The Antecedents and Consequences of Legitimate Corporate Participation in the DarkNet: A Preliminary Model

David Kenny
Dublin City University
david.kenny@dcu.ie

Grace Fox
Dublin City University
grace.fox@dcu.ie

Gary Sinclair
Dublin City University
gary.sinclair@dcu.ie

Theo Lynn
Dublin City University
theo.lynn@dcu.ie

Abstract

The DarkNet is a purposefully hidden collection of disconnected web sites that are not indexed by conventional or mainstream search engines, are not accessible by conventional means, and requires specialised software, specific knowledge, and authorisation to gain access. While typically associated with illegality and criminality, there are an increasing number of legitimate organizations active on the DarkNet. While explored widely in Computer Science, Humanities and Social Science, Engineering and Medicine, there is a paucity of research in the business and IS disciplines. The objective of this paper is to introduce the DarkNet and DarkNet Commerce, summarise extant business and IS research, albeit limited, and outline a proposed model to explore a previously unexplored relationship in the business and IS literature, namely the antecedents and consequences of the participation of legitimate organisations on the DarkNet.

1. Introduction

Since its public release in 1993, the World Wide Web ('the Web') has grown to be the commercial, social and informational hub of modern global society. The Web comprises approximately 1.7 billion websites including business and personal websites, blogs, web applications, e-commerce websites and social networking sites [1, 2]. There are approximately 4.1 billion active Internet users [3]. Internet users and online consumers are increasingly concerned about their online privacy [4], and reject the common practice of online tracking and the data capture/harvest/exploitation practices of traditional Internet companies on the mainstream web or 'ClearNet' [5]. Consequently, there is growth in the demand for hidden Internet services, private networks and the so-called 'DarkNet' [6, 7, 8, 9].

Long associated with illegality and criminality, the DarkNet has been a source of interest for researchers in different domains including computer science, social sciences, engineering and medicine [10]. The DarkNet is defined as a purposefully hidden collection of disconnected web sites that are not indexed by conventional or mainstream search engines, is not accessible by conventional means, and requires specialised software, specific knowledge, and authorisation to gain access. The DarkNet is made up of a variety of separate and distinct systems: Freenet, Tor, I2P, ZeroNet and GNUnet [11, 12]. Each of these represent 'specialised software' configured to hide and anonymize potentially identifiable information such as a user's IP address. It is anonymity, provided both to publishers of DarkNet sites, and visitors to DarkNet sites alike, that is perhaps the singular reason for the growth and popularity of the DarkNet [7, 9]. This is reflected in the increasing usage of the Tor browser [7, 13]. There are an estimated 200,000 Tor DarkNet sites in operation [13], an increase from 65,000 in 2019 [14]. Tor [13] estimates that two million people use their software clients every day, and recent industry research suggests that up to 33% of Internet users in North America have accessed the DarkNet [15]. Since 2014, an increasing number of legitimate organisations, both commercial and non-commercial, have launched a presence on the DarkNet (see Table 1).

Why do legitimate organisations participate in the DarkNet? What is the business case for investment in DarkNet activities? While the literature with respect to the ClearNet is extensive and well-established, this is not the case with the DarkNet. In response to called for further research into the DarkNet [16, 17], the present paper aims to surface significant themes in extant literature in the business, management, accounting and IS fields and set the stage for future research. We find that while current literature on the DarkNet has explored some relevant topics (i) privacy [5, 10], (ii) cybersecurity [18, 16], (iii) drug research [19] and (iv) the study of cybercriminal communities, [16, 20] (particularly DarkNet marketplaces), no research to this point has considered how the unique

URI: https://hdl.handle.net/10125/71193
978-0-9981331-4-0

Table 1. Examples of Legitimate Organisations using the DarkNet

Industry	Organisation	Activity
News and Media	BBC	
	Deutsche Welle	DarkNet News Site; SecureDrop Service for Whistleblowers
Professional Services	decoded:Legal	DarkNet legal services
Education	BBC Learning	Multimedia English language learning resources
Advertising	Ahmia	DarkNet search engine
ICT	NORD VPN	Tor over VPN (Virtual Private Network)
	Facebook	DarkNet version of Facebook with enhanced anonymity for Tor users.
	ProtonMail	Tor-encrypted Email
	Whonix	Anonymity- and Security-focused Linux Operating Systems
	DuckDuckGo	Anonymous Search Engine
	Tor	Encrypted Browser
	Ablative Hosting	Multi-hop Tor Service Hosting
	TapIIN	Tor-based social networking site
Government	US Central Intelligence Agency	DarkNet version of website and intelligence gathering service
	Dutch National Prosecution Service	Community engagement and enforcement promotion

characteristics of this new context shapes legitimate corporate participation in the DarkNet. The DarkNet is not merely a technology *per se* but rather the culmination of social, political and technological trends. As such, we find that concepts from technology innovation adoption, dynamic capabilities, as well as corporate socio-political engagement [21, 22, 23, 24] are useful for exploring organisational decision making regarding DarkNet activities. To this end, we propose and discuss a multi-level theoretical model to explore the (a) antecedents and (b) consequences of legitimate corporate participation on the DarkNet that can inform future avenues of research.

The remainder of this paper is structured as follows. The next section presents a summary of extant business and IS research on the DarkNet. Section 3 proposes a multi-level model to explore a previously unexplored relationship in the business and IS literature, the antecedents and consequences of the participation of legitimate firms in the DarkNet.

2. Literature Review

DarkNet research has been explored in a variety of domains. An initial analysis limited to peer-reviewed journal articles in Scopus between 2001 and 2020 revealed the majority of extant research is in four disciplines. Computer Science, Humanities and Social Science, Engineering and Medicine count for 80% of all publications; only 31 articles were identified in the Business, Management and Accounting (BMA) category (4%) (See Table 2). Common topics of interest include cybersecurity and privacy, criminology, and public health [10]. Within the BMA and IS category, several of these articles make only ancillary reference to the 'dark web' [25, 26] and 'DarkNet' [27]; they are not the focal topic of discussion in the papers.

The dominant theme of scholarly research on the DarkNet, in all disciplines, relates to the illicit nature of its use and the study of cybercriminal communities, particularly DarkNet marketplaces [16, 8]. Much of the discussion centers on the infamous, and now defunct, Silk Road marketplace [28, 29, 30]. The DarkNet is perceived as a threat to the business community primarily because sensitive corporate information stolen through security breaches is often later sold on DarkNet markets [11]. For society at large, its dependence on ICT for critical infrastructure leaves it prone to an increasing number of "cyber attacks committed by criminals operating from the DarkNet" [16]. Accordingly, DarkNet research (in particular, cyber-threat intelligence research) is considered to be of critical importance and relevance due to the potential for "large-scale disruption of business operations and continuity" emanating and/or coordinated from the DarkNet [31]. Of the articles we identified in the BMA discipline, only four articles published in the IS Senior Scholars' 'Basket of Eight' leading IS journals refer to the DarkNet or synonyms, and of those, only two discuss it in any meaningful way - one methodology paper [31] and one privacy paper [32]. The remaining papers focus on similar topics to these and other disciplines i.e. privacy, cybersecurity, and drug research. Only one article on the participation of legitimate organisations on the DarkNet was identified. Brooke [9] cites the cases of Adland and ProPublica, two firms that established a DarkNet presence in response to consumers' increasing use of ad blocking technologies when accessing their websites. In response to more 'privacy attuned' users, Adland refined its business model from one primarily dependent on ad revenue to a donation-based model, accepting contributions on the DarkNet using PayPal and Bitcoin. This study while perhaps lacking in

theoretical contribution and empirical testing, made a practical contribution to the literature. Notably and unsurprisingly, in a Special Issue of the Journal of the Academy of Marketing Science on the future of technology and marketing, Grewal et al. [17] call for research on the DarkNet, identifying it as a significant and important topic of research.

The media and scholarly work primarily focuses on cryptomarkets. These are digital black markets for illegal and illicit products and services e.g. drugs, false identities, pornography, counterfeit money etc. [10]. While topical and newsworthy, it would be wrong to generalise that all activity and usage of the DarkNet is, or that its users perceive it as, inherently criminogenic [33]. While DarkNet Commerce is referenced in the literature (for example, see [34]), it remains undefined. We define DarkNet Commerce as a form of commerce mediated by the DarkNet. It allows actors to participate actively in the marketing, selling, and consumption of products and services in online marketplaces and communities while leveraging the security and anonymity of DarkNet technologies. As discussed, the anonymity and security of communications is a key and differentiating factor in DarkNet commerce. This impacts all aspects of online commerce from design to delivery. For example, to mitigate against security vulnerabilities, DarkNet browsers, such as Tor, disable automatic image and JavaScript loading, as well as other functionality. Payment is often via cryptocurrencies such as BitCoin, and delivery to anonymous delivery points. Due to the multi-hop nature of DarkNet hosting, DarkNet search engines are not as advanced as those in the ClearNet and as a result many users rely on directories. Data-driven marketing and advertising is practically infeasible. Despite these challenges, legitimate organisations are active on the DarkNet. As discussed earlier, Adland and ProPublica established presences on the DarkNet in response to a shift in consumer attitudes towards privacy and against both media and mass surveillance, in particular [9, 10]. Similarly, albeit anecdotally, this would seem to be a motivation for other organisations' use of the DarkNet e.g. Facebook [35].

Clearly, a wide range of companies have legitimate products and services that DarkNet users would be interested in their generic form, for example VPNs, or a version of those products and services designed specifically for the DarkNet. However, the sales of products and services are not the only motivation for using the DarkNet for legitimate business purposes. Other research suggests public health organisations use the DarkNet to anticipate pharmacological trends and misuse in an attempt to anticipate treatment [36]. Similarly, some organisations monitor the DarkNet to identify emerging cybersecurity threats or existing breaches or vulnerabilities as a risk mitigation strategy, or in the case of IT security companies, input for new products and services [20].

Table 2. Frequency Distribution of Articles by Academic Discipline

Discipline	# of Articles	% of Articles
Computer Science	244	33%
Arts and Humanities, Social Sciences	173	23%
Engineering	80	11%
Medicine, Health and related	78	11%
Physical, Chemical, Agricultural Sciences	51	7%
Business, Management and Accounting (BMA)	31	4%
Mathematics	24	3%
IS	23	3%
Economics, Econometrics and Finance	21	3%
Decision Sciences	15	2%
Total	740	-

Research also suggests that the DarkNet is used extensively by activists, media organisations, and for whistle blowing [33]. While some news and media organisations have DarkNet versions of their services e.g. Deutsche Welle and BBC News, much more have SecureDrop services on the DarkNet for whistleblowers to share confidential information [37] (See Table 4).

Table 3. Business, Management and Accounting and Information Systems articles referencing the DarkNet

Title	Authors	Journal (Publication)	Year
Metrics for characterizing the form of security policies	Goel & Chengalur-Smith[25]	Journal of Strategic Information Systems	2010
A marketer's guide to the dark web	Brooke[9]	Marketing Research	2016
Special Section Introduction: Ubiquitous IT and Digital Vulnerabilities	Ransbotham et al.[27]	Information systems research	2016
Digital marketing: A framework, review and research agenda	Kannan[38] & Li	International Journal of Research in Marketing	2017
Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA	Posey et al.[32]	European Journal of Information Systems	2017
The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments	Broadhead[20]	Computer Law and Security Review	2018
Cryptocurrencies and Business Ethics	Dierksmeier & Seele[39]	Journal of Business Ethics	2018
Scamming and the reputation of drug dealers on Darknet Markets	Espinosa[19]	International Journal of Industrial Organization	2019
Child pornography websites on the darknet	Lee[12]	International Journal of Recent Technology and Engineering	2019
The not so dark side of the darknet: a qualitative study	Mirea et al.[33]	Security Journal	2019
DICE-E: A framework for conducting Darknet identification, collection, evaluation with ethics	Benjamin et al.[16]	MIS Quarterly: Management Information Systems	2019
The dark web and digital currencies: A potent money laundering and terrorism opportunity	Rubasundram[40]	International Journal of Recent Technology and Engineering	2019
Casting the dark web in a new light	Huang et al.[41]	MIT Sloan Management Review	2019
The Digital and Physical Footprint of Dark Net Markets	Thomaz[5]	Journal of International Marketing	2020
Learning from the Dark Web: leveraging conversational agents in the era of hyper-privacy to enhance marketing	Thomaz et al.[10]	Journal of the Academy of Marketing Science	2020
The future of technology and marketing: a multidisciplinary perspective	Grewal et al.[17]	Journal of the Academy of Marketing Science	2020
A systematic review of the dark side of CRM: the need for a new research agenda	Nguyen et al.[26]	Journal of Strategic Marketing	2020

Table 4. Examples of International Organizations using SecureDrop

Organization Type	Example Organizations
NGO	Lucy Parsons Labs (USA) Greenpeace (New Zealand) Wikileaks (UK)
Higher Education	Harvard University (USA)
News/ Media	ABC (Australia) Al-Jazeera (Qatar) Aftonbladet (Sweden) CBC (Canada Dagbladet (Norway) New York Times (USA) NPR (USA) Süddeutsche Zeitung (Germany) The Guardian (UK)

While not specifically targeting legitimate business research outlets, or examined through the lens of business theories, extant research can both inform ClearNet theory and practice but also how legitimate organisations might use the DarkNet for a variety of legitimate business activities. Such activities include market intelligence, customer support, reputation and trust building in anonymous and pseudonymous markets [42, 31, 43, 39, 19]. In his empirical analysis of the DarkNet drug trade, Thomaz [5] suggests that the operational nature of illegal enterprises on the DarkNet mirrors that of legitimate organisations, and that these criminal organisations face the same issues: segmentation and targeting processes; buyer behaviour; the four Ps (pricing, product (quality), promotion, place (distribution)); and sales processes. In the same way, might legitimate organisations learn from those trading on and using the DarkNet?

While we can posit why legitimate organisations might establish a presence on the DarkNet, there does not seem to be empirical evidence to support any such claims or the consequences of such decisions for the organisation. From an academic perspective, the idiosyncrasies of the DarkNet pose interesting questions, not least whether extant theory needs to be revalidated or renovated against the context of the DarkNet.

3. Towards a Preliminary Model

The extant business and IS literature on the DarkNet focuses nearly exclusively on criminogenic behaviour and on privacy and security issues. While these are important aspects for understanding activities and behaviour on the DarkNet, extant research provides little insight in to why legitimate organisations might participate on the DarkNet, how they arrived at the decision to participate, and what the consequences of that participation might be, positive or negative. Figure 1 presents an initial multi-level model for exploring the antecedents and consequences of participation by legitimate organisations on the DarkNet.

3.1. Antecedents

To reflect that the DarkNet is both a technology and socio-political concept, we adopt a multi-level approach to antecedents consistent with extant literature on technology adoption and dynamic capabilities [21, 22]. This allows an exploration of where the antecedents to DarkNet participation are situated e.g. within one focal level of analysis, at the intersection of one or more levels of analysis, or across multiple levels of analysis. Such analysis overcomes issues with unifocal analysis and allows greater exploration of the relative importance and relationship between different antecedents, mechanisms and levels [22].

3.1.1. DarkNet Level The DarkNet is chiefly known for its cryptomarkets, online marketplaces that facilitate the sale and distribution of illicit products and services [5]. Between January - April 2014, the top vendors on the Silk Road 2.0 marketplace had an estimated turnover of between US$140,596 - US$6.9m [44]. While the number of active DarkNet markets fluctuates, there were approximately 49 active markets in 2019 [45]. Total DarkNet market sales have grown year on year, with 70 per cent growth in 2019 to a total value of over $790 million in cryptocurrency [45]. Not all of the activity and communities on the DarkNet are of a criminal or commercial nature [7]. As discussed earlier, some companies have established a presence on the DarkNet in response to perceived demand from their existing customer base [9]. The DarkNet represents a new market. In addition to serving existing customers on the DarkNet, new entrants to an evolving market can create further demand for a given product or service [46]. The DarkNet may represent a greenfield market for an organisation with no or less intense competition than on the ClearNet. This lack of competition or intense rivalry may attract participation.

Proposition 1: *The presence of incumbent target customers on the DarkNet will stimulate participation in the DarkNet.*

Proposition 2: *The levels of competition for the firm's products and services on the DarkNet will*

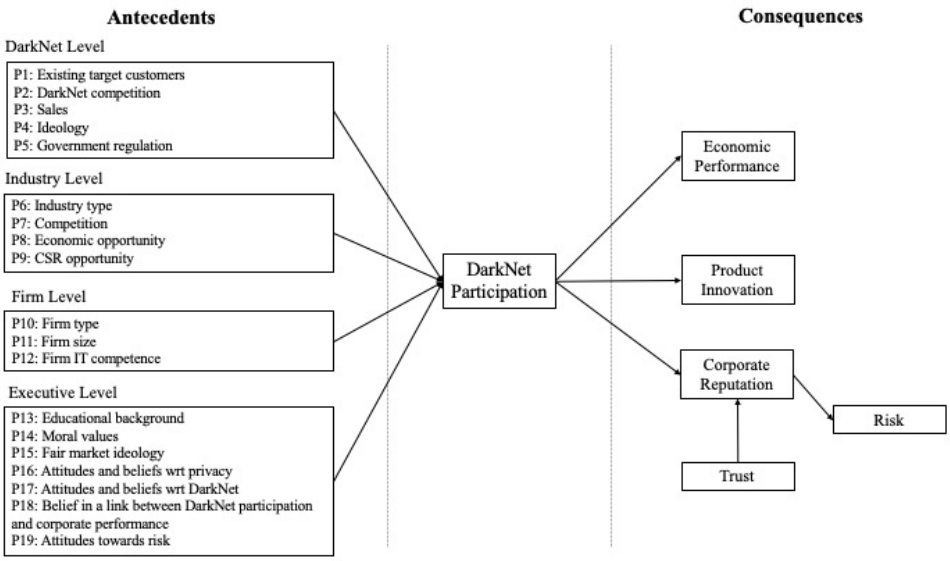

Figure 1. General model of the antecedents and consequences of DarkNet participation

stimulate participation in the DarkNet.

Proposition 3: *The level of firm sales to DarkNet user audiences is positively related to participation on the DarkNet.*

If the number of customers or the raw dollar amount of sales is potentially significant, this will attract participation. As presented earlier, there is anecdotal evidence of firms responding in an ideologically sympathetic manner in recognition of customer preferences for greater anonymity and privacy by shifting their business model [9]. Similarly, the need to avoid state and government detection (and in some cases persecution) also extends to civilian DarkNet users in certain regions of the world who are engaging in ethical behaviour and seek to circumvent censorship and maintain anonymity online [18, 47]. In recognition of this, some civil society/community and news and media organisations have established a presence on the DarkNet. Perhaps reciprocally, DarkNet users have rewarded this behaviour by supporting the business interests of the firm [9].

Proposition 4: *The presence of DarkNet users ideologically sympathetic to the firm's business interests is positively related to participation in the DarkNet.*

Proposition 5: *Higher levels of government regulation is positively related to participation in the DarkNet.*

3.1.2. Industry Level Organisations in different industries use the DarkNet including education, news and media professional services, ICT (both general use (e.g. Facebook) and DarkNet specific (e.g. Tor)), government, and non-government organisations (see Table 1). Even cursory analysis suggests both market and non-market motivations for participation on the DarkNet. In addition, the product(service)-market fit and the opportunity to exploit will vary by sector. For example, many news organisations have established a dedicated DarkNet mirror of their ClearNet websites to provide regular news and information to regions with state-mandated media censorship, and SecureDrop services to allow whistleblowers to share confidential content. This is often done as a form of corporate social responsibility. In contrast, there are a wide range of examples in the ICT sector where firms seek revenue generation opportunities through TOR-based services, cryptocurrencies, VPNs etc. Existing competitors in the ClearNet may already be active in the DarkNet thus stimulating interest and participation, a fear of missing out, so to speak. This might explain the large number of news and media firms using SecureDrop.

Proposition 6: *Participation on the DarkNet will differ based on industry type.*

Proposition 7: *The presence of existing competitors on the DarkNet is positively related to participation on the DarkNet.*

Proposition 8: *The level of economic opportunity on the DarkNet is positively related to participation on the DarkNet.*

Proposition 9: *The level of CSR in an industry is positively related to participation on the DarkNet*

3.1.3. Firm Level Clearly, there are firm-level factors that influence participation in the DarkNet. Firmographic data including geographic origin, profit motivations (for profit or not for profit) and firm size may provide insights into the decision to participate on the DarkNet. Use of the DarkNet may be more prevalent where there is more state control of media, the Internet, or commerce. As such, firm country of origin or target market may provide insights on adoption. Relatedly, organisations may participate on the DarkNet for non-market reasons. As such, profit, or non-profit motivation, is clearly a differentiating factor. Technological advancements and globalisation raise questions about the applicability of previously reported relationships between organisation size and measures of firm performance [48]. The role of firm size in DarkNet adoption may also be worthy of exploration.

Proposition 10: *Participation on the DarkNet will differ based on firm type.*

Proposition 11: *Firm size is positively related to participation on the DarkNet.*

With the exception of cryptomarkets, DarkNet sites can be used for the same purposes as ClearNet websites: e-commerce, social networking, file sharing, and discussion forums. It stands to reason that DarkNet sites are built using the same web technologies as ClearNet websites: HTML, CSS, client/server-side scripting languages (e.g. JavaScript) and hosting software [11]. While website attacks are prevalent and commonly occur on both the ClearNet and DarkNet, DarkNet hosting companies can be particularly vulnerable to the constant threat of attacks [49]. In light of this, organisations participating on the DarkNet may self-host their site. Furthermore, individual employees may open themselves up to personal attacks and therefore a greater degree of operational security awareness. This requires a level of organisational and individual IT competence, or perhaps more specifically, IT security competence. As such, it is reasonable to suggest that the level of IT competence and IT security competence would seem to be worth exploring as a determinant for participation on the DarkNet.

Proposition 12: *Firm IT competence is positively related to participation on the DarkNet.*

3.1.4. Executive Level In addition to industry and environmental conditions, the decision making of executives and managers are strong determinants of organisational process [50]. We posit that the decision to participate in the DarkNet will depend on two independent factors - the business case for participation in the DarkNet, and the executive's own personal value system. As in corporate social responsibility research, system justification theory (SJT) and fair market ideology may also help explain executive decision making to participate in the DarkNet [24]. The former explores how individuals rationalise the status quo in general, while the latter focuses specifically on how individuals justify their participation and support for the market economy system specifically [24]. In SJT, it is argued that individuals either accept the status quo and justify the system by idealizing it somehow, or seek to change the system [51]. As the modern DarkNet emerged as a reaction to constraints put in place around certain behaviours in society, SJT would seem to be a particularly relevant lens. Similarly, proponents of the fair market ideology will seek to justify and defend their right to pursue activities that generate economic value as both fair and legitimate, possibly overemphasising favorable economic expectations, and underemphasizing any potential adverse impacts or ethical concerns [52]. Given the public perception of the DarkNet as a less legitimate medium in which to conduct business, and the risks associated with DarkNet participation, the sponsoring executive's individual attitudes, beliefs, and values surrounding participation in the DarkNet is worthy of exploration. As anonymity and privacy play a central role in the DarkNet, an executive's attitudes and beliefs with regards to privacy and the relationship between participation on the DarkNet and the potential for economic gains (corporate performance) would seem to be pertinent. We also include educational background as it can serve as a proxy for fair market ideology [24].

Proposition 13: *There is a positive effect of educational background in computer science, business, economics, and law on the belief in the business case for participation in the DarkNet.*

Proposition14: *There is a negative effect of moral values on the belief in the business case for participation in the DarkNet.*

Proposition 15: *The higher individuals score on fair market ideology, the more strongly they believe in the business case for participation in the DarkNet.*

Proposition 16: *There is a positive effect of beliefs and attitudes regarding privacy on the belief in the business case for participation in the DarkNet.*

Proposition 17: *There is a positive effect of technology specific beliefs and technology specific attitudes regarding participation in the DarkNet.*

Proposition 18: *There is a positive effect of beliefs regarding participation in the DarkNet on corporate performance.*

Proposition 19: *The higher the propensity for risk taking, the more strongly they believe in the business*

case for participation in the DarkNet.

3.2. Consequences

As discussed above, participation in the DarkNet may be driven by a variety of motivations. We posit that DarkNet participation will affect firm performance in a variety of ways. Firstly, the DarkNet may open up a new channel to service existing markets. For digital product or service providers, the DarkNet may represent just another online marketplace but one where the market values anonymity or products and services that enable or enhance this anonymity or complement their worldview such as VPN providers, ProtonMail or DuckDuckGo. For others, it may open up new markets as suggested by the cases of Adland and ProPublica [9]. At the same time, a significant shift in use of the DarkNet, however improbable, also represents a threat to firm performance. For example, in July 2017, Goldman Sachs Internet analyst, Heath Terry, suggested that the DarkNet was a potentially disruptive risk to search engine providers and data-driven advertising companies [53]. Firms may also participate on the DarkNet motivated by product or service innovation. Already, firms are exploring new products or service behaviours, uses, functionality and features. Facebook not only serve existing markets through the DarkNet but have used the DarkNet to innovate how their core platform scales and operates in such constrained environments so that they provide their .onion users with a more secure experience and protecting user data against attacks by malicious third parties controlling nodes in the Tor network [54].

We also posit that firms may participate on the DarkNet motivated by corporate reputation or corporate social responsibility. Authors have suggested that privacy orientation and management can be viewed both as a corporate social responsibility [55] and a means to enhance or diminish corporate reputations [56]. This is most evident in the media and its treatment of confidential sources and the numerous media outlets and NGOs both on the DarkNet generally, and using SecureDrop specifically, provides supporting evidence to this end. It is not unreasonable to think that while some firms may participate on the DarkNet for purely commercial gain, others may participate for purely altruistic purposes. There is well established literature on the positive role of corporate reputation on firm performance [57, 58] however the link between CSR and positive firm performance is less clear. While there are numerous studies suggesting a positive association between CSR and both firm performance [59, 60] and corporate reputation [61, 62], there are also analyses that suggest no impact or negative impacts on firm performance [63, 64]. The impact of DarkNet participation on corporate reputation has not been explored in the literature.

Trust is defined as a willingness to accept vulnerability based on positive expectations of another party [65]. Trustor perceptions of benevolence, integrity and competence are key determinants of trust [66]. Given the nature of the DarkNet, participation may result in either a greater perceived trustworthiness by extant DarkNet users while contrarily perceived distrust by ClearNet users or vice-versa. As such, the impact of the aforementioned antecedents on firm-level trust and the impact of such perceptions on corporate reputation is worthy of exploration. In contrast, participation on the DarkNet may increase the perceived risk of working with the organisation.

4. Conclusion

Within the past year, two high impact scholarly publications have called for further research into the DarkNet [16, 17]. This paper introduced and defined the DarkNet and DarkNet Commerce. We highlight that contrary to mainstream and popular opinion, the DarkNet is not inherently criminogenic. We reviewed the limited literature in business, management, and IS, and presented a model for exploring the antecedents and consequences of DarkNet participation by legitimate organizations. As well as contributing to scholarly knowledge and theory, understanding the determinants for DarkNet research and potential outcomes should reveal practical insights and implications for organisations regarding their participation on the DarkNet. This includes (a) the business case for DarkNet participation; (b) a decision making process for exploring DarkNet participation; and (c) an understanding of DarkNet market dynamics and market orientation. From an academic perspective, the dearth of business and IS research combined with the idiosyncrasies of the DarkNet pose interesting questions in the context of theory development, and asks whether some extant theory can be applied to, re-examined, or renovated against the context of the DarkNet. Notwithstanding this, DarkNet research presents significant challenges, not least the lack of extant research to draw upon and expand. In this sense, a limitation of this paper and the proposed model is the limited literature it draws upon. Furthermore, the technical configuration of the DarkNet coupled with its culture of anonymity makes empirical data collection difficult [16]. It also poses both ethical and researcher safety challenges [8, 11, 16]. As such, it requires careful planning and consideration.

References

[1] M. Armstrong, "How many websites are there?." https://www.statista.com/chart/19058/how-many-websites-are-there/, 2019.

[2] Internet Live Stats, "Total number of websites 2020." https://www.internetlivestats.com/total-number-of-websites/, 2020.

[3] International Telecommunication Union, "Statistics." https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, 2020.

[4] CIGI-Ipsos, "2019 cigi-ipsos global survey on internet security and trust," Jun 2019.

[5] F. Thomaz, "The digital and physical footprint of dark net markets," *Journal of International Marketing*, vol. 28, no. 1, pp. 66–80, 2020.

[6] M. J. Barratt, S. Lenton, and M. Allen, "Internet content regulation, public drug websites and the growth in hidden internet services," *Drugs: education, prevention and policy*, vol. 20, no. 3, pp. 195–202, 2013.

[7] R. W. Gehl, "Power/freedom on the dark web: A digital ethnography of the dark web social network," *New Media & Society*, vol. 18, no. 7, pp. 1219–1235, 2016.

[8] M. J. Barratt and A. Maddox, "Active engagement with stigmatised communities through digital ethnography," *Qualitative research*, vol. 16, no. 6, pp. 701–719, 2016.

[9] Z. Brooke, "A marketer's guide to the dark web," *Marketing Research*, vol. 28, no. 1, pp. 22–7, 2016.

[10] F. Thomaz, C. Salge, E. Karahanna, and J. Hulland, "Learning from the dark web: leveraging conversational agents in the era of hyper-privacy to enhance marketing," *Journal of the Academy of Marketing Science*, vol. 48, no. 1, pp. 43–63, 2020.

[11] R. W. Gehl, "Archives for the dark web: A field guide for study," *Research Methods for the Digital Humanities*, pp. 31–51, 2018.

[12] J. Lee, "Child pornography websites on the darknet," *International Journal of Recent Technology and Engineering*, 2019.

[13] Tor Project, "Tor project - anonymity online." https://metrics.torproject.org/hidserv-dir-onions-seen.html?start=2000-01-01&end=2020-05-10, 2020.

[14] A. Kumar and E. Rosenbach, "The truth about the dark web." https://www.imf.org/external/pubs/ft/fandd/2019/09/pdf/the-truth-about-the-dark-web-kumar.pdf, 2019.

[15] J. Ilic, "More than 30% of north americans used dark web regularly in 2019." https://www.precisesecurity.com/articles/more-than-30-of-north-americans-used-dark-web-regularly-in-2019/, 2020.

[16] V. Benjamin, J. S. Valacich, and H. Chen, "Dice-e: A framework for conducting darknet identification, collection, evaluation with ethics.," *MIS Quarterly*, vol. 43, no. 1, 2019.

[17] D. Grewal, J. Hulland, P. K. Kopalle, and E. Karahanna, "The future of technology and marketing: a multidisciplinary perspective," 2020.

[18] M. Chertoff and T. Simon, "The impact of the dark web on internet governance and cyber security," *Global Commission on Internet Governance*, 2015.

[19] R. Espinosa, "Scamming and the reputation of drug dealers on darknet markets," *International Journal of Industrial Organization*, vol. 67, p. 102523, 2019.

[20] S. Broadhead, "The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments," *Computer Law & Security Review*, vol. 34, no. 6, pp. 1180–1196, 2018.

[21] L. Tornatzky and M. Fleischer, "The process of technology innovation," *Lexington, MA: Lexington Books*, vol. 165, 1990.

[22] F. T. Rothaermel and A. M. Hess, "Building dynamic capabilities: Innovation driven by individual-, firm-, and network-level effects," *Organization science*, vol. 18, no. 6, pp. 898–921, 2007.

[23] S. Lux, T. R. Crook, and D. J. Woehr, "Mixing business with politics: A meta-analysis of the antecedents and outcomes of corporate political activity," *Journal of management*, vol. 37, no. 1, pp. 223–247, 2011.

[24] S. Hafenbrädl and D. Waeger, "Ideology and the micro-foundations of csr: Why executives believe in the business case for csr and how this affects their csr engagements," *Academy of Management Journal*, vol. 60, no. 4, pp. 1582–1606, 2017.

[25] S. Goel and I. N. Chengalur-Smith, "Metrics for characterizing the form of security policies," *The Journal of Strategic Information Systems*, vol. 19, no. 4, pp. 281–295, 2010.

[26] B. Nguyen, F. Jaber, and L. Simkin, "A systematic review of the dark side of crm: the need for a new research agenda," *Journal of Strategic Marketing*, pp. 1–19, 2020.

[27] S. Ransbotham, R. G. Fichman, R. Gopal, and A. Gupta, "Special section introduction—ubiquitous it and digital vulnerabilities," *Information Systems Research*, vol. 27, no. 4, pp. 834–847, 2016.

[28] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in *Proceedings of the 22nd international conference on World Wide Web*, pp. 213–224, 2013.

[29] M. C. Van Hout and T. Bingham, "Responsible vendors, intelligent consumers: Silk road, the online revolution in drug trading," *International Journal of Drug Policy*, vol. 25, no. 2, pp. 183–189, 2014.

[30] J. Martin, *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer, 2014.

[31] V. Benjamin and H. Chen, "Securing cyberspace: Identifying key actors in hacker communities," in *2012 IEEE International Conference on Intelligence and Security Informatics*, pp. 24–29, IEEE, 2012.

[32] C. Posey, U. Raja, R. E. Crossler, and A. Burns, "Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the usa," *European Journal of Information Systems*, vol. 26, no. 6, pp. 585–604, 2017.

[33] M. Mirea, V. Wang, and J. Jung, "The not so dark side of the darknet: a qualitative study," *Security Journal*, vol. 32, no. 2, pp. 102–118, 2019.

[34] Y. Krylova, "The rise of darknet markets in the digital age: Building trust and reputation," in *Returning to interpersonal dialogue and understanding human communication in the digital age*, pp. 1–24, IGI Global, 2019.

[35] A. Greenberg, "Why facebook just launched its own 'dark web' site." https://www.wired.com/2014/10/facebook-tor-dark-site/, 2014.

[36] U. Lokala, F. R. Lamy, R. Daniulaityte, A. Sheth, R. W. Nahhas, J. I. Roden, S. Yadav, and R. G. Carlson, "Global trends, local harms: availability of fentanyl-type drugs on the dark web and accidental overdoses in ohio," *Computational and Mathematical Organization Theory*, vol. 25, no. 1, pp. 48–59, 2019.

[37] SecureDrop.org, "Directory - list of securedrops." https://securedrop.org/api/v1/directory/, 2020.

[38] P. Kannan *et al.*, "Digital marketing: A framework, review and research agenda," *International Journal of Research in Marketing*, vol. 34, no. 1, pp. 22–45, 2017.

[39] C. Dierksmeier and P. Seele, "Cryptocurrencies and business ethics," *Journal of Business Ethics*, vol. 152, no. 1, pp. 1–14, 2018.

[40] G. A. Rubasundram, "The dark web and digital currencies: A potent money laundering and terrorism opportunity," *International Journal of Recent Technology and Engineering*, vol. 7, no. 5S, pp. 476–482.

[41] K. Huang, M. Siegel, K. Pearlson, and S. Madnick, "Casting the dark web in a new light," *MIT Sloan Management Review*, vol. 60, no. 4, pp. 1–9, 2019.

[42] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker, "An analysis of underground forums," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pp. 71–80, 2011.

[43] D. Décary-Hétu and D. Laferrière, "Discrediting vendors in online criminal markets," *Disrupting criminal networks: Network analysis in crime prevention*, pp. 129–152, 2015.

[44] J. Bartlett, *The dark net: Inside the digital underworld*. Melville House, 2015.

[45] Chainalysis, "The 2020 state of crypto crime." https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf, 2020.

[46] V. Mahajan, S. Sharma, and R. D. Buzzell, "Assessing the impact of competitive entry on market expansion and incumbent sales," *Journal of marketing*, vol. 57, no. 3, pp. 39–52, 1993.

[47] M. Chertoff, "A public policy perspective of the dark web," *Journal of Cyber Policy*, vol. 2, no. 1, pp. 26–38, 2017.

[48] M. Josefy, S. Kuban, R. D. Ireland, and M. A. Hitt, "All things great and small: Organizational size, boundaries of the firm, and a changing environment," *Academy of Management Annals*, vol. 9, no. 1, pp. 715–802, 2015.

[49] C. Cimpanu, "Dark web hosting provider hacked again - 7,600 sites down." https://www.zdnet.com/article/dark-web-hosting-provider-hacked-again-7600-sites-down/, 2020.

[50] R. E. Miles, C. C. Snow, A. D. Meyer, and H. J. Coleman Jr, "Organizational strategy, structure, and process," *Academy of management review*, vol. 3, no. 3, pp. 546–562, 1978.

[51] J. T. Jost and O. Hunyady, "Antecedents and consequences of system-justifying ideologies," *Current directions in psychological science*, vol. 14, no. 5, pp. 260–265, 2005.

[52] J. T. Jost, S. Blount, J. Pfeffer, and G. Hunyady, "Fair market ideology: Its cognitive-motivational underpinnings," *Research in organizational behavior*, vol. 25, pp. 53–91, 2003.

[53] Wallace Witkowski, "Rising 'dark net' may spell trouble for google, facebook, says goldman." https://www.marketwatch.com/story/rising-dark-net-may-spell-trouble-for-google-facebook-says-goldman-2017-07-13, 2017.

[54] Tom Simonite, ""dark web" version of facebook shows a new way to secure the web." https://www.technologyreview.com/2014/11/03/170540/dark-web-version-of-facebook-shows-a-new-way-to-secure-the-web/, 2014.

[55] C. Hillenbrand and K. Money, "Corporate responsibility and corporate reputation: two separate concepts or two sides of the same coin?," *Corporate reputation review*, vol. 10, no. 4, pp. 261–277, 2007.

[56] I. Corradini and E. Nardelli, "Is data protection a relevant indicator for measuring corporate reputation?," in *International Conference on Applied Human Factors and Ergonomics*, pp. 135–140, Springer, 2020.

[57] G. S. McMillan and M. P. Joshi, "Part iv: How do reputations affect corporate performance?: Sustainable competitive advantage and firm performance: The role of intangible resources," *Corporate Reputation Review*, vol. 1, no. 1, pp. 81–85, 1997.

[58] D. Iwu-Egwuonwu and R. Chibuike, "Corporate reputation & firm performance: Empiricial literature evidence," *Ronald Chibuike, Corporate Reputation & Firm Performance: Empiricial Literature Evidence (August 16, 2010)*, 2010.

[59] S. Mishra and D. Suar, "Does corporate social responsibility influence firm performance of indian companies?," *Journal of business ethics*, vol. 95, no. 4, pp. 571–601, 2010.

[60] H. Iwamoto and H. Suzuki, "An empirical study on the relationship of corporate financial performance and human capital concerning corporate social responsibility: Applying sem and bayesian sem," *Cogent Business & Management*, vol. 6, no. 1, p. 1656443, 2019.

[61] J. M. Balmer and S. A. Greyser, "Corporate marketing: apocalypse, advent and epiphany," *Management Decision*, 2009.

[62] J. M. Balmer, S. A. Greyser, and R. Worcester, "Reflections on corporate reputations," *Management Decision*, 2009.

[63] Q. Wang, J. Dou, and S. Jia, "A meta-analytic review of corporate social responsibility and corporate financial performance: The moderating effect of contextual factors," *Business & Society*, vol. 55, no. 8, pp. 1083–1121, 2016.

[64] Y. Zhu, L.-Y. Sun, and A. S. Leung, "Corporate social responsibility, firm reputation, and firm performance: The role of ethical leadership," *Asia Pacific Journal of Management*, vol. 31, no. 4, pp. 925–947, 2014.

[65] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Academy of management review*, vol. 23, no. 3, pp. 393–404, 1998.

[66] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of management review*, vol. 20, no. 3, pp. 709–734, 1995.