Analysis of Darknet Market Activity as a Country-Specific, Socio-Economic and Technological Phenomenon

Preliminary Pre-Conference Version

Anela Sutanrikulu, Sandra Czajkowska, Jens Grossklags
Technical University of Munich
Munich, Germany

***Abstract*—The technological peculiarities of the Darknet as well as the availability of illicit items on the embedded marketplaces have raised heated debates in the media as well as keen interest by law enforcement and academics. To address this demand, in prior work, researchers have already studied the infrastructure of Darknet platforms and the global distribution of Darknet market activity.**

In our work, we take a broader perspective by studying the Darknet as a geographical, socio-economic and technological phenomenon. Our starting assumption is that there exist cross-country indicators that are related to Darknet market activity. We identify relevant indicators, and discuss their relationship to cybercrime from a theoretical perspective. We apply regression modelling and a qualitative comparative analysis (QCA) to study the impact of the identified indicators on the number of items offered on the Darknet. We find that the GDP per capita, the number of Bitcoin downloads, the number of Tor users and the education index correlate with market activity on Darknet platforms.

***Index Terms*—Darknet, cybercrime, regression analysis, QCA, socio-economic factors, technology**

I. Introduction

The Darknet refers to all encrypted communication networks that allow anonymous participation inside the Internet [1]. Within the Darknet, users can access Darknet markets, which act as digital trade platforms. The vast majority of these markets are accessible via Tor (The Onion Router) [2]. Tor allows the user to browse the Internet anonymously. Thus, this technology is used by everyone that desires privacy, such as journalists, whistleblowers, but also criminals. Additionally, Tor allows users to host Darknet market websites whose locations are hidden, so called hidden services [3]. Next to legal items, Darknet platforms offer access to drugs, pornography, weapons, terrorist communities, and human trafficking [4]. According to the Tor Project, two million users access the Internet daily using Tor [5]. However, hidden service traffic is estimated to be only about 3.4% of the total Tor traffic [6]. Although these estimates are modest, they are non-trivial [7].

The Council of Europe together with the United Nations Office on Drugs and Crime tries to counter the increasing number of cyber incidents, and takes action by implementing cross-country law enforcement programs. One of the most acknowledged acts is the Convention on Cybercrime [8]. Cybercrime, as described in the Convention, refers to technology-enabled activities. These activities are divided into four groups: 1) Offences against the confidentiality, integrity and availability of computer data and systems; 2) Computer-related offences; 3) Content-related offences (e.g., pornography); and 4) Offences related to infringements of copyright and related rights. Those four groups of activities can also be found on or be enabled by Darknet platforms.

According to the United Nations, cybercrime takes a form of a transnational crime, which may have its source in different regions and can affect different societies [9]. Further, the core concepts of cybercrime stem from traditional crime. Nonetheless, new forms of crime have emerged, such as those related to the Internet [10]. However, since the concept of crime and its cyber-version are not radically different [11], for the purpose of this work, we also draw on research on the crime-sociology relationship and apply those works to cybercrime analogously.

The problem of cybercrime is closely tied to the advent of new and popular communication technologies. Hence, there are several studies, which focus on the technological background of cybercrime, in particular, on Darknet platforms [12], [13]. The platform of the greatest interest was the Silk Road, which was extensively researched with respect to sales and transaction volumes [14]. Other studies explained the usage of cryptocurrencies and its complementary effect on Darknet platforms [15], [16]. A further stream of research focused on explaining trading processes and the distribution of vendors [17]. The bulk of these studies focus on the Darknet being a platform for illegal drugs and pharmaceutical products.

However, research should not solely focus on processes and technologies behind the Darknet, since there is also an offline perspective affecting individuals, who are using Darknet marketplaces or are indirectly influenced by them [18]. This offline perspective includes the environment of cyber-criminals and their motivation to commit cybercrime using Darknet platforms. The environment is related to economic and social triggers, which need to be understood and analyzed to, for example, effectively prepare anti-crime procedures [19]. To put it differently, crime is an integral part of society [20], therefore, cybercrime must not only be understood in the cyberspace, but the incentives need to be considered on a social, economic, and regional level. In fact, research has called for understanding the adoption of darknet markets taking into account socio-economic factors [17].

Our study is focused on this research need. Using an exploratory research approach we seek to evaluate the socio-economic elements influencing cyber-criminals as well as the technology enablers to explain Darknet market activity (as measured by sales offers) across countries. To the best of our knowledge, it is the first study to investigate these effects, focusing not only on drugs, but on all available items on the Darknet that can be associated with a shipping country. We analyze cross-country social factors that influence cybercrime behavior, but we limit our study to activities and offerings on the Darknet. We expect that there are groups of countries with a similar Darknet market activity having comparable socio-economic and technology conditions. Hence, we set the following research question:

RQ: *What regional, socio-economic, or technological factors are related to Darknet market activity across countries?*

Our paper is structured as follows. In Section II, we will provide an overview of three dimensions of crime research: regional, socio-economic, and technological. We will further provide a theoretical background guiding our variable choices. Sections III and IV will give an overview of our data collection process and quantitative approach. In Sections V and VI, we will discuss our results and provide implications. In Section VII, we will offer concluding remarks and present future research possibilities.

II. Related Work

Crime remains "a social and economic phenomenon and is as old as the human society" [11]. In fact, there is a stream in the literature, that has demonstrated the existence of a natural crime rate [21], [22]. In other words, crime could be controlled by introducing new forms of security measures or law enforcement, but the resulting crime decay would be visible only in the short run. In the long run, crime returns to its natural level [23], [24]. This crime equilibrium is also visible on the Darknet. In 2017, three of the largest Darknet markets: AlphaBay, Hansa and RAMP were closed by law enforcement agencies [25]. However, this stopped the criminals and the business only temporarily, until they migrated to other markets or platforms [25]. However, there must be certain circumstances that regulate the natural crime rate across regions.

Therefore, taking into account achievements of current research, we consider the problem of cybercrime with respect to Darknet market activity and aim to investigate influencing factors. These include the geography, the social and economic conditions of the place of occurrence, and the enabling technologies.

A. Regional dimension

It has already been shown that Darknet trade is geographically distributed [17]. However, neither is the distribution of crime uniform across countries, nor are other factors such as economic inequality [26]. It means that cybercrime has its source in specific regions in the world and affects victims located in specific locations. Given that Darknet related crime is concentrated in several areas around the world [17], we assume that crime-affected regions hold similar characteristics.

Urbanization rate. One example of such regions are areas with a high urbanization rate [26], [27]. Given a large number of different cultures and communities within urban societies [28], urban areas are considered to be enhancing crime rates [29]. Even on a global scale, there are differences in the likelihood to commit crime, particularly cybercrime. It has been recorded that Eastern European countries, such as Russia, have a high level of cybercrime [30], [31].

Corruption. On the other hand, crime is directly related to the criminal. However, each individual's activity comes from a place of occurrence, i.e. the place where an individual is located [18]. Although the motivation of all criminals across the world may be comparable, only those individuals, who are given the opportunity by a country to commit a series of crimes, will be successful [26]. Opportunity, in this context, means that some countries are unable to track cybercrime activities or to provide an appropriate level of cyber security. Hence, criminals are empowered by a low law enforcement level. One factor that indicates countries' low level of law enforcement is corruption. Generally, corruption is associated with the inability to act upon crime. Therefore, corruption may encourage cybercrime [18].

B. Socio-economic dimension

The United Nations Office on Drugs and Crime argued that economic factors may influence the evolution of crime trends [32]. Although criminal behavior may be influenced by personal characteristics, criminals may as well be sensitive to environmental factors. For instance, there are people who are influenced by society to excel in their studies and to build a successful career. In the same way, there are people, who are pushed to crime by being exposed to a set of economic and social conditions [18]. According to research, crime is to a certain extent an integrated part of a social situation [18], [20]. Therefore, it is crucial to understand how crime and society are interrelated.

GDP and Money Laundering. Social and economic inequality as well as stratification of the society may lead to frustration and exclusion of the lower stratum of society. It may further encourage people from lower socio-economic classes to find additional revenue sources or to search for more affordable goods and services. For instance, impoverished people may be more willing to infringe on copyright, e.g. by not purchasing legal software or content [33]. Hence, they are more likely to look into alternative offers, such as those placed on Darknet platforms.

It is assumed that a high GDP indicates a general well-being of all participants in the economy. Nonetheless, researchers found that high GDP per capita and unemployment play an important role in cybercrime [30], which may imply economic inequality. Given that criminals have an economic or financial motive and earn money through their illegal activities, they have to inject their obtained assets into the legal economy through money laundering [34]. Although money laundering is a crime by itself, it is directly related to Darknet sales, i.e., money received from sales has to be laundered.

Education. Similarly, studies have shown that education effectively reduces income inequality [35]. Furthermore, earnings increase with a worker's degree of education. It has also been shown that schooling significantly reduces criminal activity [36]. Hence, a low education rate, i.e., fewer years of schooling may increase the probability of individuals engaging in crime.

C. Technological dimension

With the advent of new technologies, many forms of cybercrime have emerged. Technologies have led to an efficiency increase of daily activities, but have also contributed to the growth of crime efficiency [37]. Given that cybercrime can be defined as crime enabled by a technology, there is no doubt that cybercrime and technologies co-evolve [38]. For example, technologies that enable criminals to stay anonymous on the Internet, such as Tor, make cybercrime much more attractive than traditional crime, where it is more difficult to hide one's identity.

Patent applications. The overall technological advancement of a country, which can be measured in the number of patent applications, shows the extent to which people are familiar with the usage of current technologies [39]. Generally, better educated individuals tend to have a better technology understanding. The technological advancement of a country is an indicator, how well-versed citizens are in Internet usage. In fact, unemployed individuals skilled in computer science are argued to be more likely to engage in online crime, given their technical know-how and the poor economic environment [30].

Tor and Bitcoin. Criminals that act on the Darknet do not only rely on Tor, but also on cryptocurrencies, which have gained popularity in crime networks and Darknet trade. In particular, Bitcoin has long been the only means of payment on many Darknet platforms. Studies showed that 46% of Bitcoin transactions were related to illegal activities [40] and that historical transactions can be related to previous Darknet market sales [2].

III. Data

Darknet Data: We retrieved Darknet data from the Internet Archive [41], a freely accessible non-profit library, which had an archive of scrapped data from Darknet marketplaces collected by the researcher Gwen Branwen. The collection further included data gathered by other researchers. Thus, the entire dataset consisted of 89 Darknet markets and 37+ related forums [42]. The dataset contained mainly HTML and PHP files, image data, CSV files, and different configuration files. For the purpose of our study, we removed the forum data. Furthermore, we focused only on data that held information about product offers on the Darknet.

We extracted data consisting of item names, vendor names and the shipping from countries. Given that this information was not available for all marketplaces, we ended up with a dataset consisting of 38 markets[1]. The market data had different timestamps from 2013 until 2015, given the different running times of those marketplaces. Since some vendors offered items on multiple markets, we deleted all multiple appearances of the same item offer, i.e., items that had the same name and same vendor name. Thus, we retrieved 402.093 item offerings (see Figure 1). This dataset comes with certain limitations. Although we deleted duplicates of the exact same offer, we did not remove postings of the same products, e.g., different doses of the same drug provided by the same vendor. Furthermore, the general quality of the information provided on Darknet platforms remains questionable. Vendors may provide false information, both for their items as well as their shipment location. Similarly, vendors may use different names or identities. Therefore, seemingly disparate item offerings may refer to the same item [43].

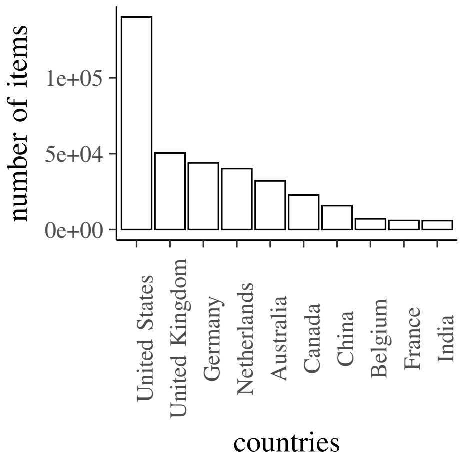

Fig. 1. Distribution of the number of items for top 10 selling countries

Other Data: In order to explain the number of items per country, we collected the latest data available for the factors discussed in Section II. This additional data was publicly available on the Internet and was mapped to 159 countries: population [44], corruption perception index [45], compliance with the Anti-Money Laundering and Countering Terrorism Financing International Standard (AML) [46], economic inequality (Gini) index [47], [48], percentage of population living in urban areas (urbanization) [49], education index [50], GDP [51], unemployment percentage [52], number of patent grants for direct applications [53], number of relay Tor users [54], number of bridge Tor users [55], number of Bitcoin downloads [56], and number of Bitnodes [57]. After removing entries with missing values from the dataset, we ended up with 95 observations. A description of these variables is available in Table I.

[1] 1776, Abraxas, Absolem, Agora, Alpaca, AlphaBay, Amazon Dark, Andromeda, Atlantis, Cloud9, Deepzon, Dodge Road, Dream Market, Drugslist, East India Company, Evolution, FreeBay, Free Market, Hansa, Hydra, Kiss, Middle Earth, Nucleus, Outlaw Market, Oxygen, Panacea, Pandora, Pigeon, Sheep, Silkkitie, Silk Road, The Onion Market, The Pirate Market, Tochka, TorEscrow, TorMarket, Utopia, White Rabbit

TABLE I
SOURCES AND DESCRIPTION FOR ADDITIONAL DATA USED IN THE STUDY

List of data sources		
Variable	**Description**	**Reference**
Population	List of countries with respective total population by country	[44]
Corruption Perception Index	Perceived levels of public sector corruption in 180 countries and territories. Drawing on 13 surveys of business people and expert assessments, the index scores on a scale of zero (highly corrupt) to 100 (very clean)	[45]
Total AML/CFT	Compliance with the Anti-Money Laundering and Countering Terrorism Financing International Standard (AML)	[46]
Economic inequality (gini index)	The distribution of income across income percentiles in a population	[47], [48]
Urbanization	Percentage of population living in urban areas	[49]
Education index	Mean Years of Schooling and Expected Years of Schooling	[50]
GDP	Gross domestic product per capita	[51]
Unemployment	Rate of unemployment	[52]
Patent applications	Number of patent grants for direct applications	[53]
TOR users1	Number of relay Tor users	[54]
TOR users2	Number of bridge Tor users	[55]
Bitcoin	Number of Bitcoin downloads	[56]
Bitnodes	Number of bitnodes	[57]

IV. Analysis

In order to investigate the relationship between Darknet offers and the different cross-country factors, we applied the following methods of analysis:

Regression Analysis (using *R* [58]): Regression analysis aimed to explore if there are regional, socio-economic or technological factors, which are related to Darknet offerings. We performed two regression techniques, independently. Thus, we first applied *multivariate regression* to determine the existence of a relationship between certain factors and Darknet offerings. Rather than quantifying the exact effect that each factor has on Darknet offerings, we observed the significance of the factors. Second, we applied a *regression tree analysis* to test the results from the former one and to note the similarities. Ultimately, we aimed to find the most important variables related to Darknet offerings with the regression analyses.

Qualitative Comparative Analysis (using *fsQCA* [59]): In addition to the regression analysis, we performed a qualitative comparative analysis (QCA) to support our findings from the regression analysis. By applying a different analysis technique, we aimed to test if the same variables show a similar significant correlation. QCA is a method that indicates whether a variable is a minor or major contributor in a given set of combinations of variables that are jointly related to the outcome [60]. Therefore, we aimed at obtaining a set of factors that relate to a high number of items on Darknet.

Given that our dataset included 95 countries (159 exist in total), we assumed it to be a representative dataset to derive global implications. Nevertheless, applying independent methods would strengthen our results and make the outcome more robust. As a data pre-processing step, to enable a fair comparison between countries, we divided all count variables by the population. This way, we could perform a per capita analysis.

A. Regression Analysis

1) Multivariate Regression: The regression analysis had the goal to fit a model that would explain the response variable; number of items on the Darknet per capita, by the other variables in the dataset. Given the non-linear relationship between the response and the predictor variables, an option to restore linearity was to log-transform the response and to use a multivariate regression model. We tested the null hypothesis (1) that there is no predictor variable influencing the number of Darknet items, against our actual hypothesis (2) that there is at least one variable influencing our response. We performed the testing with a significance level of 0.05 (the b_i's are the corresponding coefficients of the 12 predictors):

$$H_0 : b_i = 0 \tag{1}$$

$$H_1 : \text{at least one } b_i \neq 0 \tag{2}$$

We used the R build-in function lm to build the model. The fitted multivariate regression model followed the linearity assumption; the residuals are equally scattered around zero and show no pattern, the sample quantities lie on a straight line, and the influence plot and cook's distance plot show no over-dominant observation. After fitting the model with all predictors, we used the AIC step-wise selection criterion in both directions to find the subset including the best predictor variables.

The final model summary is shown in Table II, indicating the predictors' significance. To test our hypotheses, we used a simple F-test. Given that $F_0 = 45.16 \geq F_{5,89} = 2.32$, we rejected the null hypothesis H_0. The adjusted R-squared (0.7) shows a fair linear effect on the log-transformed response.

2) Regression Tree: In order to evaluate the results from the multivariate model, we used an additional regression method called regression trees. This method partitions the dataset into smaller groups and fits a simple model to each sub-group. We

TABLE II
SUMMARY OF THE MULTIVARIATE REGRESSION MODEL WITH THE LOG-TRANSFORMED RESPONSE VARIABLE

	Estimate	Std. Error	t value	Pr(< $\|t\|$)
(Intercept)	-1.782e+01	9.692e-01	-18.383	< 2e-16***
AML	5.179e-02	2.575e-02	2.011	0.04732*
education index	4.011e+00	1.762e+00	2.277	0.02521*
GDP⋆	2.046e-05	1.125e-05	1.819	0.07232
Bitcoin downloads⋆	4.079e+02	1.227e+02	3.323	0.00129**
tor relay users⋆	2.805e-01	1.399e-01	2.004	0.04807 *
Observations	95			
R^2	0.717			
Adjusted R^2	0.701			
Residual Std. Error	1.591 (df = 89)			
F Statistic	45.162*** (df = 5; 89)			
Note:	*p<0.1; **p<0.05; ***p<0.01			
Note:	⋆ per capita			

TABLE III
VARIABLE IMPORTANCE OF BAGGED REGRESSION TREE MODEL

GDP per capita	100.000
corruption	89.572
bitnodes per capita	75.115
Bitcoin downloads per capita	73.0863
education index	51.953
tor relay users per capita	51.075
tor bridge users per capita	19.205
gini index	8.684
patent per capita	6.146
urbanization	5.339
unemployment	2.222
AML	0.000

used the same dataset as before, but this time performing no log-transformation of the response, because regression trees do not rely on any assumptions about the data. First, we split our dataset into training (85%) and testing (15%) and then used grid search to find the max depth of the tree as well as the min observation split. To build the tree, we used the R $rpart$ package. Second, we performed bagging, i.e. combining and averaging multiple models, to reduce variance. Thus, we were able to assess predictors' importance on the response across bagged trees. The root mean squared error (RMSE) on the testing data was 0.0003122384, which is reasonably small. Table III shows all predictor variables and their importance on a scale from 0 (low) to 100 (high).

B. QCA

To extend our results from the regression analysis, we conducted a qualitative comparative analysis (QCA). We performed the QCA according to the methodology provided in the literature [59], [61]. The results of QCA should indicate a set of combinations, which are associated with a high number of items on Darknet platforms. In our case, combinations refer to sets of country-specific characteristics that are jointly related to high item offers on the Darknet. Given the results from regression, we assumed that Bitcoin downloads per capita, Tor users, GDP per capita, and the education index have an impact on high number of items per capita sold on the Darknet. Furthermore, we included corruption and AML as explanatory variables in our analysis, given their conflicting significance in the two regression models. Hence, our sample contained 95 cases and we used 6 causal conditions. Therefore, we assumed the appropriate number of conditions in the model [62]. Finally, we obtained a data set with a satisfactory variability across sample countries [59]. Each country represented an individual set of characteristics, which resulted from specific explanatory variables. After specifying our research model, we conducted a calibration process. For each of the aforementioned variables, we used a median to specify a middle threshold of outcome and causal conditions. For upper and lower thresholds, we used a percentile at the point of 0.75 and 0.25, respectively. Additionally, we performed a truth table analysis. The truth table presented a list of all combinations of explanatory variables for a given data set. The truth table showed that cases were distributed among several possible combinations, which indicated that no more conditions had to be added to the model [61]. We eliminated configurations by setting frequency and consistency thresholds. After optimizing the configurations with respect to the sample size, we set the minimum frequency threshold to 1 and the minimum consistency threshold to 0.80.

V. RESULTS

A. Regression Results

The regression analysis using the multivariate model with a log-transformed response, suggested a positive relationship between the number of items per capita on Darknet markets and the variables: Bitcoin downloads per capita, education index, AML, Tor relay users per capita, and GDP per capita. Therefore, our results show that there may be socio-ecnomic and technological factors influencing Darknet market activity. Given that our model is an ordinary least squares regression including only continuous data, we interpret the regression coefficient of a predictor variable, as the expected change in log of the response with respect to a one-unit increase in the predictor, holding all other variables fixed. The most significant predictor was the Bitcoin downloads per capita variable (having the smallest p-value). Thus, a one-unit increase in Bitcoin downloads per capita increases the log of the number of items per capita by $4.079e + 02$. The relationship between the coefficients of the other predictors and the response variable can be interpreted accordingly (Table II).

The analysis using regression trees suggested that all variables except AML influence to some extent the number of items per capita on Darknet markets. However, the most influential variable was by far GDP per capita, having the maximum importance. Other important variables were: corruption, Bitnodes per capita, Bitcoin downloads per capita, education and tor relay users per capita. Given that we applied bagging to the regression trees, which combines multiple trees into a single procedure to reduce variance and improve accuracy, the statistical interpretation of this method was poor. Therefore, the resulting tree and the split could not be shown. Nevertheless, given the nature of our study, having a rank of the predictors with a small RMSE was sufficient. Although the two regression methods did not produce the exact same results, they did have a few similarities. Both methods indicated that GDP per capita, education, Bitcoin, and Tor users seem to have a significant effect on Darknet market activity.

B. QCA Results

Standard analysis of QCA method showed two configurations of results. The intermediate solution indicated three different factors' configurations which explain 75% of the cases that led 88% of the time to high number of items. Based on the set consistency threshold (0.80), the model expressed results distributed among 22 combinations. In the end the model enables to explain 75% of the cases with 3 different combinations:

1) Bitcoin downloads * Tor relay users * ∼Corruption * ∼AML
2) Bitcoin downloads * Tor relay users * ∼Corruption * Education
3) Bitcoin downloads * Tor relay users * GDP * Education

Table 3 gives an overview of the results, that are described above.

The results were compared with parsimonious solution, as the intermediate solution provided only simple counterfactuals [61]. The parsimonious solution suggested that Bitcoin downloads and Tor users have the most significant impact on a high number of items sold on Darknet. It means that both of these factors are more robust, i.e. they are more likely to remain unchanged in case of a model adjustment.

We investigated also countries that contribute to the configuration of Bitcoin downloads and Tor users. The results of standard analysis indicated several countries, that had a major contribution to the set including the per capita variables, number of Bitcoin download and number of Tor users: Sweden, Lithuania, Finland, Netherlands, Luxembourg, Switzerland, Estonia, Ireland, Latvia, Germany, Austria, Malta, Norway, Bulgaria, Slovenia, United Kingdom, Czech Republic, United States and Denmark. As those countries belong to countries of rather high GDP (higher than the median GDP for the 95 countries in our dataset), this result suggests that highly developed countries are more associated with Darknet activity.

VI. Discussion

For our analysis, we merged different Darknet market data sources found on the Internet Archive [41]. The data comprised 38 markets and included 402.093 item offerings. We grouped the offerings per country and further included regional, socio-economic, and technological indicators. We assessed the effect of these indicators on the number of item offerings on the Darknet. We used two different methods of analysis using two different kinds of software. First, we performed a multivariate regression with a transformation as well as a bagged regression tree analysis using R [58]. Second, we used qualitative comparative analysis using fsQCA [59] to support our results from the former analysis.

Literature research shows that both personal characteristics of an individual as well as environmental factors may lead to crime [18]. Nevertheless, we are not accounting for the sensitivity of certain individuals to the environment in our study. Rather, we show that a general social situation is related to crime, as suggested by [20]. Our regression analysis shows that there are various factors that influence Darknet market activity. The analysis indicates a relationship between GDP per capita, education, Bitcoin, and Tor users with the number of items on the Darknet (per shipping country). Darknet market activity is higher in countries that have a high GDP per capita. This indicates that wealthy nations are more likely to get involved or be exposed to Darknet activities. A study showed that Darknet drug vendors are primarily located in a small number of consumer countries. Therefore, given that GDP shows the level of spending and general consumption of a nation, it could be argued that countries with a high GDP are attractive for Darknet vendors due to highly active marketplaces and a high demand for goods and services. Hence, GDP and cybercrime are related [30]. Nonetheless, our results do not show any significance when it comes to the relationship between economic inequality and unemployment with Darknet market activity. Although the AML variable shows importance in the linear regression model, this could neither be confirmed by the regression tree nor by the QCA. Thus, the country compliance with AML/CFT International Standard with respect to Darknet market activity remains questionable and a subject for future research.

Furthermore, our results imply that cybercrime and certain technologies might co-evolve [38]. Although the number of patent grants, used as a variable for a general technological development of a country, does not hold a high significance in our study, there are technologies that are particularly important for Darknet activities. The indicator of Bitcoin downloads is significant in both of our analysis methods. With the advent of Bitcoin technology, cyber-criminals obtained tools, which enabled them to trade anonymously on the Darknet. Furthermore, QCA results show that a combination of Bitcoin downloads and Tor users jointly lead to a high number of items sold on the Darknet. Tor usage is strongly associated with Darknet activity. Although many services and products offered on the Darknet, the Tor hidden services, are illegal [4], some individuals do not use Tor for illicit purposes. Individuals use Tor to protect their data privacy from government spies and surveillance systems

TABLE IV
CONFIGURATIONS FOR HIGH NUMBERS OF ITEMS ON DARKNET PLATFORMS SOURCE: OWN REPRESENTATION BY ADAPTING CONFIGURATION CHART USED BY FISS [60]

	Solution 1	Solution 2	Solution 3
Tor relay users⋆	◯	◯	◯
Bitcoin downloads⋆	◯	◯	◯
AML	⊕		
Corruption	⊕	⊕	
GDP⋆			○
Education index		○	○
Consistency	0.82	0.81	0.90
Raw Coverage	0.14	0.18	0.69
Unique Coverage	0.02	0.00	0.55
Overall Solution Consistency	0.88		
Overall Solution Coverage	0.75		

Note: ⋆ per capita
Note: A white circle indicates the presence of a condition and a white circle with "x" indicates its absence. Large circles indicate core conditions; small circles indicate peripheral conditions. Blank spaces indicate "Don't care".

as well [63]. Therefore, both technologies do not always coexist, but in case they do, they are likely to lead to a high number of items sold on the Darknet. Additionally, research suggests a strong relationship between GDP per capita and the adoption of the Bitcoin blockchain by country [64]. This indicates a likelihood of an interaction between GDP, general Bitcoin usage and Darknet market activity.

Although research shows that schooling significantly reduces criminal activity [36], we found that the education index is positively related to the number of items sold on Darknet markets. The QCA results suggest a certain interaction between the technological variables and education. Thus, our findings imply that better educated individuals usually have a better technological understanding and are more familiar with the Darknet-enabling technologies.

Moreover, the bagged regression tree shows that the corruption perception index is an important variable in explaining the number of Darknet items. Similarly, the QCA specifies one case of factor combinations, which indicates that low levels of corruption are related to a high response outcome. The corruption perception index shows how corrupt the public sectors of a certain country are, where a low index indicates high corruption and vice versa [45]. The QCA results show the presence of a low corruption perception index, meaning that the activity of vendors on the Darknet is greater in more corrupted countries. This suggests that the presence of corruption influences online crime and encourages illegal cyber-activity [18].

As already stated, the data indicates that the top ten selling countries account for 90% of all items sold on the Darknet. These top countries include: United States, United Kingdom, Germany, Netherlands, Australia, Canada, China, Belgium, France, and India. These countries were also found to be representative in the Darknet drug trade study by [17]. Furthermore, 4 countries out of 10 top selling countries (United States, United Kingdom, Germany and Netherlands) were indicated also in QCA results. Hence, the appearance of the same group of countries in separate studies suggests that the Darknet trade has a nonuniform geographical distribution [17]. If we consider the common characteristics of these countries, we note that all of them have a high GDP. Moreover, according to the literature, areas with a high urbanization rate correlate with high crime rates [29]. In our analysis, we could not observe a general significant effect of the urbanization rate on Darknet market activity. However, we note that the urbanization rate of the top ten selling countries is above 75% (except India and China), indicating a relationship between a high number of items sold and a high urbanization. Furthermore, the corruption perception index for the above mentioned countries is also rather high (except for India and China), which means that most of the top ten selling countries are less corrupted.

VII. CONCLUSION

In this study, we aimed to explore the various factors, which might influence Darknet trade. Specifically, we studied what impacts the number of items sold on the Darknet across countries. We based our quantitative research on the literature that aimed to explain cybercrime as a sociological and economic phenomenon. We further explored regional and technological drivers to explain Darknet market activity. Thus, we collected data from 38 Darknet markets, which included overall 159 countries. Finally, we added per-country data for regional, socio-economic, and technological indicators.

To evaluate the influence of country related variables on the number of items sold on the Darknet, we used two methods: regression analysis and qualitative comparative analysis (QCA). The results showed that there are specific factors that may influence Darknet trade and there are groups of countries that hold similar characteristics with respect to their activity on the Darknet.

Regression analysis implied a relationship between the GDP per capita, the education index, the number of Bitcoin downloads and the number of Tor users and the number of items sold on the Darknet per shipping country per capita. The influence of those variables was further explored in the QCA. The latter showed that Bitcoin downloads and Tor users were jointly present in the combination of factors that lead to high number of items on the Darknet.

The top ten shipping countries were characterized by a comparatively high GDP. This may imply that these countries represents attractive marketplace for Darknet vendors due to the higher buying power of their citizens. Furthermore, we found that cybercrime activity on the Darknet co-evolves with certain technologies. Particularly, the relationship between the number of Bitcoin downloads and Tor users with Darknet market activity indicates that Darknet vendors and users have high acquaintance with technology.

To the best of our knowledge, this is the first study to research the relationship between regional, socio-economic, and technological factors and Darknet item offers. However, given the limited availability of country-level data, our assumptions cannot provide a full understanding of global Darknet trade. Researchers should channel efforts to find information on more countries that have users on the Darknet. Moreover, having complete datasets for economic indicators across countries would be beneficial for further research. International institutions with dedicated programs against cybercrime as well as national authorities should cooperate to map the supply and demand chain of illegal trade. A profound understanding of individuals' incentives to engage in cybercrime as well as knowledge about the distribution of illegal items on the Darknet can enable a successful battle against the dark space of the Internet.

Acknowledgments: We thank the reviewers and the conference attendees for their constructive feedback.

References

[1] S. Aked, C. Bolan, and M. Brand, "Determining what characteristics constitute a darknet." Australian Information Security Management Conference, Edith Cowan University, 2013.

[2] C. Janze, "Are cryptocurrencies criminals best friends? Examining the co-evolution of Bitcoin and darknet markets," in *Twenty-third Americas Conference on Information Systems (AMCIS)*, 2017.

[3] D. Anon, "Make your site visible on the dark web: A guide to Tor hidden services," 2018. [Online]. Available: https://privacy.net/make-site-visible-dark-web-tor-hidden-services/

[4] D. Moore and T. Rid, "Cryptopolitik and the darknet," *Survival*, vol. 58, no. 1, pp. 7–38, 2016.

[5] The Tor Project, "Users." [Online]. Available: https://metrics.torproject.org/userstats-relay-country.html

[6] ——, "Some statistics about onions," 2015. [Online]. Available: https://blog.torproject.org/some-statistics-about-onions

[7] European Monitoring Centre for Drugs and Drug Addiction and Europol, "Drugs and the darknet: Perspectives for enforcement, research and policy," 2017. [Online]. Available: https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy

[8] Council of Europe, "Convention on Cybercrime. European Treaty series no. 185," 2001.

[9] United Nations Office on Drugs and Crime, "Cybercrime." [Online]. Available: https://www.unodc.org/unodc/en/cybercrime/index.html

[10] R. J. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *Workshop on the Economics of Information Security (WEIS)*, 2012.

[11] K. Dashora, "Cyber crime in the society: Problems and preventions," *Journal of Alternative Perspectives in the Social Sciences*, vol. 3, no. 1, pp. 240–259, 2011.

[12] M. J. Barratt, J. A. Ferris, and A. R. Winstock, "Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States," *Addiction*, vol. 109, no. 5, pp. 74–83, 2014.

[13] V. Bhaskar, R. Linacre, and S. Machin, "The economic functioning of online drugs markets," *Journal of Economic Behavior & Organization*, vol. 159, pp. 426–441, 2017.

[14] N. Christin, "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace," in *22nd International Conference on World Wide Web*, 2013, pp. 213–224.

[15] F. Glaser, K. Zimmermann, M. Haferkorn, M. Weber, and M. Siering, "Bitcoin - Asset or currency? Revealing users' hidden intentions," *22nd European Conference on Information Systems (ECIS)*, 2014.

[16] S. Kethineni, Y. H. Cao, and C. Dodge, "Use of Bitcoin in darknet markets: Examining facilitative factors on Bitcoin-related crimes," *American Journal of Criminal Justice*, vol. 43, pp. 141–157, 2018.

[17] M. Dittus, J. Wright, and M. Graham, "Platform criminalism: The 'last-mile' geography of the darknet market supply chain," in *Proceedings of the 2018 World Wide Web Conference*, 2018, pp. 277–286.

[18] J. Lusthaus and F. Varese, "Offline and local: The hidden face of cybercrime," *Policing: A Journal of Policy and Practice*, 2017.

[19] D. M. Levi, "The economic, financial & social impacts of organised crime in the eu," 2013. [Online]. Available: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493018/IPOL-JOIN_ET\%282013\%29493018_EN.pdf

[20] D. Canter and D. Youngs, "Crime and society," *Contemporary Social Science*, vol. 11, no. 4, pp. 283–288, 2016.

[21] J. P. Sahu and C. K. Mohanty, "Is there a natural rate of crime in India?" *Contemporary Social Science*, vol. 11, no. 4, pp. 334–346, 2016.

[22] P. Narayan, I. Nielsen, and R. Smyth, "Is there a natural rate of crime?" *American Journal of Economics and Sociology*, vol. 69, no. 2, pp. 759–782, 2010.

[23] A. Buck, M. Gross, S. Hakim, and J. Weinblatt, "The deterrence hypothesis revisited," *Regional Science and Urban Economics*, vol. 13, no. 4, pp. 471–486, 1983.

[24] A. Buck, S. Hakim, and U. Spiegel, "The natural rate of crime by type of community," *Review of Social Economy*, vol. 43, no. 2, pp. 245–259, 1985.

[25] European Union Agency for Law Enforcement Cooperation, "Internet organised crime threat assessment 2018." [Online]. Available: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

[26] V. Garg and L. Camp, "Why cybercrime?" *ACM SIGCAS Computers and Society*, vol. 45, no. 2, pp. 20–28, 2015.

[27] C. R. Shaw and H. D. McKay, *Juvenile delinquency and urban areas*. The University of Chicago Press, 1942.

[28] C. S. Fischer, "Toward a subcultural theory of urbanism," *American Journal of Sociology*, vol. 80, no. 6, pp. 1319–1341, 1975.

[29] E. Gumus, "Crime in urban areas: An empirical investigation," *Akdeniz I.I.B.F. Dergisi*, vol. 4, no. 7, pp. 98–109, 2004.

[30] A. Ilievski and I. Bernik, "Social-economic aspects of cybercrime," *Innovative Issues and Approaches in Social Sciences*, vol. 9, no. 3, pp. 8–22, 2016.

[31] Cyber Defcon Project, "Global security map," 2019. [Online]. Available: http://globalsecuritymap.com/

[32] United Nations Office on Drugs and Crime, "Monitoring the impact of economic crisis on crime," 2011. [Online]. Available: http://www.unodc.org/documents/data-and-analysis/statistics/crime/GIVAS_Final_Report.pdf

[33] C. Osorio, "A contribution to the understanding of illegal copying of software: Empirical and analytical evidence against conventional wisdom," Massachusetts Institute of Technology, Tech. Rep., 2002.

[34] European Union Agency for Law Enforcement Cooperation, "Money laundering." [Online]. Available: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/money-laundering

[35] A. Abdullah, H. Doucouliagos, and E. Manning, "Does education reduce income inequality? A meta-regression analysis," *Journal of Economic Surveys*, vol. 29, no. 2, pp. 301–316, 2015.

[36] L. Lochner and E. Moretti, "The effect of education on crime: Evidence from prison inmates, arrests, and self-reports," *American Economic Review*, vol. 94, no. 1, pp. 155–189, 2004.

[37] R. Broadhurst, P. Grabosky, M. Alazab, B. Bouhours, S. Chon, and C. Da, "Crime in cyberspace: Offenders and the role of organized crime groups," Australian National University Cybercrime Observatory, Tech. Rep., 2013.

[38] S. McQuade, "Technology-enabled crime, policing and security," *The Journal of Technology Studies*, vol. 32, no. 1, pp. 32–42, 2006.

[39] D. Archibugi, "Patenting as an indicator of technological innovation: A review," vol. 19, no. 6, p. 357–368, 1992.

[40] S. Foley, J. R. Karlsen, and T. J. Putnins, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" *The Review of Financial Studies*, vol. 32, no. 5, pp. 1798–1853, 2019.

[41] G. Branwen, "Files for dnmarchives." [Online]. Available: https://archive.org/download/dnmarchives

[42] ——, "Dark net market archives, 2011-2015." [Online]. Available: https://archive.org/details/dnmarchives

[43] X. H. Tai, K. Soska, and N. Christin, “Adversarial matching of dark net market vendor accounts.” ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2019, pp. 1871–1880.
[44] United Nations Department of Economic and Social Affairs, “World population prospects 2019.” [Online]. Available: https://population.un.org/wpp/Download/Standard/Population/
[45] Transparency International, “Corruption perceptions index 2018.” [Online]. Available: https://www.transparency.org/en/cpi/2018/results
[46] C. V. Yepes, “Compliance with the AML/CFT international standard: Lessons from a cross-country analysis,” International Monetary Fund, Tech. Rep., 2011.
[47] The World Bank, “GINI index.” [Online]. Available: https://data.worldbank.org/indicator/si.pov.gini
[48] Central Intelligence Agency, “The world factbook.” [Online]. Available: https://www.cia.gov/library/publications/the-world-factbook/rankorder/2172rank.html
[49] Our World in Data, “Urbanization.” [Online]. Available: https://ourworldindata.org/urbanization
[50] United Nations Development Programme, “Human development reports education index.” [Online]. Available: http://hdr.undp.org/en/content/education-index
[51] International Monetary Fund, “GDP per capita, current prices.” [Online]. Available: https://www.imf.org/external/datamapper/NGDPDPC@WEO/WEOWORLD
[52] The World Bank, “Unemployment.” [Online]. Available: https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS?end=2018&start=1991
[53] World Intellectual Property Organization, “Patent.” [Online]. Available: https://www3.wipo.int/ipstats/
[54] The Tor Project, “Userstats relay country.” [Online]. Available: https://metrics.torproject.org/userstats-relay-country.csv
[55] ——, “Userstats bridge country.” [Online]. Available: https://metrics.torproject.org/userstats-bridge-country.csv
[56] Source Forge, “Bitcoin download statistics.” [Online]. Available: https://sourceforge.net/projects/bitcoin\\/files/stats/map?dates=2008-01-01+to+2019-08-22
[57] Bitnodes, “Global bitcoin nodes distribution.” [Online]. Available: https://bitnodes.earn.com/\#global-bitcoin-nodes-distribution
[58] R Core Team, *R: A Language and Environment for Statistical Computing*, R Foundation for Statistical Computing, Vienna, Austria, 2017. [Online]. Available: https://www.R-project.org/
[59] C. Ragin, *User's Guide to Fuzzy-Set / Qualitative Comparative Analysis*. [Online]. Available: http://www.u.arizona.edu/~cragin/fsQCA/download/fsQCAManual.pdf
[60] P. C. Fiss, “Building better causal theories: A fuzzy set approach to typologies in organization research,” *Academy of Management Journal*, vol. 54, no. 2, 2011.
[61] P. T. Leppänen, A. F. McKenny, and J. C. Short, “Qualitative comparative analysis in entrepreneurship: Exploring the approach and noting opportunities for the future,” *Standing on the Shoulders of Giants (Research Methodology in Strategy and Management)*, vol. 11, pp. 155–177, 2019.
[62] D. Berg-Schlosser and G. Meur, “Comparative research design: Case and variable selection,” in *Applied Social Research Methods: Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*, B. Rihoux and C. C. Ragin, Eds., 2009, vol. 51, pp. 19–32.
[63] C. Osborne and Z. Whittaker, “Cyber security 101: Protect your privacy from hackers, spies, and the government,” 2019. [Online]. Available: https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/
[64] F. Parino, M. G. Beiró, and L. Gauvin, “Analysis of the Bitcoin blockchain: Socio-economic factors behind the adoption,” *EPJ Data Science*, vol. 7, no. 1, 2018.