Article

Not peer-reviewed version

Technology Acceptance Level of Dark Web Users

H.Eray Çelik * and Serbest Ziyanak *

Posted Date: 17 April 2024

doi: 10.20944/preprints202404.1156.v1

Keywords: Dark Web; Deep Web; Structural Equation Modeling; Technology Acceptance Model

 doi:10.20944/preprints202404.1156.v1

Article

Technology Acceptance Level of Dark Web Users

Serbest Ziyanak [1,2] and H. Eray Çelik [1,2,*]

[1] Van Yüzüncü Yıl University, Statistical Information Science, Van, Turkey
[2] Khoja Akhmet Yassawi International Kazakh-Turkish University, Engineering Faculty, Department of Computer Engineering, Kazakhstan
* Correspondence: ecelik@ayu.edu.kz

Abstract: "Dark Web" usually describes a new world of e-living space perceived as a place, free from constraints, in which its main actors generally are criminal, unstable, and mentally disturbed individuals. Nowadays, advancements in information and internet technologies have made the Dark Web more accessible in recent decades. The Dark Web is a virtual world component; therefore, assessing users' behavior may be crucial in understanding motivation to use it. This study aims to discuss the behavior patterns of Dark Web users within the theoretical framework of the technology acceptance model via a structural equation model. The resulting structural equation model showed that considered causal relationships were statistically significant.

Keywords: Dark Web; Deep Web; Structural Equation Modeling; technology acceptance model

1. Introduction

Rapid developments in information and communication technologies (ICTs) are reshaping our lives and society. New technologies are intensively reorganizing our daily lives. Internet and social media use is expanding worldwide, with 66% of the global population accessing the Internet and 62.3% using social media [1,2]. Due to these advancements, accessing the collective knowledge of billions of people has become effortless [3].

Simultaneously, numerous studies focus on modeling and explaining the behavioral patterns of modern individuals using these technologies. Using clear and concise language is essential when explaining user behavior related to information technologies. In recent years, many new concepts have become associated with information technologies and have become the main determinants of their use. Several studies have been conducted in this field [4]. The concepts of computer crime, internet crime, cybercrime, virtual crime, and crime in informatics have become ubiquitous in our daily lives. These terms now define the landscape of information technologies. The rise of digital aspects in everyday life has made cybercrime and victimization common [5].

The Internet's ever-expanding presence has made cybercrime a global phenomenon. Criminals are constantly changing their methods due to the rapid pace of technological advancements [6]. As a result, new types of crimes and methods of committing them are emerging. The UNODC (2022) highlights the challenges posed by informality in social media tools, location-independent crimes, rapid communication of criminal groups, different approaches in countries' internet policies, legal deficiencies, proxy servers, Deep Web, Dark Web, etc. [2]. It is necessary to urgently initiate legal studies in this field and establish a common legal and administrative approach among countries to combat crimes committed on the Internet effectively.

Today, cybercrimes include individual crimes and crimes with organized structures. Organized cybercrime's structural complexity and organizational form vary [2]. In addition to the lack of legal regulations in the fight against cybercrime, social media platforms at the global level and the lack of basic information technology literacy are essential factors.

Hackers view interventions on the web, such as shutting down websites, blocking access, slowing down internet speed, and censorship, as a violation of internet freedom. They believe such interventions and legal regulations have created a dark, out-of-control world. This world is similar

 doi:10.20944/preprints202404.1156.v1

to the dark gates of Morannon in J.R.R. Tolkien's Middle-earth, a land of evil that is almost impossible to conquer. The term "Dark Web" describes a new world of e-living space perceived as a place of freedom, free from constraints but associated with evil. Unfortunately, this world has been rapidly invaded by deviant, criminal, unstable, sociopathic, lawless, and mentally disturbed individuals who have become the main actors. The concepts of Freenet and Darknet, first discussed in the 2000s, have evolved into a new dimension today. The recent development of language models for artificial intelligence has significantly impacted. The widespread Use of AI technologies has brought the "Dark Web" back into discussion. As a result of AI applications, internet users' behavior patterns and competence levels are rapidly changing.

The general purpose of this study is to attempt, for the first time in the literature, to model technology acceptance among Dark Web users. Within the Technology Acceptance Model (TAM) framework, it is used to understand and explain the behavioral patterns of Dark Web users. For this purpose, the classic TAM was extended to include trust and risk factors. User behavior was predicted based on the causal relationships between the latent variables in the TAM.

2. Surface Web, Deep Web, and Dark Web

While the Internet is a resource that enables the exchange of data for communication between individuals in a decentralized manner, there are differences in how individuals access information online based on standard or proprietary web browsing and encryption protocols. There are three ways to describe how data is accessed over the Internet. Therefore, the Internet ecosystem is divided into the Surface, Deep, and Dark web [3,7–9].

Most Internet users browse content using the Surface Web, a part of the Internet where popular search engines index sites and can be easily viewed using traditional web browsers. The Internet is designed as a platform for millions of people to interact online. The most publicly accessible part of the Web world is the Surface Web. This area includes all the websites or pages found using search engines such as Google, Bing, and Yahoo. In short, the Surface Web is what the average user calls "the Internet" [2,10–15].

Web pages that standard search engines cannot index are part of the Deep Web or hidden web [16]. Deep Web pages are not accessible through web browsers and are therefore not included in the Surface Web. The Deep Web is the more significant part of the iceberg hidden from Surface Web users [10,17]. The Deep Web is not only used for criminal or malicious activities. Authorities and policymakers are interested in using the Deep Web for illegal practices [15].

The Dark Web is an encrypted network built on the Internet that can be accessed using specialized software. It contains websites that are not indexed and are, therefore, part of the dark web. The networks are defined as dark because they allow users to hide their identities and support illegal activities. The logical structure of the Dark Web is based on protecting user identity and hiding network activities [18]. The Dark Web is often portrayed as a hub for illicit and enigmatic activities [10,19].

The Dark Web has existed beneath the internet surface for a long time. It has become a powerful tool against governments [18]. Despite this, the Dark Web remains obscure to most people. Its notoriety increased in 2013 with the arrest of Silk Road operator Ross William Ulbricht (aka Dread Pirate Roberts) [20].

The Dark Web, part of the Deep Web, is accessible only through specialized computer software. It is primarily used for illegal activities such as cybercrime, drug trafficking, and human exploitation. According to Gollnick and Wilson, most internet users are unaware of the Dark Web and do not use it [21].

Although many studies treat the concepts of Deep Web and Dark Web as the same, there is a significant difference between the two [22–24]. The Deep and Dark Web hosts over 90% of the Internet [3,10,25–27]. The Dark Web is a subset of the Deep Web [28,29]. Although the Deep Web is used for both legal and illegal activities, the Dark Web is primarily used for illegal activities. While the size of the Dark Web is immeasurable, the size of the Deep Web is much larger than the visible Surface Web. The Deep Web is estimated to be 4000-5000 times larger than the Surface Web. As a result of the

 doi:10.20944/preprints202404.1156.v1

changing dynamics of information access and presentation, the Deep Web is growing exponentially at a rate that cannot be quantified [10,15,22,23]. However, due to the anonymity of the Dark Web, information about its users and overall traffic is scarce. Measuring and determining the size of the Dark Web and the number of users is impossible. Published reports and research need to be more comprehensive in fully describing the content and traffic of the Dark Web [15]—studies on this expanding facet of the Internet focus on developing surveillance mechanisms [14,30].

Several distinguishing features must be present to be considered a Dark Web site. The Dark Web contains obscure and complex data and is difficult to access [31]. It refers to a space that can be accessed using an encryption tool called The Onion Router (Tor) [32–34]. Accessing the Dark Web involves using specific networks, namely Tor, I2P, and Freenet [11]. Among these networks, Tor is the most commonly used due to its user-friendliness and ability to protect user privacy, particularly for those seeking to bypass censorship [35–38][[. The Tor network is estimated to have between 2 and 2.5 million daily users [39–41]. Tor is designed to protect the privacy of all users, even those who may wish to conceal their identities for illicit purposes [19,42,43]. The Use of Dark Web platforms by cybercriminals has significantly increased the number of illegal products available, from a few thousand in 2013 to hundreds of thousands today [40,41]. Tor is frequently used for cybercriminal activities [28].

Generative AI is increasing, which presents both opportunities and cybersecurity threats. Cybercriminals are adopting and utilizing generative AI tools, such as WormGPT and FraudGPT, to enhance their attacks, as evidenced by posts on Dark Web forums. Domenic, from AVAST, reports that ChatGPT clones have emerged on the Dark Web [44].

The Dark Web is anonymous and cannot distinguish between criminals and ordinary users [10]. Its unique structure makes it user-unfriendly, unlike the web platforms we know in the classical sense. Access is complicated, requiring more internet proficiency than normal internet users. This study aimed to model the behavior patterns of Dark Web users using the Technology Acceptance Model (TAM). The classical TAM has been expanded to include risk and trust factors. This new model was used for the first time in the literature to determine the level of technology acceptance among Dark Web users.

3. Technology Acceptance Model (TAM)

Technology acceptance refers to an individual's willingness to use technology. TAM aims to explain technology usage by individuals through the lens of information and psychological theories. It has a wide range of applications in various disciplines and is used to describe how individuals use technology within these fields. Based on the Theory of Reasoned Action (TRA), Davis developed the TAM [45]. TAM aims to estimate individual behavior with the use of a customized system. Its primary purpose is to predict and explain user acceptance of an information system. The model assumes two factors when predicting individual behaviors of technology usage: perceived usefulness and perceived ease of Use [45,46]. TAM suggests that user acceptance is determined by Perceived Usefulness (PU) and Perceived Ease of Use (PEU). This study used an extended model by adding Perceived Trust (PT) and Perceived Risk (PR) factors, which are the primary two factors in the model. These four factors (Figure 1) explain the model's causal relationships between attitude, intention, and behavioral use. The model uses intrinsic relationships to describe behaviors.

PEU is a perception that assesses the extent to which an individual is confident in using a system and whether the Use of the system can make it easier for someone to do something or does not require much effort. According to Davis (1989), it reflects the user's belief that information systems are easy to use and do not require much effort. It also includes the perceived ease of use of those who wish to use the information system [45].

PU is an individual's evaluation of the benefits that are provided by the use of new information technology in a particular context. In the TAM, perceived usefulness reflects task-related productivity, performance, and effectiveness. Usability is the degree to which the user expects the target system to be easy to use [45]. Perceived usefulness and perceived usability are evaluations of

 doi:10.20944/preprints202404.1156.v1

the usefulness and ease of using a given system. It is important to note that these evaluations are subjective and should be identified as such.

Many studies have experimentally confirmed the influence of PU and PEU on attitude toward system usage and its subsequent impact on behavioral intention [45–52]. In summary, the two most critical factors in explaining attitudes toward the use of technology are the PU and PEU latent variables in TAM. Attitudes toward technology will translate into behavior when the technology is highly usable and useful.

Trust is a complex and multi-dimensional concept [47]. It positively impacts users' attitudes [48]. Trust is the state of reliability in an individual's positive expectations of what others will do based on previous interactions in various situations [49]. The trust variable is directly related to PU. Research has shown a positive correlation between trust and PU. A sense of pre-existing trust in a system can reduce uncertainty and increase confidence in its use, affecting the adaptation to using the system. It is also possible to define perceived trust using the Dark Web as a willingness to take risks.

E-services are software-based information systems accessed via the Internet [50]. Perceived risk, which refers to the probability of loss from using a desired service, is a crucial factor in online transactions [50,51]. Users' acceptance or rejection of technology is closely linked to their risk perception [52]. The concept of perceived behavioral control in Ajzen's theory of planned behavior explains the relationship between perceived risk and intention to act. Perceived risk has the potential to positively influence the willingness to perform a task since attitudes typically determine actions [53]. It is important to note that risk is not a one-dimensional concept. A great deal of research has identified various aspects of risk. These include psychological, performance, privacy, financial, time, security, social, and overall risk [50,54–58]. It is a realistic problem that users perceive a lack of security, safety, and privacy in a system. Cyber attacks like hacking and phishing can deter users from using internet-based services [59–63]. It is essential to prevent these attacks and ensure the security of users' information.

Individual attitudes toward a specific behavior are shaped by personal beliefs and evaluations of its consequences [64]. Attitudes are a person's overall evaluation of the performance of a behavior; attitudes are a person's evaluation of the performance of a behavior [47]. The Theory of Planned Behavior (TPB) posits that individual attitudes impact users' behavioral intentions [65], subsequently influencing their behavior. Behavioral intention to use refers to the strength of an individual's intention to engage in specific behaviors or activities [51].

Figure 1 below shows the theoretical model of the TAM, which includes the PU, PEU, PT, and PR latent variables, as well as the causal relationships of the Attitude Towards Using the Dark Web (ATU-D) and Use of the Dark Web (USE-D) latent variables.

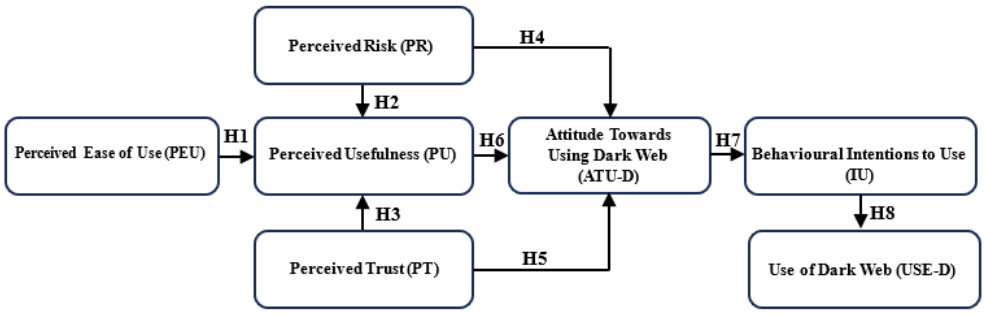

Figure 1. Research Model.

This research examines and discusses the causal relationships related to the following hypotheses within the given theoretical model:

H1: Perceived ease of use (PEU) positively affects the Dark Web users' perceived usefulness (PU).

H2: Perceived risk (PR) positively influences the Dark Web users' perceived usefulness (PU).

H3: Perceived trust (PT) positively influences the Dark Web users' perceived usefulness (PU).

H4: Perceived risk (PR) positively affects Attitudes towards the use of the Dark Web (ATU-D).

 doi:10.20944/preprints202404.1156.v1

H5: Perceived trust (PT) positively affects Attitudes towards the use of the Dark Web (ATU-D).

H6: The perception of usefulness (PU) positively impacts attitudes toward the use of the Dark Web (ATU-D).

H7: The positive effect of Attitude Towards Using the Dark Web (ATU-D) on Behavioural Intentions to Use (IU).

H8: Behavioral intentions to use positively impact the use of the Dark Web (USE-D).

4. Materials and Methods

4.1. Participants and Data Collection

This study aims to model the usage behaviors of internet users on the Dark Web within the TAM framework. The elements in the theoretical model will be explained, and the relationships between them will be explored. In this regard, an active Dark Web user identity was created for eight months to reach Dark Web users, and a trust-based relationship was established with Deep Web users. A total of 200 invitations were sent to individuals who have been using the Dark Web for at least two years, with 174 respondents providing complete answers to the research questions. The survey link was shared on five different Dark Web forums, and all calls for participation were made through the Dark Web to ensure user safety. Participants declared their voluntary and informed consent to participate in the study.

The participants' average age was 32, and they reported an average daily internet usage time of 8 ± 0.75 hours. The average time spent on the Dark Web was calculated as 6.5 hours. Of the participants, 58.6% reported using English, 15% Russian, 10% German, and 16.4% other languages. Notably, all participants were male, and 32% reported being married. All participants defined the Dark Web as a space of freedom and reported using it to hide their identities.

4.2. Measure

Twenty-five items were collected under seven latent variables, as shown in Figure 1. USE-D (3 items), IU (3 items), ATU-D (3 items), PU (4 items), PEU (4 items), PR (4 items) and PT (4 items). The items in the model are compiled and adapted from different studies [47,51,66–68]. The linguist applied the prepared measurement tool in each field in English, Russian, and German. Each question is measured on a 5-point Likert scale with the endpoints "strongly agree (5)" and "strongly disagree (1)".

4.3. Data Analysis and Results

Structural Equation Modeling (SEM) was used to explain the causal relationships of the theoretical model described in Figure 1. SEM is used in many disciplines to solve research problems related to causal relationships between latent structures measured by observed variables [47,69,70]. The covariance structure between the observed variables is used to examine the linear structural relationships between all the variables in the model. SEM allows researchers to identify the direct and indirect effects between variables. LISREL 9.3 was used for the analysis.

Structural Equation Modeling (SEM) was used to explain the causal relationships of the theoretical model described in Figure 1. SEM is used in many disciplines to solve research problems related to causal relationships between latent structures measured by observed variables [53,74,75]. The covariance structure between the observed variables is used to examine the linear structural relationships between all the variables in the model. SEM allows researchers to identify the direct and indirect effects between variables. LISREL 9.3 was used for the analysis.

Confirmatory factor analysis (CFA) was used to test the reliability and validity of the data obtained. The measurement model consisted of 25 items describing seven latent constructs: PEU, PU, PR, PT ATU-D, IU, and USE-D. Testing the measurement model obtained a good fit to the data. The results of the CFA indicate that the measurement model was statistically acceptable: $\chi 2/df=1.71$, GFI=0.90, AGFI=0.90, and CFI=0.92.

Cronbach's Alpha (CA) and Composite Reliability (CR) provided strong evidence of reliability [77]. To establish scale reliability, CA and CR must be greater than 0.70 [54]. In this study, the overall

 doi:10.20944/preprints202404.1156.v1

CA values were above 0.70 for each factor, as shown in Table 1, and the overall CA value was calculated as 0.907. Similarly, CR values above 0.70 were obtained for all factors. The fit indices indicate a good fit between the data and the measurement model. The CFA results are presented in Table 1 below.

Table 1. Confirmatory factor analysis results (Convergent reliability).

Factor / Item	Std. loading	Cronbach's α	CR
Perceived Ease of Use (PEU)		0.796	0.808
PEU1	0.74		
PEU2	0.76		
PEU3	0.78		
PEU4	0.70		
Perceived Usefulness (PU)		0.787	0.818
PU1	0.74		
PU2	0.78		
PU3	0.78		
PU4	0.66		
Perceived Risk (PR)		0.850	0.863
PR1	0.75		
PR2	0.72		
PR3	0.80		
PR4	0.76		
Perceived Trust (PT)		0,810	0.857
PT1	0.76		
PT2	0.78		
PT3	0.84		
PT4	0.81		
Attitude (ATU-D)		0.791	0.812
ATU-D1	0.94		
ATU-D2	0.85		
ATU-D3	0.62		
Intention (IN)		0.720	0.783
IN1	0.80		
IN2	0.78		
IN3	0.71		
Use of Dark Web (USE-D)		0.861	0.844
USE-D1	0.84		
USE-D2	0.82		
USE-D3	0.89		

The causal structure of the proposed research model was tested using SEM. The test showed a reasonable fit between the data and the proposed structural model. The fit statistics, RMSEA 0.10, SRMR 0.05, GFI 0.90, AGFI 0.90, and NFI 0.96, all indicate a good fit.

To determine the validity of the hypothesized paths, the statistical significance of all estimated structural parameters was examined. The estimates of the structural parameters and the results of the hypothesis testing are presented in Table 2.

Table 2. Lisrel results for the research model.

Hypothesis	Causal path	Path coefficient	t - value	Results
H1	PEU→PU	0.67	4.72	Supported
H2	PR→PU	0.43	2.81	Supported
H3	PT→ PU	0.55	3.58	Supported

 doi:10.20944/preprints202404.1156.v1

H4	PR→ ATU-D	0.48	3.02	Supported
H5	PT→ ATU-D	0,56	2.60	Supported
H6	PU→ ATU-D	0,61	4.25	Supported
H7	ATU-D→IU	0.40	2.52	Supported
H8	IU→ USE-D	0.81	7.02	Supported

The results related to the analysis of the structural model in Table 2, the structural relationships are shown in Figure 1, and conceptualized under four hypotheses are seen to be statistically significant. All hypotheses are verified, and that is used to evaluate the structural model is calculated as $\chi 2/df = 1.90$.

Table 2 confirms that hypothesis H1 ($\gamma = 0.67$; $t = 4.72$) is statistically supported, indicating a positive effect of PEU on PU.

Furthermore, hypothesis H2, which suggests a positive relationship between perceived risk and PU, was also statistically confirmed ($\gamma = 0.43$; $t = 2.81$).

Research hypothesis H3, which proposes a positive effect of perceived trust on PU, was also confirmed. The analysis revealed a statistically significant relationship between the two variables ($\gamma = 0.55$; $t = 3.58$).

Hypothesis H4, which posits that perceived risk positively affects attitude, was confirmed by the SEM analysis ($\gamma = 0.48$; $t = 3.02$).

Similarly, Hypothesis H5, which suggests that perceived trust positively affects attitude, was also confirmed by the SEM analysis ($\gamma = 0.56$; $t = 2.60$).

The SEM analysis confirmed Hypothesis H6 ($\beta = 0.61$; $t = 4.25$), which suggests that perceived usefulness positively affects attitude.

Hypothesis H7 ($\beta = 0.40$; $t = 2.52$) was also confirmed, indicating that individual attitudes positively affect usage intention.

Finally, Hypothesis H8 ($\beta = 0.81$; $t = 7.02$), which explains that intention to use affects behavior, was also accepted.

5. Conclusions

This study aims to discuss the behavior patterns of Dark Web users in a theoretical framework. For this purpose, the statistical accuracy of 8 hypotheses formed from 7 latent variables under the technology acceptance model was investigated. Based on the findings obtained from the study, it was decided that all causal relationships were statistically significant by validating the research hypotheses regarding the adoption of deep web usage. At the same time, the results obtained with the primary TAM model used in this study showed a significant agreement with other studies in the literature.

This study determined that PEU, PU, PR, PT, ATU-D, and IU latent variables have a statistically significant effect on USE-D. Also, users' beliefs that the Dark Web is accessible and valuable predict their positive attitudes toward using it.

In future research, the technology acceptance model used in this study can be extended by adding other external latent variables (system quality, information security, anxiety, etc.). Also, the reasons for deep web usage can be discussed in detail to determine the socio-psychological status of deep web users using different scales. Although the technology acceptance model has many uses in the literature, this study is the first to predict the level of technology acceptance of deep web users. The results showed that Dark Web users' attitudes and behaviors towards using the Dark Web can be explained using TAM.

Rapid developments in information and internet technologies have made the deep web widely available and popular. Although the deep web is the most essential part of the virtual world, we already have very little accurate and valid information about this world. Understanding the new world and its users and doing theoretical and practical studies are necessary. Only taking security preventions or seeing the whole deep web as the virtual face of the illegal activities world is seen as the biggest obstacle to being a part of this new world and trying to understand this new World.

 doi:10.20944/preprints202404.1156.v1

Dark Web users who step into the extreme world of freedoms continue to build a world where some new rules and beliefs are outside all social norms. With the rise of modern social networks, it is necessary to understand the attitudes, behaviors, and patterns of internet users on these social networks. Also, we predicted the sociological consequences of these networks in human relations and social structures by showing more academic effort.

Author Contributions: Conceptualization, S.Z. and H.E.Ç.; methodology, S.Z.; formal analysis, H.E.Ç.; writing—original draft preparation H.E.Ç.; writing—review and editing, S.Z. and H.E.Ç. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional **Review Board Statement:** Not applicable.

Informed **Consent Statement**: Informed consent was obtained from all subjects involved in the study.

Data **Availability Statement:** The data presented in this study are available on request from the corresponding author.

Conflicts **of Interest:** The authors declare no conflicts of interest.

References

1. Chaffey, D. Global Social Media Statistics Research Summary 2024. Available online: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (accessed on 10 September 2023).
2. UNODC, Digest of Cyber Organized Crime Second Edition; Vienna, 2021. Available online: https://www.unodc.org/documents/organized-crime/tools_and_publications/Digest_of_Cyber_Organized_Crime_2nd_edition_English.pdf (accessed on 10 September 2023).
3. Davis, S.; Arrigo, B. The Dark Web and Anonymizing Technologies: Legal Pitfalls, Ethical Prospects, and Policy Directions from Radical Criminology. Crime Law Soc Change 2021, 76, 367–386, doi:10.1007/s10611-021-09972-z.
4. Lederer, A.L.; Maupin, D.J.; Sena, M.P.; Zhuang, Y. Technology Acceptance Model and the World Wide Web. Decis Support Syst 2000, 29, 269–282, doi:10.1016/S0167-9236(00)00076-2.
5. Gundur, R.V.; Levi, M.; Topalli, V.; Ouellet, M.; Stolyarova, M.; Chang, L.Y.-C.; Mejía, D.D. Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. CrimRxiv 2021, doi:10.21428/cb6ab371.5f335e6f.
6. Shillito, M.R. Untangling the 'Dark Web': An Emerging Technological Challenge for the Criminal Law. Information and Communications Technology Law 2019, 28, 186–207, doi:10.1080/13600834.2019.1623449.
7. Okyere-Agyei, S. The Dark Web – A Review. Advances in Multidisciplinary and Scientific Research Journal Publication 2022, 1, 209–214, doi:10.22624/aims/crp-bk3-p34.
8. Upulie H.D.I; Prasanga, P.D.T. Dark Web, Its Impact on the Internet and the Society: A Review; 2021. Available online: https://uu.diva-portal.org/smash/get/diva2:1792762/FULLTEXT01.pdf (accessed on 10 September 2023).
9. Kaur, S.; Randhawa, S. Dark Web: A Web of Crimes. Wirel Pers Commun 2020, 112, 2131–2158, doi:10.1007/s11277-020-07143-2.
10. Chertoff, M. A Public Policy Perspective of the Dark Web. Journal of Cyber Policy 2017, 2, 26–38, doi:10.1080/23738871.2017.1298643.
11. Jin, P.; Kim, N.; Lee, S.; Jeong, D. Forensic Investigation of the Dark Web on the Tor Network: Pathway toward the Surface Web. Int J Inf Secur 2024, 23, 331–346, doi:10.1007/s10207-023-00745-4.
12. Sherman C.; Price G. The Invisible Web: Uncovering Sources Search Engines Can't See. Libr Trends 2003, 52, 282–298.
13. Król, K. Geoinformation in the Invisible Resources of the Internet. Geomatics, Landmanagement and Landscape 2019, 3, 53–66, doi:10.15576/gll/2019.3.53.
14. Beshiri, A.S.; Susuri, A. Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. Journal of Computer and Communications 2019, 07, 30–43, doi:10.4236/jcc.2019.73004.
15. Finklea, K. Dark Web. Congressional Research Service; 2017. Available online: https://sgp.fas.org/crs/misc/R44101.pdf (accessed on 15 July 2023).

16. Saleem, J.; Islam, R.; Kabir, M.A. The Anonymity of the Dark Web: A Survey. IEEE Access 2022, 10, 33628–33660, doi:10.1109/ACCESS.2022.3161547.
17. Pederson, S. Understanding the Deep Web in 10 MinUtes; 2013; Available online: https://img.deepweb-sites.com/wp-content/uploads/2015/11/deep-web-whitepaper-v3_for-approval.pdf (accessed on 20 July 2023).
18. Denic, N. V.; Devetak, S. Dark Web − As Challenge Of The Contemporary Information Age. Trames 2023, 27, 115–126, doi:10.3176/tr.2023.2.02.
19. Onyango S.; Steenvoorden E.; Scholten J.; Jansen S. Assessing the Health of the Dark Web:: An Analysis of Dark Web Open Source Software Projects. In; Gregory, P., Kruchten, P., Eds.; Lecture Notes in Business Information Processing; Springer International Publishing: Cham, 2021; Vol. 426, pp. 125–134 ISBN 978-3-030-88582-3.
20. Rudesill, Dakota S.; Caverlee, J.; Sui D. The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box 2015. Ohio State Public Law Working Paper No. 314, doi: 10.2139/ssrn.2676615.
21. Gollnick C., W.E. Separating Fact from Fiction: The Truth about the Dark Web; 2016; Available online: https://www.scribd.com/document/329783168/The-Truth-About-the-Dark-Web (accessed on 10 September 2023).
22. Gladyshev, P. Cybercrime as a Consequence of Unreasonable Expectations. IEEE Secur Priv 2019, 17, 84–87, doi:10.1109/MSEC.2019.2913772.
23. Dalins, J.; Wilson, C.; Carman, M. Criminal Motivation on the Dark Web: A Categorisation Model for Law Enforcement. Digit Investig 2018, 24, 62–71, doi:10.1016/j.diin.2017.12.003.
24. Balhara, A.; Ubba, S.; Sharma, Y.; Chawla, P. Exploring and Analyzing Dark Web. SSRN Electronic Journal 2021, doi:10.2139/ssrn.3879619.
25. Dingledine, R.; Mathewson, N.; Syverson, P. Tor: The Second-Generation Onion Router; Washington, 2004; Available online: https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.pdf (accessed on 10 September 2023).
26. Zantout, B.; Haraty, R. I2P Data Communication System. In Proceedings of the In Proceedings of ICN: the Tenth International Conference on Networks; Curran, January 2011; pp. 401–409.
27. Clarke, I.; Sandberg, O.; Wiley, B.; Hong, T.W. Freenet: A Distributed Anonymous Information Storage and Retrieval System. In Designing Privacy Enhancing Technologies; Federrath, H., Ed.; Springer, Berlin, Heidelberg: Berlin, Heidelberg, 2001; Vol. 2009, pp. 46–66.
28. Sanchez-Rola, I.; Balzarotti, D.; Santos, I. The Onions Have Eyes. In Proceedings of the 26th International Conference on World Wide Web; International World Wide Web Conferences Steering Committee: Republic and Canton of Geneva, Switzerland, April 3, 2017; pp. 1251–1260.
29. Hayes, D.; Cappa, F.; Cardon, J. A Framework for More Effective Dark Web Marketplace Investigations. Information 2018, 9, 186, doi:10.3390/info9080186.
30. Arora, M.; Kanjilal, U.; Varshney, D. An Intelligent Information Retrieval: A Social Network Analysis. International Journal of Web Based Communities 2012, 8, 213, doi:10.1504/IJWBC.2012.046263.
31. Ngo, V.M.; Gajula, R.; Thorpe, C.; Mckeever, S. Discovering Child Sexual Abuse Material Creators' Behaviors and Preferences on the Dark Web. Child Abuse Negl 2024, 147, doi:10.1016/j.chiabu.2023.106558.
32. Owen, G.; Savage, N. The Tor Dark Net, Global Commission on Internet Paper Series 20; Waterloo, Ontario, 2015;
33. Chertoff, M.; Simon, T. The Impact of the Dark Web on Internet Governance and Cyber Security; Waterloo, Ontario, 2015;
34. Greenberg, A. Hacker Lexicon: What Is the Dark Web, 2014. Available online: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (accessed on 10 October 2023).
35. Aceto, G.; Pescapé, A. Internet Censorship Detection: A Survey. Computer Networks 2015, 83, 381–421, doi:10.1016/j.comnet.2015.03.008.
36. Gupta, A.; Maynard, S.B.; Ahmad, A. The Dark Web Phenomenon: A Review and Research Agenda; 2019; In Australasian Conference on Information Systems. Perth, WA. Available online: https://arxiv.org/ftp/arxiv/papers/2104/2104.07138.pdf (accessed on 10 October 2023).
37. Ofusori, L.O.; Hendradi, R. Understanding the Impact of the Dark Web on Society: A Systematic Literature Review. International Journal of Information Science and Management 2023, 21, 1–21, doi:10.22034/ijism.2023.1978002.0/DOR.

 doi:10.20944/preprints202404.1156.v1

38. Negi, N. Comparison of Anonymous Communication Networks-Tor, I2P, Freenet. International Research Journal of Engineering and Technology 2017.
39. Jardine, E.; Lindner, A.M.; Owenson, G. The Potential Harms of the Tor Anonymity Network Cluster Disproportionately in Free Countries. Proc Natl Acad Sci U S A 2020, 117, 31716–31721, doi:10.1073/pnas.2011893117.
40. Dittus, M.; Wright, J.; Graham, M. Platform Criminalism: The "last-Mile" Geography of the Darknet Market Supply Chain. In Proceedings of the The Web Conference 2018 - Proceedings of the World Wide Web Conference, WWW 2018; Association for Computing Machinery, Inc, April 10 2018; pp. 277–286.
41. Ebrahimi, M.; Chai, Y.; Samtani, S.; Chen, H. Cross-Lingual Cybersecurity Analytics in the International Dark Web with Adversarial Deep Representation Learning. MIS Q 2022, 46, 1209–1226, doi:10.25300/MISQ/2022/16618.
42. Broséus, J.; Rhumorbarbe, D.; Morelato, M.; Staehli, L.; Rossy, Q. A Geographical Analysis of Trafficking on a Popular Darknet Market. Forensic Sci Int 2017, 277, 88–102, doi:10.1016/j.forsciint.2017.05.021.
43. Jardine, E. Privacy, Censorship, Data Breaches and Internet Freedom: The Drivers of Support and Opposition to Dark Web Technologies. New Media Soc 2018, 20, 2824–2843, doi:10.1177/1461444817733134.
44. Domenic, M. Dark Web Facts Revealed: Myths and Stats About the Secret Web Available online: https://www.avast.com/c-dark-web-facts (accessed on 10 December 2023).
45. Davis, F.D. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly 1989, 13, 319, doi:10.2307/249008.
46. Davis, F.D.; Bagozzi, R.P.; Warshaw, P.R. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Manage Sci 1989, 35, 982–1003, doi:10.1287/mnsc.35.8.982.
47. Davis, F.D.; Venkatesh, V. A Critical Assessment of Potential Measurement Biases in the Technology Acceptance Model: Three Experiments. Int J Hum Comput Stud 1996, 45, 19–45, doi:10.1006/ijhc.1996.0040.
48. Mathieson, K. Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. Information Systems Research 1991, 2, 173–191, doi:10.1287/isre.2.3.173.
49. Moon, J.-W.; Kim, Y.-G. Extending the TAM for a World-Wide-Web Context. Information & Management 2001, 38, 217–230, doi:10.1016/S0378-7206(00)00061-6.
50. Taylor, S.; Todd, P.A. Understanding Information Technology Usage: A Test of Competing Models. Information Systems Research 1995, 6, 144–176, doi:10.1287/isre.6.2.144.
51. Venkatesh, V. Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model. Information Systems Research 2000, 11, 342–365, doi:10.1287/isre.11.4.342.11872.
52. Buabeng-Andoh, C. Predicting Students' Intention to Adopt Mobile Learning. Journal of Research in Innovative Teaching & Learning 2018, 11, 178–191, doi:10.1108/JRIT-03-2017-0004.
53. Çelik Eray, H.; Yılmaz, V. Extending the Technology Acceptance Model for Adoption of E-Shopping. Journal of Electronic Commerce Research 2011, 12, 152–164.
54. Kelly, A.E.; Palaniappan, S. Using a Technology Acceptance Model to Determine Factors Influencing Continued Usage of Mobile Money Service Transactions in Ghana. J Innov Entrep 2023, 12, doi:10.1186/s13731-023-00301-3.
55. Gefen, D. E-Commerce: The Role of Familiarity and Trust. Omega (Westport) 2000, 28, 725–737, doi:10.1016/S0305-0483(00)00021-9.
56. Featherman, M.S.; Pavlou, P.A. Predicting E-Services Adoption: A Perceived Risk Facets Perspective. Int J Hum Comput Stud 2003, 59, 451–474, doi:10.1016/S1071-5819(03)00111-3.
57. Nadillah, H.P.; Saputri, S.A.; Meiryani Behavioral Intention to Use E-Tax Systems: An Application of Technology Acceptance Model and Perceived Risk. In Proceedings of the 2023 International Conference on Digital Applications, Transformation and Economy, ICDATE 2023; Institute of Electrical and Electronics Engineers Inc., 2023.
58. Hassan, H.E.; Wood, V.R. Does Country Culture Influence Consumers' Perceptions Toward Mobile Banking? A Comparison between Egypt and the United States. Telematics and Informatics 2020, 46, 101312, doi:10.1016/j.tele.2019.101312.
59. Ajzen, I. The Theory of Planned Behavior. Organ Behav Hum Decis Process 1991, 50, 179–211, doi:10.1016/0749-5978(91)90020-T.

 doi:10.20944/preprints202404.1156.v1

60. Cunningham, S.M. The Major Dimensions of Perceived Risk. In Risk Taking and Information Handling in Consumer Behavior; Graduate School of Business Administration, Harvard University Press: Boston, MA, 1967; pp. 82–108.
61. Bellman, S.; Lohse, G.L.; Johnson, E.J. Predictors of Online Buying Behavior. Commun ACM 1999, 42, 32–38, doi:10.1145/322796.322805.
62. Grewal, D.; Gotlieb, J.; Marmorstein, H. The Moderating Effects of Message Framing and Source Credibility on the Price-Perceived Risk Relationship. Journal of Consumer Research 1994, 21, 145, doi:10.1086/209388.
63. Mitchell, V.W. Understanding Consumers' Behaviour: Can Perceived Risk Theory Help? Management Decision 1992, 30, 26–31, doi:10.1108/00251749210013050.
64. Mutahar, A.M.; Aldholay, A.; Isaac, O.; Jalal, A.N.; Kamaruddin, F.E.B. The Moderating Role of Perceived Risk in the Technology Acceptance Model (TAM): The Context of Mobile Banking in Developing Countries. In Proceedings of the Lecture Notes in Networks and Systems; Springer Science and Business Media Deutschland GmbH, 2022; Vol. 299, pp. 389–403.
65. Gerrard, P.; Barton Cunningham, J.; Devlin, J.F. Why Consumers Are Not Using Internet Banking: A Qualitative Study. Journal of Services Marketing 2006, 20, 160–168, doi:10.1108/08876040610665616.
66. Oly Ndubisi, N.; Jantan, M. Evaluating IS Usage in Malaysian Small and Medium-sized Firms Using the Technology Acceptance Model. Logistics Information Management 2003, 16, 440–450, doi:10.1108/09576050310503411.
67. Nor, K.M.; Pearson, J.M. An Exploratory Study into the Adoption of Internet Banking in a Developing Country: Malaysia. Journal of Internet Commerce 2008, 7, 29–73, doi:10.1080/15332860802004162.
68. Polasik, M.; Wisniewski, T.P. Empirical Analysis of Internet Banking Adoption in Poland. International Journal of Bank Marketing 2009, 27, 32–52, doi:10.1108/02652320910928227.
69. Kesharwani, A.; Bisht, S.S. The Impact of Trust and Perceived Risk on Internet Banking Adoption in India: An Extension of Technology Acceptance Model. International Journal of Bank Marketing 2012, 30, 303–322, doi:10.1108/02652321211236923.
70. Shih, H.P. An Empirical Study on Predicting User Acceptance of E-Shopping on the Web. Information and Management 2004, 41, 351–368, doi:10.1016/S0378-7206(03)00079-X.
71. Read, W.; Robertson, N.; McQuilken, L. A Novel Romance: The Technology Acceptance Model with Emotional Attachment. Australasian Marketing Journal 2011, 19, 223–229, doi:10.1016/j.ausmj.2011.07.004.
72. Teo, T. Factors Influencing Teachers' Intention to Use Technology: Model Development and Test. Comput Educ 2011, 57, 2432–2440, doi:10.1016/j.compedu.2011.06.008.
73. Teo, T. A Case for Using Structural Equation Modelling (SEM) in Educational Technology Research: Colloquium. British Journal of Educational Technology 2010, 41, doi:10.1111/j.1467-8535.2009.00999.x.
74. Byrne, B.M. Structural Equation Modeling with EQS: Basic Concepts, Applications, and Programming, Second Edition; Routledge, 2013; ISBN 9780203726532.
75. Reisinger, Y.; Turner, L. Structural Equation Modeling with Lisrel: Application in Tourism. Tour Manag 1999, 20, 71–88, doi:10.1016/S0261-5177(98)00104-6.