Research on Dark Web Applications and Regulatory Methods: Postprint

Authors: Zhao Zhiyun, Zhang Xu, Luo Zheng, Yuan Weiping

Date: 2023-10-08T00:00:00+00:00

Abstract

[Purpose / Significance] Through analyzing the application status and development trends of the dark web domestically and internationally, and conducting in-depth research on the potential harms it may bring, this study aims to provide references for China to carry out dark web supervision.

[Method / Process] This study collects relevant literature on dark web research from domestic and international sources, investigates and summarizes the basic concepts, characteristics, and application situations of the dark web both domestically and internationally, with a focus on analyzing the potential harms that the dark web may bring, as well as existing regulatory measures and trends regarding the dark web at home and abroad.

[Results / Conclusion] The study finds that countries such as the United States, Russia, and the United Kingdom have invested resources in research on dark web data mining and supervision, but currently still face issues such as the abuse of privacy protection and the difficulty of cracking encryption. Regulatory recommendations are proposed, including strengthening dark web technology research, advancing legislation on encryption services, and formulating international rules.

Full Text

The Study of Utilization and Regulations of the Deep Web

Authors: Zhao Zhiyun[1], Zhang Xu[1], Luo Zheng[2], Yuan Weiping[3]
Affiliations: 1. National Computer Network Emergency Response Technical Team/Coordination Center of Jiangsu, Nanjing 210003; 2. National Computer Network Emergency Response Technical Team/Coordination Center of Guangzhou, Guangzhou 510665; 3. National Computer Network Emergency Response Technical Team/Coordination Center of Guangzhou, Guangzhou 510665

Abstract

[**Purpose/Significance**] Following the Paris terrorist attacks, the "deep web" encryption technology used by ISIS terrorists for coordination and planning came to light, with some suggesting the dark web may become the next safe haven for terrorist organizations. This paper analyzes the basic concepts, characteristics, and applications of the deep web, examines its potential harms, and proposes regulatory recommendations to provide reference for dark web supervision in China. [**Method/Process**] This study collected domestic and international literature on deep web research, investigating and summarizing the fundamental concepts, characteristics, and application contexts of the dark web, with particular focus on analyzing its potential harms and existing regulatory measures and trends both domestically and internationally. [**Result/Conclusion**] The study finds that countries including the United States, Russia, and the United Kingdom have invested resources in research on deep web data mining and regulation, yet continue to face challenges such as the abuse of privacy protections and difficulties in encryption cracking. This paper proposes regulatory recommendations including strengthening deep web technology research, advancing legislation on encryption services, and establishing international rules.

Keywords: deep web; terrorist attack; data safety; encryption regulation
Classification Number: G250.73

1. Introduction

The Paris terrorist attacks revealed that ISIS terrorists utilized "deep web" encryption network technology for coordination and planning, with some analysts suggesting the dark web could become the terrorists' next safe haven [1]. Building upon an introduction to the basic concepts, characteristics, and applications of the deep web, this paper conducts an in-depth analysis of its harms and regulatory measures, offering relevant insights and policy recommendations.

2. Basic Concepts and Characteristics of the Deep Web

2.1 Basic Concepts The deep web, also known as the deep network, was first termed by Bergman in 2001 [2]. Typical deep web networks primarily fall into three categories: (1) Anonymous networks like I2P built on packet-switching foundations, where applications can communicate securely and anonymously, including anonymous web browsing, chatting, blogging, and file transfer; (2) Anonymous networks like Tor built on P2P distributed technology, where each user's computer becomes an encrypted relay connection, ensuring no single relay or server can learn the complete connection trail when users access the dark web; and (3) Self-organizing anonymous networks like Firechat built on autonomous mechanisms, where nodes collaborate through specific self-organizing protocols

to complete tasks, adapting to various network conditions including offline scenarios [3-4]. The counterpart to the "deep web" is the "surface web," also called the clear web. According to analyses by ZOL.com.cn and other sites, the surface web accounts for only about 4% of total network data, while the deep web contains approximately 7.9 zettabytes (1 ZB = 100 million TB), representing about 96% of all network data [5].

2.2 Main Characteristics **2.2.1 Simple Access.** Accessing the deep web requires only basic circumvention skills and downloading software of just a few megabytes, followed by simple configuration to achieve anonymous access. Additionally, deep web development organizations have released access software for smartphone platforms, further facilitating dark web connectivity.

2.2.2 Strong Anonymity. The deep web employs distributed, multi-node data access methods and multi-layer encryption, designing an encrypted IP address for each data packet during communication. Obtaining deep web browsing records requires cracking its encryption systems, making user tracking extremely difficult.

2.2.3 Concealed Financial Transactions. Illegal transactions on the deep web predominantly use Bitcoin as payment. In legally recognized Bitcoin trading markets within China, one Bitcoin can easily be exchanged for several thousand RMB, with the entire process from order placement to cash withdrawal taking less than 30 minutes. The complete anonymity of Bitcoin transactions ensures the safety of these illegal traders.

2.2.4 Chaotic Ideology. The deep web was originally created by individuals with libertarian and anarchist ideologies, and many users share these political leanings. With deliberate promotion by the U.S. military and government, libertarian tendencies within the deep web have become particularly pronounced. The network hosts numerous articles attacking socialist state systems and targeting leaders of countries like North Korea and China. Given that even drug trafficking and murder go unchecked, the ideological confusion within this space is readily apparent.

3. Application Contexts and Harm Analysis of the Deep Web

3.1 Application Contexts The success of the deep web is inseparable from U.S. military funding. In May 1996, the U.S. Naval Research Laboratory funded three scientists to publish a paper titled "Hiding Routing Information" at Cambridge University, proposing the technological prototype for the deep web. By October 2003, this project was open-sourced as Tor (The Onion Router), managed by the non-profit Electronic Frontier Foundation (EFF). However, as of 2011, 60% of its funding still originated from the U.S. government. Tor is widely regarded as having established the foundation and order of the deep web ecosystem.

Deep web relay nodes are globally distributed with numerous users. According

to September 2013 estimates by researchers from Georgetown University and the U.S. Naval Research Laboratory [6], Tor maintained approximately 3,000 relay nodes on the internet, primarily located in Germany, the United States, and France, with additional nodes in China, Australia, the Netherlands, Finland, Austria, the United Kingdom, and other countries. Tor' s daily user base numbers around 950,000, widely distributed across Germany, China, the United States, Italy, Turkey, the United Kingdom, Japan, and other nations, with particularly high concentrations in Germany, China, and the United States.

The deep web is extensively utilized in several domains to protect data security: (1) In military applications requiring high communication security, it effectively prevents adversaries from actively tracking and analyzing data, proving significant for military communications security and national defense; (2) In e-commerce, it serves to protect business secrets and personal privacy; and (3) In cloud services, it helps users establish encrypted channels to protect the privacy of cloud service users.

3.2 Harm Analysis Malicious actors exploit the anonymity of the deep web for illegal transactions and cyber attacks: (1) **Illegal Transactions:** These include drug trafficking, child pornography, weapons sales, identity forgery, assassination services, sale of state intelligence, and illicit financial services. The infamous drug trafficking website "Silk Road," shut down in October 2013, utilized the deep web to conceal user identities and evade government oversight and law enforcement [7]. Security researchers discovered in January 2013 that criminals had formed a billion-dollar Bitcoin black market network through the deep web. The deep web' s strong anonymity and concealed financial transactions make it an ideal platform for buying and selling secrets. (2) **Cyber Attacks:** In December 2012, operators used the Tor anonymous network to control the Skynet botnet, launching DDoS attacks against multiple government websites. (3) **Illegal Information Transmission:** Criminals transmit illegal information and images through the deep web and engage in deliberate sabotage through anonymous SMTP servers generating spam email. Anonymous deep web servers also host various other illegal online activities.

The deep web has become a potential "safe haven" for terrorism. ISIS has adopted the deep web as a propaganda machine to circumvent large-scale government censorship. Following the Paris attacks, evidence indicated that ISIS' s propaganda apparatus, Al-Hayat Media Center, was rapidly relocated to the deep web [8]. A jihadist forum published a mirror site of ISIS terrorist data on the deep web around November 15, 2015. After Twitter and Facebook faced government and public pressure to shut down numerous ISIS-related accounts, the forum recommended that visitors use the open-source software Telegram, which features self-destructing messages. Telegram' s complex encryption algorithms, automatic message destruction capabilities, and lack of server-based content storage make it a perfect "terrorist invisibility" channel. Following the Paris attacks, at least 78 ISIS groups were identified on Telegram [8]. In the new

form of counter-terrorism warfare, such services have become national security threats. Due to Telegram' s refusal to cooperate with security agencies, it has been blocked by some national governments.

Encrypted communication networks were utilized in Hong Kong' s "Occupy Central" movement and other mass incidents. During Hong Kong' s "Occupy Central" activities, FireChat was downloaded 100,000 times in less than a day and became the primary communication and dissemination tool for organizers. Its centerless, mesh-networking characteristics enable rapid self-organizing for large-scale information dissemination in dense areas [9]. FireChat was also used in Taiwan' s "Sunflower Student Movement," with some netizens claiming it has become essential software for civil movements. During Hong Kong' s political reform voting period, multiple pan-democratic legislators began using the encrypted communication software Telegram with its "burn-after-reading" functionality.

4. Regulatory Measures and Challenges

4.1 Regulatory Measures Following the Paris attacks, concerns about regulating private information transmission prompted legislative action and increased investment worldwide. France' s parliament formally authorized the government to shut down any internet public communication services involved in terrorist activities during states of emergency [10]. The U.S. Federal Communications Commission (FCC) recommended revising wiretapping laws to expand surveillance scope, with officials calling on technology companies to provide access to encrypted communications including calls, messages, and emails. The FBI and CIA further demanded that Apple and Google create backdoors in smartphone communication encryption [11]. The United Kingdom increased funding for MI5, MI6, and GCHQ by 15%, planning to invest £1.9 billion over five years to combat cyber attacks and cyber terrorism, establishing a new national cyber center 集中 ing Britain' s top experts [12]. The German government planned to add 500 positions in intelligence agencies [13]. South Korea, Vietnam, and other countries have also strengthened legislation addressing cyber terrorism and communication privacy protection [14-15].

4.2 Key Regulatory Challenges Despite substantial investment in combating the deep web, prospects remain uncertain. UK government funding for university research continues to increase, with the Heilbronn Institute—a collaborative organization of research elites from multiple British universities—focusing primarily on tracking research projects directed by intelligence agencies. In February 2014, Russian President Putin signed a bill allowing the government to disconnect Russia' s entire internet during necessary periods and requiring website owners with daily visits exceeding 3,000 to register with the government and relinquish anonymity. U.S. government agencies including the FBI, DEA, ATF, and NSA spend tens of millions of dollars annually to infiltrate illegal deep web sites. The U.S. Defense Advanced Research Projects Agency

(DARPA) launched the Memex deep web search engine in early 2015 to conduct deep mining of the dark web, accessing hidden information beyond the reach of Google and other commercial search engines, though this tool is exclusively available to the U.S. military. A leaked NSA document from June 2012 revealed that the agency was not optimistic about cracking the deep web, explicitly stating it would "never be possible to completely uncover the real identities of all deep web users" [16]. Notably, the founder of Silk Road was not caught through vulnerabilities in the deep web itself, but rather through excessive recruitment and code assistance information left on the regular internet.

4.2.1 Cloud Services Complicate Tracking. Experts indicate that cloud services make tracking illegal activities on the deep web more difficult. For instance, Amazon' s Elastic Compute Cloud (EC2) supports virtual computer functionality, and Tor developers have called on people to join this service to run bridges—interconnection devices between two or more networks or virtual points for secret networks through which communications can be routed. With cloud service support, creating a substantial number of bridges becomes easy, spawning more and better "hiding places" and increasing the number of anonymous networks.

4.2.2 Privacy Protection Enables Abuse. The deep web represents a product of vigorous internet technology development, reflecting legitimate demands for anonymous browsing and privacy protection, yet it is simultaneously filled with illegal criminal transactions and ideological attacks. This creates a difficult contradiction: how to balance privacy protection with combating deep web crimes. U.S. officials have bluntly questioned European countries over whether excessive focus on privacy issues sacrifices public security capabilities. When the U.S. established the new Cyber Threat Intelligence Integration Center in February 2015, President Obama promised to advance stricter cybersecurity legislation. France' s parliament passed new anti-terrorism laws in 2015, including stricter monitoring of online platforms and penalties for terrorist propaganda. However, currently no country has enacted detailed legal constraints on deep web access behavior.

4.2.3 Hidden Interfaces and Mobile Monitoring Difficulties. Deep web communication is built upon the internet, and monitoring deep web access software downloads could effectively track usage patterns. However, deep web "interface" information is currently disseminated covertly, typically through private chats or one-to-one communication, making it difficult to identify downloaders and their intentions, especially when they use BT downloads and cloud storage sharing to evade supervision. The proliferation of mobile devices has further increased the frequency of deep web access software downloads and usage on smartphone platforms, raising the cost of tracking user behavior.

5. Recommendations for Strengthening Deep Web Regulation

Given that the deep web enables harmful information penetration, conceals real network identities, and facilitates electronic black market transactions posing significant security risks, the following recommendations are proposed to better combat harmful deep web activities:

5.1 Strengthen Deep Web Technology Research for Beneficial Applications. The deep web is a product of robust internet technology development that reflects legitimate public demands for anonymous browsing and privacy protection, yet it is filled with illegal criminal transactions and ideological attacks that could potentially become channels for enemy recruitment and infiltration. Sufficient attention should be paid to researching these technologies, strengthening confidentiality management, and taking proactive measures against deep web-related leaks. Additionally, the technical architecture of the deep web effectively defends against network probing and traffic analysis attacks, offering valuable insights for constructing secure command and office networks for military applications.

5.2 Advance Legislation on Internet Encryption Services. To effectively address regulatory challenges posed by encryption applications in the deep web, relevant state departments should strengthen legislation on internet encryption service supervision. First, clearly define and establish the legal basis for internet information content security supervision, clarifying the rights and obligations of regulatory agencies, service providers, network operators, and users, and implementing network information security responsibilities. Building upon this foundation, further refine laws and regulations concerning internet encryption service supervision, drawing on international common practices in counter-terrorism, technical investigation, crime prevention, child protection, and intellectual property rights. For example, explicitly require enterprises providing encryption services to offer regulatory interfaces before data encryption and compression to meet government management needs.

5.3 Establish International Rules to Constrain Abusive Monitoring Using Technological Advantages. In August 2013, the U.S. National Security Agency admitted to monitoring the Tor network and sharing intercepted information with other agencies including the DEA and FBI, claiming it was primarily used to solve drug and child pornography cases. However, the agency avoided addressing whether such cyber monitoring violates national sovereignty, infringes upon citizens' fundamental rights, or complies with international law. To fundamentally ensure the positive applications of Tor on the internet and prevent technological powers like the United States from privately abusing network capabilities, it is necessary to promote the establishment of a multilateral, transparent, and democratic internet governance mechanism, accelerate the formulation of cyberspace behavior norms, regulate the behavior of various actors, and expedite the creation of a new cyberspace order.

References

[1] Dark web will become the next safe haven for ISIS [EB/OL]. [2015-12-20]. http://www.freebuf.com/articles/86048.html.
[2] RAGHAVAN S, GARCIA-MOLINA H. Crawling the hidden Web [EB/OL]. [2015-08-12]. http://ilpubs.stanford.edu:8090/456/1/2000-36.pdf.
[3] SUN L, PAN J. "Deep web" : The gray area of the internet world [J]. International Science and Technology Trends, 2005(12): 36-39.
[4] LIU X. Research on anonymous communication based on Tor network [D]. Shanghai: East China Normal University, 2011.
[5] Sinful paradise? Taking you to understand the unsearchable dark web [EB/OL]. [2015-12-20]. http://oa.zol.com.cn/494/4945765_{all}.html.
[6] JOHNSON A, WACEK C, JANSEN R, et al. Users get routed: Traffic correlation on Tor by realistic adversaries [C]// Proceedings of the 2013 ACM SIGSAC conference on computer & communications security. New York: ACM, 2013: 337-348.
[7] "Silk Road" suspected of drug trafficking [EB/OL]. [2015-01-14]. http://www.techweb.com.cn/internet/2015-01-14/2115554.shtml.
[8] After Paris, ISIS moves propaganda machine to Darknet [EB/OL]. [2015-12-20]. http://www.csoonline.com/article/3004648/security-awareness/after-paris-isis-moves-propaganda-machine-to-darknet.html#tk.rss_{all}.
[9] New media usage in Hong Kong' s "Occupy Central" incident [EB/OL]. [2015-12-20]. http://www.neweyeshot.cn/archives/15961.
[10] French parliament authorizes government to shut down networks at any time [EB/OL]. [2015-12-20]. http://www.chinanews.com/gj/2015/11-20/7636179.shtml.
[11] FCC chairman: FBI wants more wiretapping power after Paris attacks [EB/OL]. [2015-12-20]. http://www.cnbeta.com/articles/449539.
[12] UK provides additional funding to three major intelligence agencies to counter terrorist threats [EB/OL]. [2015-12-20]. http://www.chinanews.com/gj/2015/11-16/7626267.shtml.
[13] Intelligence agencies "recruiting troops"to combat terrorism and far-right extremism [EB/OL]. [2015-12-20]. http://www.dw.com/zh/%E6%83%85%E6%8A%A5%E9%83%A8%E9%97%A%E5%AF%B9%E6%8A%97%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E4%B8%8E%E6%9E%81%18851449.
[14] Korean media: In the era of global counter-terrorism, the South Korean government cannot continue to "watch from the sidelines" [EB/OL]. [2015-12-20]. http://finance.chinanews.com/gj/2015/11-17/7626853.shtml.
[15] Vietnam demands severe punishment for users inciting terrorism on social networks [EB/OL]. [2015-12-20]. http://www.apdnews.com/XinHuaNews/264368.html.
[16] The hidden "deep web"empire [EB/OL]. [2013-11-18]. http://www.nbweekly.com/news/world/201311/3501
[17] Onion link [EB/OL]. [2015-12-20]. http://onion.link/.
[18] ZHANG W. Challenges and countermeasures for onion routing applications [J]. Video Engineering, 2015, 39(1): 103-105.

Author Contributions

Zhao Zhiyun: Conceived the research topic and revised the final manuscript;
Zhang Xu: Researched deep web regulatory details and drafted the manuscript;
Luo Zheng: Analyzed deep web concepts and characteristics, and organized regulatory measures;
Yuan Weiping: Investigated deep web application contexts.

Responsible Editor: Xu Jian
Received Date: December 30, 2015
Publication Date: April 19, 2016

Note: Figure translations are in progress. See original paper for figures.