DARK WEB INFOSEC

RESEARCH PAPER

Team - 2

Santhi Sampath Gamidi, Naga Kartheek Peddisetty, Anirudh Devella, Pavan Yenugu

MPS Data Science, University at Buffalo

2nd Semester

CDA 551LEC S4S: Cybersecurity, Privacy & Ethic

Dr. Arman Falahati

May 7th, 2024

Abstract

The Dark Web represents a critical yet enigmatic component of the internet, hidden from conventional search engines and accessible only through specialized anonymizing software like The Onion Router (Tor) and the Invisible Internet Project (I2P). This research paper delves into the multifaceted role of the Dark Web, emphasizing its impact on information security across personal, organizational, and national levels. While it serves as a sanctuary for privacy and freedom of expression, particularly under oppressive regimes, it simultaneously facilitates a range of illicit activities, including cybercrime and illegal marketplaces. By conducting a thorough literature review and employing advanced encryption technologies for analysis, this study explores both the protective and perilous elements of the Dark Web. It examines how the inherent anonymity of the Dark Web can be safeguarded against misuse while supporting legitimate uses. The paper aims to bridge the gap between enhancing cybersecurity measures and understanding the complex dynamics of the Dark Web. The findings reveal the essential nature of robust cybersecurity protocols that effectively mitigate risks without infringing on rights to privacy and freedom, proposing a balanced approach to managing the paradoxes of the Dark Web. This comprehensive examination provides insights into the dual nature of the Dark Web, proposing strategies for improving security practices without compromising the fundamental values of privacy and anonymity.

Keywords

Dark Web, Anonymity Technologies, Tor (The Onion Router), I2P (Invisible Internet Project), Encryption, Privacy Protection, Illegal Marketplaces, Cyber Threats
Information Security, Data Anonymity, Cybercrime.

Introduction

The proliferation of the internet has catalyzed unprecedented levels of connectivity and information exchange. However, it also presents significant challenges in maintaining privacy and security, particularly with the emergence of the Dark Web. The Dark Web offers anonymity and freedom from surveillance, leveraging technologies such as The Onion Router (Tor) and the Invisible Internet Project (I2P) to create secure, encrypted networks. These tools protect user identities and activities from unauthorized tracking and surveillance, fostering a haven for both legitimate privacy-focused users and illicit actors (Macrina & Phetteplace, 2015; Astolfi, Kroese, & Van Oorschot, 2015).

While the Dark Web is often stigmatized due to its associations with illegal activities, it also plays a crucial role in supporting fundamental freedoms and privacy. Tor, for instance, was originally developed to safeguard U.S. intelligence communications but has since become pivotal for journalists, whistleblowers, and human rights activists operating under oppressive regimes (Abbott, Lai, Lieberman, & Price, 2007). This duality underscores the complex nature of the Dark Web—balancing the benefits of anonymity against the potential for misuse. Libraries and educational institutions, recognizing the value of such technologies, have begun advocating for and educating the public about the importance of privacy tools like Tor, reinforcing the principles of intellectual freedom (Macrina & Phetteplace, 2015).

Despite their benefits, technologies enabling the Dark Web, such as Tor and I2P, face numerous challenges and criticisms. Misconceptions and fears about their misuse often overshadow the positive impacts of these tools. Furthermore, these technologies must continuously evolve to address emerging security threats and maintain user trust. Engaging with and enhancing these systems requires a nuanced understanding of both their technical mechanisms and their broader implications for privacy and security (Astolfi, Kroese, & Van Oorschot, 2015). As this research progresses, it aims to demystify the Dark Web and foster a balanced discussion on its role in modern digital ethics and security, emphasizing the critical need for technologies that uphold human rights and personal freedoms in an increasingly surveilled world.

Process and Methodology

The foundation of this research involved a meticulous and comprehensive literature review, which aimed to encompass a wide spectrum of sources related to the Dark Web and its implications for cybersecurity. Initial data gathering was conducted through academic databases such as Google Scholar and IEEE Xplore, as well as through physical resources available in college libraries. This multi-source approach ensured a robust collection of peer-reviewed articles, white papers, and authoritative publications that are closely related to the complexities of the Dark Web and the technologies it employs.

Throughout the research process, advanced search filters were applied consistently to hone on the most relevant studies. Keywords like "Dark Web," "anonymity tools," "Tor," and "I2P" were used to filter out unrelated publications and direct the research focus towards significant contributions in the field. Additionally, AI tools, specifically ChatGPT, played a crucial role in the preliminary stages of research. These AI-generated prompts and initial drafts were instrumental in developing a structured approach to the investigation, helping to outline the main areas of focus and organize the flow of the research narrative.

As the project progressed from the initial stages to the final paper, there was a notable shift in focus towards the specific tools used within the Dark Web, such as Tor and I2P. This transition was reflected in the methodologies used to acquire and analyze data. The research began with a broad query into the security implications of the Dark Web but gradually narrowed to examine how specific technologies facilitate both legitimate and illicit activities. This pivot was evident in the changing nature of the sources cited; earlier references were broader in scope, discussing general aspects of the Dark Web, while later references, acquired through targeted searches on specialized platforms and database filters, focused more on specific technologies and their operational frameworks.

In constructing the final paper, a detailed examination of tools like Tor and I2P underscored their dual capabilities providing anonymity for users seeking privacy and security, and serving as a conduit for unlawful activities. This nuanced examination required a refined methodological approach.

Literature review

The foundation of this research is deeply rooted in the technical mechanisms and architectures of anonymizing technologies, primarily focusing on The Onion Router (Tor) and the Invisible Internet Project (I2P). Both these technologies play pivotal roles in facilitating anonymity on the Dark Web, yet they operate based on distinct architectural principles and protocols designed to shield user identity and enhance security.

Tor:
Tor is renowned for its sophisticated method of "onion routing," where Internet traffic is directed through a worldwide network of servers and volunteers' nodes. This routing process is integral to its functionality; it encrypts the data multiple times and sends it through a series of relays, peeling away one layer of encryption at each step, thus concealing the user's location and usage from any surveillance or traffic analysis. Each relay only knows the identity of the immediately preceding and following nodes, ensuring that no single point can link the source to the endpoint. This method is crucial for maintaining anonymity and is often employed by those needing to evade censorship and surveillance without compromising on their location or identity (Abbott, Lai, Lieberman, & Price, 2007).

I2P:
In contrast, I2P specializes in creating a secure and anonymous layer over the Internet by utilizing a peer-to-peer network structure. Unlike Tor, which is optimized for anonymizing the connections to the regular Internet, I2P is designed primarily for anonymous internal communication. It encrypts network traffic and sends it through a network of routers operated by users, employing garlic routing—a technique like onion routing but which bundles multiple messages together, enhancing security and efficiency. Each user in the I2P network participates as a router, which significantly increases the robustness of the network against surveillance and external analysis (Astolfi, Kroese, & Van Oorschot, 2015).

Both Tor and I2P employ sophisticated methods to counter cyber threats. Tor utilizes transiently held encryption keys and automatic route randomization to thwart traffic analysis and potential de-anonymization attacks. Similarly, I2P's architecture allows users to customize their security and anonymity levels, balancing latency, and privacy according to their needs. This adaptability makes I2P particularly effective in high-security environments (Chertoff, 2017; Basheer & Alkhatib, 2021). Understanding these technologies is crucial for analyzing the Dark Web's impact on cybersecurity.

While Tor and I2P can protect privacy and free speech, they also facilitate illegal activities, raising debates on their regulation to balance privacy with legal and ethical concerns (Kaur & Randhawa, 2020). Exploring these technologies enriches both academic discussions on cybersecurity and practical approaches to enhancing online privacy measures against emerging threats. Thus, technical knowledge from these systems is vital for developing effective strategies in navigating the Dark Web landscape.

Discussion of results

Operational Mechanics

Encryption and Data Routing:
Tor protects users' privacy by routing their internet traffic through a worldwide volunteer network of servers. This process, known as onion routing, involves encrypting data multiple times as it passes through a series of relays. Each relay decrypts only a single layer revealing the next relay in the circuit, which prevents any single relay from knowing the complete path of the data. This ensures that neither the source nor the destination, nor the content of the internet traffic, can be determined at any point (Dingledine, Mathewson, & Syverson, 2004).

I2P, on the other hand, uses a message-based approach, where data is encapsulated in layers of encryption, similar to Tor but functions within a strictly peer-to-peer paradigm. Each data packet in I2P travels through a series of routers in a random and dynamically changing path. This setup not only anonymizes the communication but also makes the network resistant to various forms of attacks and censorship (Zantout & Haraty, 2011).

Comparison of Routing Methodologies:
While both Tor and I2P provide substantial privacy through multi-layered encryption and the use of volunteer-operated relays, their routing methodologies differ significantly in terms of their focus and operation. Tor focuses on anonymizing the data paths on the public internet, making it highly suitable for circumventing censorship and accessing the wider web anonymously. In contrast, I2P is optimized for internal communication between users within the I2P network, making it ideal for those requiring high levels of security and privacy for internal communications rather than accessing the public internet.

The operational mechanics of Tor and I2P highlight their commitment to privacy but also underscore the diverse applications and potential vulnerabilities inherent to each system. Understanding these technologies' intricacies is crucial for users who rely on them for anonymity and security online, as each system's architecture offers different advantages and challenges.

Ensuring Security on the Dark Web

Confidentiality

- **Protecting Information:** The cornerstone of using the Dark Web securely is ensuring that sensitive data remains shielded from unauthorized access. Technologies like Tor and I2P play a crucial role in this by routing internet traffic through multiple servers, thereby masking users' IP addresses and protecting their identity from exposure (Reed, Syverson, & Goldschlag, 1998).
- **Encryption and Anonymity:** Both Tor and I2P utilize complex encryption algorithms to anonymize traffic. This not only protects data from being accessed during transit but also helps maintain user anonymity, making it exceedingly difficult for third parties to track online activities (Dingledine, Mathewson, & Syverson, 2004).
- **Personal Safeguards:** Users are advised to avoid sharing personal information over the Dark Web. Even with encryption, persistent digital footprints can lead to exposure. Adopting practices such as using pseudonyms and ensuring privacy settings are secure across all platforms can significantly enhance confidentiality.

Integrity

- **Data Preservation:** It is essential that data remains intact and unaltered during transmission and storage to maintain its integrity. Technologies like blockchain have been suggested to enhance integrity by creating immutable records of data transactions on the Dark Web (Christin, 2013).
- **Secure Practices:** Users must verify the authenticity of websites and ensure communications are secured using HTTPS, which encrypts data between the web browser and the site, preventing man-in-the-middle attacks and eavesdropping.
- **Threat of Manipulation:** The Dark Web is notorious for hosting malicious actors who may attempt to alter data through various means, including SQL injection, cross-site scripting, and other forms of cyber-attacks. Users should remain vigilant and employ comprehensive security tools and practices to safeguard their data (Canali et al., 2013).

Availability

- **Resource Access:** Ensuring that resources and services are continuously accessible is vital, particularly on the Dark Web where anonymity can complicate direct interactions with service providers. Decentralized services and redundancies can prevent single points of failure, thereby improving service availability.
- **Network Reliability:** The stability of networks like Tor largely depends on the reliability of their infrastructure, which includes volunteer-operated relays and bridges. Fluctuations in the number of active nodes can affect network performance and reliability (Johnson et al., 2013).
- **Potential Disruptions:** Users must be aware of potential disruptions such as network congestion, denial of service attacks, or governmental interference which might impact network availability. Utilizing alternative routes and having backup access methods can help mitigate these risks (Winter & Lindskog, 2012).

Enhancing Security and Privacy through Privacy by Design

Privacy by Design in Tor and I2P: Tor and I2P integrate privacy and data protection from the start, utilizing advanced encryption and routing to protect user data. Tor employs onion routing, where data is encrypted in layers, revealing only the next destination at each relay, thus concealing the data's origin and endpoint (Chertoff, 2017). I2P uses a similar strategy but on a peer-to-peer basis, enhancing anonymity and making data paths hard to trace (Kavallieros et al., 2021).

Network Decentralization and Its Benefits: Both networks leverage decentralization to boost security and resilience. In Tor, the relay system's decentralized structure ensures that compromising one node does not expose the network, keeping data encrypted throughout its journey (Goel, 2015). I2P's network, consisting of numerous volunteer-operated routers, benefits from a robust routing algorithm that dynamically adjusts paths to counter threats and maintain network integrity (Nazah et al., 2020).

Robustness Against Cyber Attacks: Tor and I2P are designed to withstand various cyber threats like DDoS attacks, surveillance, and traffic analysis. Their decentralized routing complicates surveillance, making it difficult to correlate data entry and exit points, thus mitigating spying risks (Dalins, Wilson, & Carman, 2018). Additionally, their ability to reroute around blocked nodes provides resistance against censorship, ensuring information remains accessible even in restricted environments (Basheer & Alkhatib, 2021).

Cybersecurity Threats from the Dark Web

Common Threats:
The Dark Web poses several cybersecurity threats that exploit its anonymity and privacy-enhancing features. These threats include:

- **Data Breaches:** Unauthorized access to confidential information remains a significant risk associated with the Dark Web. Entities operating in the Dark Web can exploit security vulnerabilities to access and steal sensitive personal or corporate data, leading to massive data breaches (Dalins, Wilson, & Carman, 2018).
- **Malware Distribution:** The Dark Web is a notorious platform for distributing malicious software. Malware distributed via the Dark Web can range from ransomware to spyware and Trojans, often targeting unsuspecting users and organizations to disrupt operations, steal data, or demand ransom (Basheer & Alkhatib, 2021).
- **Financial Frauds:** The anonymizing features of the Dark Web also facilitate various forms of financial fraud, including phishing schemes, credit card fraud, and other scams designed to deceive individuals and plunder financial accounts (Kaur & Randhawa, 2020).
- **Ransomware Attacks:** Ransomware, which locks out legitimate users from their systems and demands ransom for access restoration, is commonly spread through the Dark Web. These attacks can cause severe disruptions and lead to significant financial and data losses (Chertoff, 2017)

Challenges in Traceability in Tor and I2P Networks

- **Tor:** Tor's design routes data through multiple relays, encrypting it at each step. This structure means each relay knows only its immediate neighbors in the data's path, not the data's origin or destination, greatly complicating the traceability of users' activities and identities (Goel, 2015).
- **I2P:** Similarly, I2P's peer-to-peer routing makes tracking difficult. Traffic moves through a changing network of volunteer routers, with each path being unique and randomly determined.

This decentralization, paired with end-to-end encryption, significantly enhances anonymity and challenges traceability (Nazah et al., 2020).

Legal Uses and Ethical Considerations of Anonymity Technologies

- **Privacy Protection:** Anonymity technologies such as Tor and I2P play a critical role in protecting personal information, especially in restrictive countries where government surveillance can be invasive. These technologies enable secure communication for journalists, activists, and whistleblowers, who rely on the confidentiality of their online activities to safeguard themselves and their sources from reprisals (Dingledine, Mathewson, & Syverson, 2004). For instance, in authoritarian regimes, these tools help protect the rights of those challenging governmental policies by allowing them to communicate and organize without fear of identification.
- **Educational and Research Purposes:** These technologies also facilitate academic research on topics that may be censored or restricted within certain jurisdictions. By providing access to otherwise blocked resources, they support educational equity across diverse geopolitical landscapes (Lewman, 2014). Furthermore, IT professionals leverage these tools to study internet security measures and test system vulnerabilities in a controlled, secure environment, enhancing the overall robustness of digital infrastructures (Clark et al., 2007).
- **Accessing Public Domain Content:** Platforms like Tor and I2P are instrumental in circumventing geo-restrictions, allowing users from various regions to access public domain content that may be unavailable in their countries due to copyright issues or government censorship (Blossom, 2010). This includes downloading books, articles, and other educational materials that are freely available to the public but blocked regionally.

Illegal Uses

- **Illicit Marketplaces:** While these technologies offer significant benefits, they are also used for illicit purposes. Dark web marketplaces facilitate the anonymous buying and selling of drugs, firearms, and other illegal items without regulatory oversight, posing serious legal and societal risks (Christin, 2013). These platforms operate under the radar of law enforcement, making it challenging to trace and shut down such operations effectively.
- **Malicious Cyber Activities:** Anonymity technologies can be exploited to carry out cybercrimes, including hacking and the distribution of malware. Such activities not only harm individuals and organizations but also compromise the integrity of critical information systems. Additionally, these platforms can be used for distributing or accessing harmful content, such as child exploitation material and facilitating human trafficking, which are significant global concerns (Aldridge & Décary-Hétu, 2016).

Navigating Gray Areas

- **Cryptocurrency Transactions:** The use of cryptocurrencies in conjunction with anonymity technologies is legal but often raises suspicions due to the potential for money laundering or financing illegal activities. The pseudonymous nature of transactions makes it a preferred method for transferring funds discreetly in the dark web economy.
- **Geo-restriction Circumvention:** Circumventing geo-restrictions to access content through tools like VPNs and Tor is generally not illegal but may violate terms of service agreements with content providers. This area remains legally ambiguous and varies significantly between jurisdictions.

Security Considerations When Using Anonymity Technologies

Monitoring by ISPs and Exit Nodes: When using technologies like Tor and I2P, one of the critical vulnerabilities occurs at the points of data entry and exit. Internet Service Providers (ISPs) can detect the use of Tor and I2P, though they cannot decrypt the data or determine what information is being accessed or posted. However, the exit nodes in the Tor network, where encrypted traffic re-enters the regular internet, can potentially expose user data if the traffic is not encrypted with HTTPS. This vulnerability can allow an exit node operator to intercept sensitive information if additional security measures, like SSL/TLS, are not in place.

To mitigate these risks, users should:

- Ensure that websites use HTTPS to prevent exit nodes from viewing unencrypted traffic.
- Use bridges in Tor, which are not listed in the main Tor directory, making it harder for ISPs to detect Tor usage.

Government Surveillance: The potential for government surveillance on users of anonymity technologies is significant due to the resources available to state actors. These organizations can operate large numbers of exit nodes themselves or monitor traffic at key internet exchanges. This monitoring can potentially de-anonymize users if combined with other tracking techniques, such as browser fingerprinting or timing attacks.

Protection against such surveillance includes:

- Using a Virtual Private Network (VPN) in conjunction with Tor or I2P can help obscure one's traffic from ISPs and shield entry points into these anonymity networks from direct monitoring.
- Keeping anonymity software up to date to protect against known vulnerabilities that could be exploited to reveal user identities or activities.

Security Considerations When Using Tor

Who Can Track My Data?

- **Internet Service Providers (ISPs):** ISPs can detect that you are using Tor but cannot see the content or specific sites you visit within the Tor network.
- **Exit Nodes:** The final relay, or exit node, can see your traffic exiting the Tor network. If the site is not HTTPS-secured, the exit node could potentially view this data, although they cannot see your IP address or directly identify you (Edman & Syverson, 2009).
- **Government Surveillance:** With substantial resources, government agencies may monitor Tor exit nodes or employ advanced tracking techniques to target specific individuals.

Mitigating Tracking Risks

- **Use of VPNs:** Employ a VPN to hide traffic from ISPs and enhance encryption.
- **Endpoint Security:** Protect your device against malware to maintain Tor's effectiveness.
- **Website Security:** Only visit verified, secure websites. Avoid sharing personal info on unsecured sites.
- **Regular Updates:** Consistently update your Tor browser and security software to safeguard against new threats.

Additional Security Practices

- **Download Caution:** Be cautious about downloading files or running programs from unknown sources on the dark web.
- **Tails OS:** Use Tails OS for dark web activities to enhance privacy and isolate your main operating system (Dingledine & Mathewson, 2006).

Security Considerations When Using I2P

Who Can Track My Data?

- **ISPs:** Can detect I2P usage but cannot view encrypted content or destinations.
- **Router-Level Observations:** Traffic seen by volunteer routers cannot directly identify users due to encryption and routing protocols.
- **Network Vulnerabilities:** Susceptible to analysis by well-resourced entities, though decentralization provides significant protection.

Mitigating Tracking Risks

- **Robust Encryption:** Multi-layer encryption through routers enhances confidentiality.
- **Network Configuration:** Adjust settings for balance between performance and privacy.
- **Continuous Updates:** Regularly update I2P to secure against vulnerabilities.

Additional Security Practices

- **Safe Browsing:** Exercise caution in sharing personal information and choosing websites.
- **Endpoint Security:** Use antivirus software and keep systems updated to prevent malware.
- **Diverse Communication:** Use I2P’s secure communication tools for enhanced privacy.
- **Firewall and VPN:** Combine I2P with a VPN for extra security and ISP obfuscation.
- **Specialized Operating Systems:** Use systems like Tails or Whonix for additional isolation when accessing I2P.

Navigating the Dark Web: Best Practices and Precautions

Recommended Practices for Dark Web Navigation

- **Research and Understanding:** Learn about the Dark Web and its tools like Tor and VPNs before access, to navigate safely (Bada, Sasse, & Nurse, 2015).
- **Secure Connection:** Use a VPN with the Tor browser for enhanced encryption and identity protection.
- **Tor Browser Usage:** Only download Tor from official sources to avoid compromised software.
- **URL Verification:** Only interact with verified. onion domains to avoid phishing risks.
- **Operational Security:** Avoid using personal information or identifiable details.
- **Skepticism and Vigilance:** Be cautious of scams and verify authenticity before engaging.
- **Regular Updates:** Keep security software updated to defend against new threats.
- **Personal Information Limitation:** Share minimal personal information to reduce risk.

Practices to Avoid on the Dark Web

- **Illegal Activities:** Refrain from illegal actions like buying controlled substances or weapons (Finklea & Theohary, 2015).

- **Suspicious Links:** Avoid clicking links from unknown sources to prevent malware risks.
- **Security Software:** Always keep your VPN and security software active while browsing.
- Misplaced Trust: Be skeptical of too-good-to-be-true offers to avoid scams (Whitty, 2013).
- **Sharing Personal Information:** Do not share personal details that could risk your anonymity or safety.
- **Illegal Content:** Avoid illegal or unethical content like red rooms or exploitative material.
- **Logout Procedures:** Always log out and close your browser after sessions to prevent data leaks.

Conclusion

Balancing Anonymity with Accountability on the Dark Web

The dual nature of technologies like Tor and the Invisible Internet Project (I2P) presents both opportunities and challenges for users of the Dark Web. These tools are crucial for protecting user privacy and freedom of expression, especially in environments where such liberties are restricted. However, the anonymity they provide also creates potential for misuse, such as illegal activities and cyber threats that can exploit the very same features designed to protect user privacy.

The challenge lies in striking a balance between leveraging the beneficial aspects of anonymity technologies and minimizing their potential for harm. This balance requires not only technical solutions but also a robust legal and ethical framework. Policies and regulations that govern the use of such technologies must ensure they do not infringe on fundamental human rights while also deterring and penalizing misuse effectively.

Education plays a pivotal role in achieving this balance. Users must be educated about the risks and responsibilities associated with using anonymity technologies. Awareness campaigns should focus on teaching users how to navigate the Dark Web safely and responsibly, emphasizing the importance of ethical behavior in digital spaces.

Future Directions for Dark Web Governance

- **Ongoing Education:** Promote regular educational initiatives on safe practices and ethical considerations for using anonymity tools.
- **Enhanced Legal Frameworks:** Develop international legal frameworks to effectively address and combat Dark Web challenges.
- **International Cooperation:** Foster global cooperation to enforce laws against Dark Web-related issues like cybercrime.
- **Technology Development:** Continuously advance anonymity technologies to enhance security and accessibility.
- **Public-Private Partnerships:** Strengthen collaborations between governments, businesses, and NGOs to improve Dark Web governance.

By addressing these aspects, the potential of the Dark Web as a tool for positive change and protection of privacy can be maximized, while minimizing its risks and ensuring a safe digital environment for all. The journey towards a balanced approach will require coordinated efforts and a commitment to continuous improvement and vigilance from all stakeholders involved.

References

Aldridge, J., & Décary-Hétu, D. (2016). Cryptomarkets and the Future of Illicit Drug Markets. The Internet and Drug Markets (European Monitoring Centre for Drugs and Drug Addiction: Insights 21). https://data.europa.eu/doi/10.2810/324608

Basheer, R., & Alkhatib, B. (2021). Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. Journal of Computer Networks and Communications, 2021, Article ID 1302999, 21 pages. https://doi.org/10.1155/2021/1302999

Blossom, J. (2010). Content Nation: Surviving and Thriving as Social Media Changes Our Work, Our Lives, and Our Future. Wiley Publishing. https://smpsebastiao.wordpress.com/wp-content/uploads/2010/09/e-book_gcc_blossom_2009_content-nation.pdf

Canali, D., et al. (2013). On the effectiveness of risk prediction based on malicious web site blocking lists. In Proceedings of the 2013 International Conference on Security and Cryptography (SECRYPT). https://doi.org/10.1145/2590296.2590347

Chertoff, M. (2017). A public policy perspective of the Dark Web. Journal of Cyber Policy, 2(1), 26-38. http://dx.doi.org/10.1080/23738871.2017.1298643

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd International Conference on World Wide Web. https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf

Dalins, J., Wilson, C., & Carman, M. (2018). Criminal motivation on the dark web: A categorisation model for law enforcement. Digital Investigation. Elsevier. https://doi.org/10.1016/j.diin.2017.12.003

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The Second-Generation Onion Router. Naval Research Lab. https://www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf

Finklea, K., & Theohary, C. (2015). Cybercrime: Conceptual issues for Congress and U.S. Law enforcement. Congressional Research Service Report. https://sgp.fas.org/crs/misc/R42547.pdf

Greenberg, A. (2015). This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers. Penguin Books.

Kaur, S., & Randhawa, S. (2020). Dark Web: A Web of Crimes. Wireless Personal Communications, 112, 2131–2158. https://doi.org/10.1007/s11277-020-07143-2

Macrina, A., & Phetteplace, E. (2015). The Tor Browser and Intellectual Freedom in the Digital Age. Reference & User Services Quarterly, 54(4), 17-20. Retrieved from https://www.jstor.org/stable/10.2307/refuseserq.54.4.17

Syverson, P., Reed, M., & Goldschlag, D. (1997). Anonymous Connections and Onion Routing. IEEE Symposium on Security and Privacy. https://www.ieee-security.org/TC/SP2020/tot-papers/syverson-1997.pdf

Whitty, M. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. British Journal of Criminology. https://www.cl.cam.ac.uk/~rja14/shb17/whitty.pdf

Winter, P., & Lindskog, S. (2012). How China is blocking Tor. arXiv preprint. https://doi.org/10.48550/arXiv.1204.0447

Appendix

Abbott, T. G., Lai, K. J., Lieberman, M. R., & Price, E. C. (2007). Browser-based attacks on Tor. In International Workshop on Privacy Enhancing Technologies (pp. 184-199). Berlin, Heidelberg: Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-540-75551-7_12

Astolfi, F., Kroese, J., & Van Oorschot, J. (2015). I2P - The Invisible Internet Project. Leiden University Web Technology Report. https://staas.home.xs4all.nl/t/swtr/documents/wt2015_i2p.pdf

Bada, M., Sasse, M. A., & Nurse, J. R. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society. https://doi.org/10.48550/arXiv.1901.02672

Clark, J., van Oorschot, P. C., & Adams, C. (2007). Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability. Proceedings of the Symposium on Usable Privacy and Security. https://www.freehaven.net/anonbib/cache/tor-soups07.pdf

Goel, S. (2015). Anonymity vs. Security: The Right Balance for the Smart Grid. Communications of the Association for Information Systems, 36. https://doi.org/10.17705/1CAIS.03602

Johnson, A., et al. (2013). Users get routed: Traffic correlation on Tor by realistic adversaries. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. https://apps.dtic.mil/sti/tr/pdf/ADA602282.pdf

Kavallieros, D., Myttas, D., Kermitsis, E., Lissaris, E., Giataganas, G., & Darra, E. (2021). Understanding the Dark Web. In B. Akhgar, M. Gercke, S. Vrochidis, & H. Gibson (Eds.), Dark Web Investigation (pp. xx-xx). Springer, Cham. https://doi.org/10.1007/978-3-030-55343-2_1

Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9197590

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communications, 16(4), 482-494. https://doi.org/10.1109/49.668972

Zantout, B., & Haraty, R. (2011). I2P Data Communication System. IEEE Xplore. https://personales.upv.es/thinkmind/dl/conferences/icn/icn_2011/icn_2011_19_10_10010.pdf