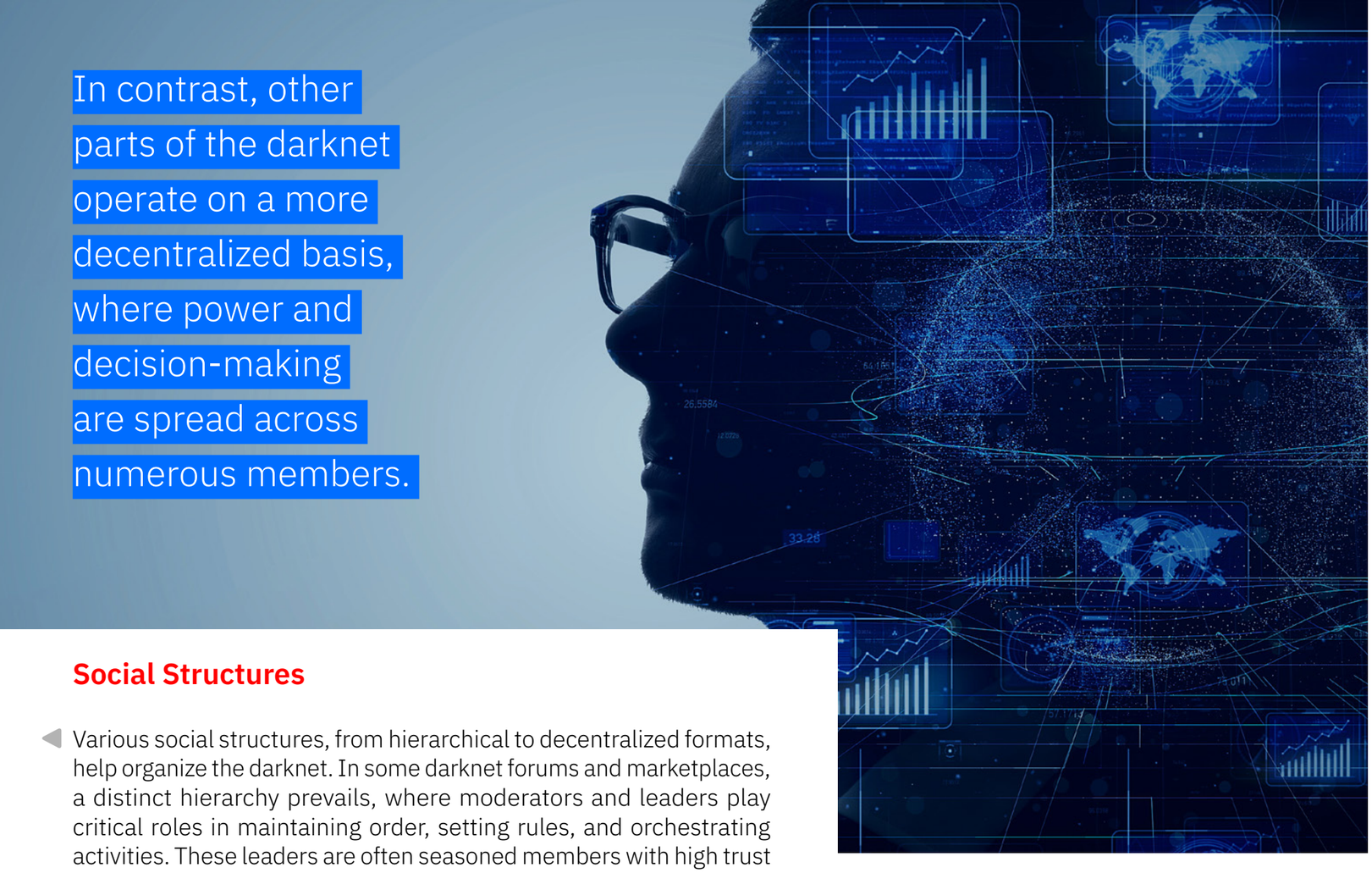
While it is true that the anonymity provided by the darknet does make it harder for law enforcement to operate, this is a tradeoff for the ability to positively protect privacy and enable free expression in restrictive environments.

The **subculture** of Cybercriminals

The darknet hosts diverse communities ranging from hackers to political activists, each bound by shared norms and values that maintain order within this hidden realm. Communication is safeguarded through encrypted messaging apps and specialized forums, which are crucial for preserving anonymity and facilitating a free exchange of ideas. These platforms not only support illicit activities but also serve as venues for legitimate discussions on topics like technology and politics, reflecting the complex social dynamics of the darknet.

Conflict resolution and cooperation within these communities adapt to the lack of traditional law enforcement oversight, relying instead on reputation-based systems to mediate disputes. This framework supports a culture where trust is paramount, and members often collaborate to achieve common goals or resolve threats.

In contrast, other parts of the darknet operate on a more decentralized basis, where power and decision-making are spread across numerous members.



Social Structures

Various social structures, from hierarchical to decentralized formats, help organize the darknet. In some darknet forums and marketplaces, a distinct hierarchy prevails, where moderators and leaders play critical roles in maintaining order, setting rules, and orchestrating activities. These leaders are often seasoned members with high trust and authority within the community.

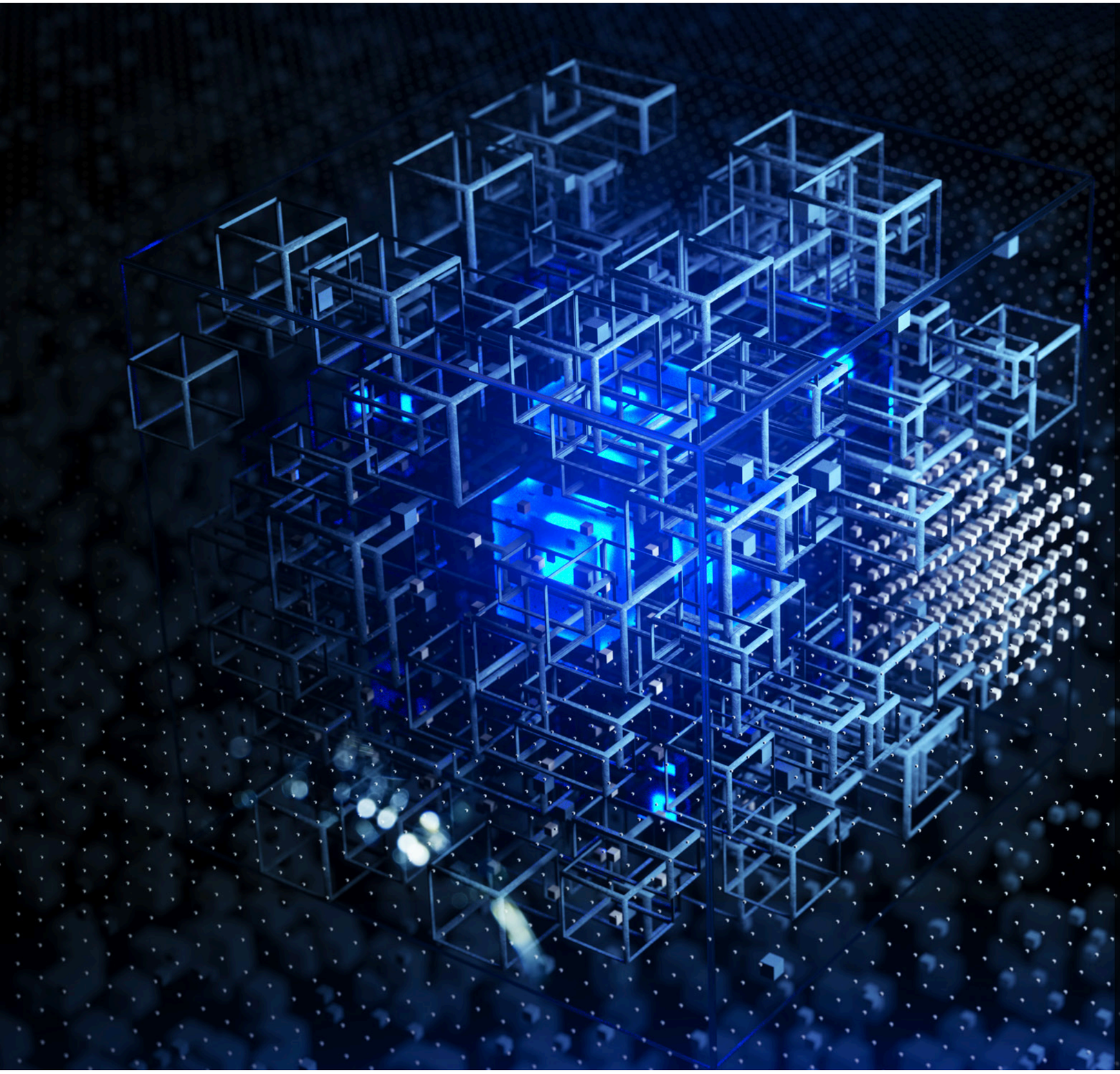
In contrast, other parts of the darknet operate on a more decentralized basis, where power and decision-making are spread across numerous members. This reduces the reliance on a single leader and potentially increases the community's resilience against disruptions such as law enforcement actions.

Becoming a member of these tightly-knit communities is typically rigorous, involving vetting procedures to ensure trustworthiness and loyalty. Prospective members might need to be vouched for by existing members or prove their skills and intentions through various tests. Once admitted, new members gradually learn the cultural ropes, including the specific jargon and symbols in the group. This specialized language and the use of symbols strengthen group identity and serve as a barrier to entry, keeping the uninitiated at bay and enhancing security. These cultural elements signify membership and status within the group, marking the insiders from outsiders and often determining one's access to deeper layers of the community or more sensitive information.

Building Trust

Trust is a commodity as valuable as the goods and services exchanged within its confines. Given the anonymity and legal risks, cybercriminals have developed sophisticated systems to build and maintain trust. Central to these systems are reputation mechanisms, escrow services, and cryptographic verification processes that ensure transaction integrity and authenticity.
Verifying goods and services on the darknet begins with escrow systems, which hold funds in a secure account until all parties are satisfied with the transaction. This system protects buyers from fraudulent sellers by only releasing payment once the goods are received and verified.
Cryptography such as Pretty Good Privacy (PGP) builds on escrow by securely verifying identities and encrypting communications. This ensures that messages, transactions, and identities remain confidential and authentic, shielding them from external and internal threats.

Reputation systems further cement trust within the community. Like feedback systems on well-known e-commerce platforms, darknet marketplaces employ user-generated feedback mechanisms to rate sellers. These ratings give prospective buyers a historical trust profile for each seller, influencing buyer decisions and behavior. Vendor bonds intensify this trust framework, with marketplaces weeding out unserious or fraudulent sellers by requiring vendors to deposit a significant amount of cryptocurrency as a bond. Only those committed to long-term operations are willing to secure such bonds.



Evolution of **Cybercrime** on the Darknet

The evolution of cybercrime on the darknet is a continuous technological arms race, where advancements in security and digital technologies spur cybercriminals to develop more sophisticated methods to bypass these measures. Global events such as economic downturns further influence this innovation cycle, which can increase cybercriminal activities as individuals seek illicit financial gains. These dynamics are encapsulated in the rise of Cybercrime-as-a-Service (CaaS), which has transformed cybercrime into a more organized and accessible profession. CaaS offers ready-made cybercrime tools and services, enabling even those with minimal technical know-how to conduct complex attacks, thus broadening the scope and scale of cybercriminal operations.

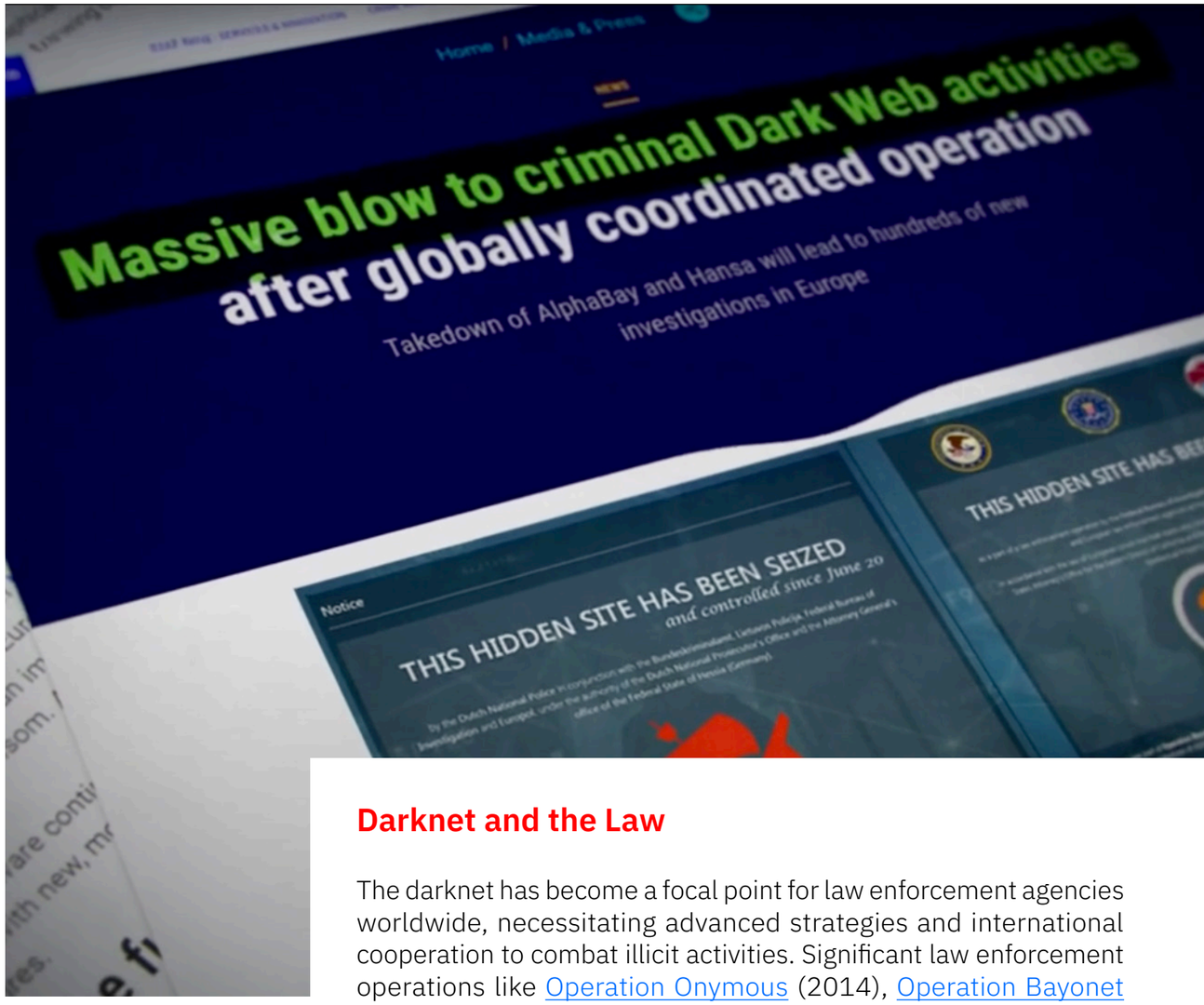
As law enforcement and regulatory bodies ramp up their techniques to combat online crime, cybercriminals on the darknet continually adapt, employing advanced encryption, sophisticated traffic routing, and complex money-laundering techniques to evade detection. This ongoing adaptation complicates law enforcement efforts and highlights the professionalization and resilience of cybercriminal networks. The growing prevalence of CaaS further accelerates this problem, transforming cybercrime, making it more systemic and challenging to curb, and significantly impacting the landscape of global cybercrime on the darknet.

Illegal Activities

The darknet has significantly evolved as a hub for illegal activities, with notable shifts in the types and methods of operations. Drug trafficking on the darknet has expanded beyond traditional recreational drugs to include a broader array of pharmaceuticals and synthetic substances, reflecting advancements in evasion and distribution techniques. This expansion is mirrored in the realm of illegal weapon sales, which have also become more sophisticated and discreet. darknet arms dealers now employ advanced shipping and concealment methods, enabling them to navigate tighter security measures and extend their reach across international borders.

Financial fraud has similarly grown in complexity, with cybercriminals developing new schemes such as elaborate phishing attacks, ransomware, and complex money laundering operations that leverage the global financial system.

The proliferation of cryptocurrencies has further facilitated these illegal activities by providing a means for secure, anonymous transactions that are difficult to trace. This use of digital currencies has simplified funding for illegal dealings and posed significant challenges to law enforcement efforts, complicating the detection and interception of transactions and contributing to the ongoing arms race between cybercriminals and authorities.



Darknet and the Law

The darknet has become a focal point for law enforcement agencies worldwide, necessitating advanced strategies and international cooperation to combat illicit activities. Significant law enforcement operations like Operation Onymous (2014), Operation Bayonet (2017), Operation DisrupTor (2020), and Operation Dark HunTor (2021) have disrupted major illicit markets, bolstering the fight against darknet-based crime. As cybercrime is a global problem, these operations were only successful due to multiple countries' collaborative efforts.

The darknet's anonymity complicates law enforcement efforts, as tracking users and their activities becomes formidable.

Finnish law enforcement deserves special mention for their rapid and effective response to these international efforts in Operation DisrupTor, which set high operational speed and efficiency standards.

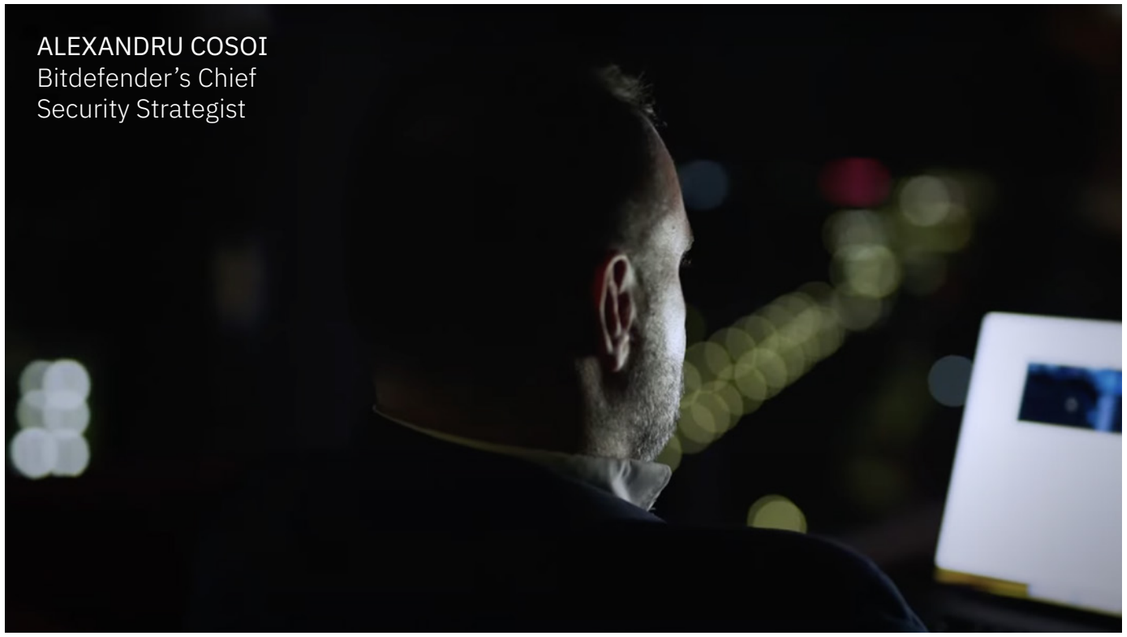
However effective some operations have been, policing the darknet is still challenging. The darknet's anonymity complicates law enforcement efforts, as tracking users and their activities becomes formidable. Jurisdictional issues further complicate these efforts, as cybercriminals often operate across multiple countries, exploiting legal discrepancies between different jurisdictions.

Law enforcement agencies also face operational hurdles, such as a lack of specialized training, challenges maintaining the chain of custody for digital evidence and navigating legal loopholes that cybercriminals exploit. For instance, privacy-focused services and jurisdictions with lax cybercrime laws can inadvertently provide safe havens for darknet operations.

Finnish law enforcement deserves special mention for their rapid and effective response to these international efforts in Operation DisrupTor, which set high operational speed and efficiency standards.

The international community needs to work together to develop a solution to fight cybercrime. Countries adopting cross-border legal frameworks can streamline law enforcement operations. Similarly, enhanced sharing protocols would facilitate timely and effective responses to emerging cyber threats and coordinate efforts against complex, transnational cybercrime networks. Promoting global cybersecurity standards and practices across private and public sectors can enhance data protection, incident response, and critical infrastructure security worldwide, making cybercriminals work harder.

Frontline EXPERTISE



Alexandru Cosoi, Bitdefender's Chief Security Strategist, is experienced in addressing the war on cybercrime. He sees the Darknet's threat landscape as becoming more complex due to technological advancements and more sophisticated cybercriminal tactics driven by advanced analytics and machine learning. Despite this impending challenge, Cosoi predicts that despite the evolution of their tactics, defenders will do the same in growing their countermeasures.

He notes that recent success in dismantling major darknet marketplaces such as Hansa and AlphaBay shows that law enforcement can adapt and become more effective in dealing with these threats. Cosoi emphasizes that these victories did not happen in a bubble but required international cooperation, allowing global law enforcement agencies to effectively leverage their growing capabilities to combat cybercrime.

Cosoi notes that despite innovative new cybersecurity strategies, the burden does not solely lie with law enforcement. Strengthening public-private partnerships will be crucial in helping address the growing challenges the darknet will bring to the battle.

Bitdefender has been and will continue to be a strong partner, playing a proactive role in these efforts. This includes collaboration with law enforcement to provide crucial cybersecurity expertise, which has been instrumental in several key operations. By analyzing network traffic, decrypting communications, and exposing vulnerabilities within criminal networks, Bitdefender has significantly impacted the operational capabilities of darknet markets.

Bitdefender has been and will continue to be a strong partner, playing a proactive role in these efforts. This includes collaboration with law enforcement to provide crucial cybersecurity expertise, which has been instrumental in several key operations.

Building a **Stronger** Future

As we look toward building a stronger future in cybersecurity, the vision is clear: by eliminating walls between international agencies, strengthening public-private partnerships, and embracing the collective responsibility to combat cybercrime, we can forge a path to a safer digital world. This collaborative approach not only enhances our ability to tackle the complexities of the darknet but also preserves it as a bastion of safety for those who genuinely need anonymity—such as whistleblowers and those under oppressive regimes—without it serving as a safe harbor for criminals.

Fighting cybercrime is a shared challenge that transcends borders and sectors. By fostering a deeper understanding among governments, businesses, and individuals worldwide, we can ensure that the darknet does not become a playground for illicit activities but remains a critical tool for personal safety and freedom of expression. Through these concerted efforts, the future of cybersecurity looks bright, securing the digital landscape while upholding the fundamental values of privacy and freedom.

Bitdefender® Global Leader In Cybersecurity

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Trusted. Always.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.