Cybercriminal Markets

Economics of Cyber Security Assignment 3 Block 4

Erin Bartholomew, Marrit Hoppenreijs, Christian van Bruggen, Sarah Vetter

Delft University of Technology

Abstract: Cybercriminal markets host a vast number of sales of illegal goods, both physical and digital. The challenge of tracking and stopping those sales falls on several national and international organizations. By investigating relationships and capabilities of various actors, one can develop a more concrete understanding of the wider costs and benefits of potential actions. Furthermore, variance in metrics are further investigated to determine potential causes of that variance. Specifically, the influence of law enforcement budget and drug use in various countries will be investigated to determine if they have an impact on the total sales in cybercriminal markets.

Keywords: cybercriminal markets, underground forums, cybersecurity countermeasures, security metric variance, factor analysis

1 Introduction

This paper explains three potentials actor's countermeasures in order to combat cybercriminal markets. The incentives in combating the cybercriminal markets will be described and which externalities affects the actor's strategies in a positive and negative manner. Additionally, this paper analyses the factors that influence the security performance in relation to the metric based in the first assignment.

2 Countermeasures

The countermeasures that could be applied by the Dutch National Police, Law Enforcement Agencies of other countries, and the forum owners in combating cybercrime on the underground forums, will be explained in this section.

2.1 Concrete countermeasures

The following paragraphs analyse the concrete countermeasures the actors can take to mitigate the security issue of cybercriminal markets by infiltrating the forums and gathering information.

As described in previous assignments, the LE agencies, would like to combat cybercriminal markets to reduce illegal trade and to ensure national security. The mentioned strategy and countermeasure is to get in the trust chain by infiltrating the forums and gathering information. The information will be used to identify and prosecute the forum owners, buyers and sellers, aiming to disrupt criminal activities and illegal trade. By taking down forums it makes it harder for buyers and sellers to find each other and to anonymously trade illegal goods. They would have to seek new forums or will distrust the forum transactions overall. This would reduce the total transactions going on in the forums. The LE´s could monitor the cybercriminal markets and activities and track data.

Dutch National Police - Law enforcement agency
One successful example of infiltrating forums to be mentioned is that in June 2017, the Dutch National Police and Public Prosecution Service, together with help from other European institutions, successfully took over and down Hansa Market, a very popular darknet market. They first dismantled the market by arresting the two administrators, then they transferred the infrastructure from Lithuania to Dutch Servers and ran an exact copy of the site. By the end of June they had gathered a large insight to the numbers of sellers and buyers who had traded hard drugs, tracking more than 50,000 transactions of

mostly soft and hard drug sales. This strategy managed to seriously damage the perceived anonymity, credibility and reliability of such marketplaces [1].

Currently, the Dutch National Police runs specialized teams to countermeasure cybercriminal activities. Those teams include IT and cyber security specialists, detectives as well as businesses and knowledge institutions (TNO). In 2017 and 2018 the Dutch National Police aims to hire hundreds of digital specialists [2].

However, it should be considered that cyber criminals are known to take advantage of the digital infrastructure to conduct international cybercrime and to minimize their chance of getting caught. Therefore, the profitability of cybercrime prevails high. International collaboration therefore is often mentioned as an effective response [3]. Due to that, law enforcement agency countermeasures on a European level will be elaborated further in the following paragraph.

Law Enforcement Agencies in Other Countries

The cybercriminal markets are not focused on a single location or language, therefore a collaborative operation between different countries is required for an effective countermeasure approach. When the marketplaces; AlphaBay and Hansa, were taken down this was also a result from a collaboration between the different LE agencies in Europe and the US. The servers of AlphaBay were seized through the collaborative work of authorities in Thailand, Canada, France, Britain and Lithuania. The founder Alexandre Cazes was arrested on behalf of the US in Thailand [4].

However, since there are conflicting interests of countries and their law systems, this countermeasure is quite difficult to collaborate. Therefore, it is a good start to work on an European level and then spread to a global approach. In counter terrorism this is also be done by the European Counter Terrorism Centre (ECTC) that exchange information and conduct analysis [5], which results in less terrorism attacks. Exchange information internationally is a countermeasure that could be applied by the LE agencies in more effective operations to successfully combat cybercriminal markets. The internationally shared information can be used as a starting point to national arrest of sellers and buyers, which is explained in the previous section.

2.1.3 General Intelligence and Security Service

The Dutch general intelligence and security service (AIVD) research terrorism, extremism and espionage. The AIVD is responsible for the domestic security as well as gathering foreign information.

On the domestic security side, AIVD gather information on suspicious internet domains and illegal services that may be interest to law enforcement [6]. The information leads to charges in criminal cases and has helped agents take down illegal digital operations.

On the intelligence service side, the underground forums are used in mining threat intelligence. To give an example, an eastern European cybercriminal attempted to sell an unpatched system vulnerability to a middle eastern government broker. The sale was identified through research on the underground market and is prevented (source). By analyzing threat (actors) in the underground forums, a state can prevent that sensitive information shows up on the underground forums. Threat intelligence analytics, which include prioritizing the threats and indicate the false positives on the underground forums is a countermeasure of the AIVD. The sensitive information leads to the prevention of digital attacks that affect the national security [7].

2.2 Incentives of the actors

There are different motivations to pursue the countermeasures identified in 2.1, which will be summarized in this chapter according to the perspective of the identified actors.

Dutch National Police
We identified in our first paper that from a national government-based security organization perspective, their main interest is to keep illegal goods from entering their country. Furthermore, they are driven to prevent the trade of illegal goods to prevent crime and ensure national security. We also mentioned that according to ENISA, the security and reliability of the internet and electronic communication are a major concern as it is largely affecting economy and society. In the example of AlphaBay, there are several known cases of deaths followed by purchases of drugs through the underground forum, according to the US attorney general. The founder of AlphaBay would have faced charges relating to narcotics distribution, identity theft, money laundering and related crimes. To prevent such incidents are clearly an incentive to combat cybercriminal markets to the Dutch National Police, as well as related law enforcement agencies [4].

Law enforcement agencies in other countries:
The reduction of crime in their own country is certainly a motive for law enforcement agencies. But for successful combat of cybercrime, international collaboration is necessary. A forum may not only focus on a single location. In the example of the takedown of Hansa Market, 10,000 international delivery addresses were collected, 500 of them in the Netherlands. Making it clear that in order to ensure consequences to those sales, Law enforcement agencies of other countries need to collaborate, especially by exchanging such data.

General Intelligence and Security Service
As mentioned in section 2.1.3., the The AIVD is responsible for the domestic security and gathering foreign information. The aim of the AIVD is to protect national security by recognizing timely threats, international political developments and risks that are not directly visible and do research at home and abroad (source). Thus, the incentive of conducting threat intelligence analytics on the underground forums is protecting the national security.

2.3 Externalities

Externalities are a loss (negative) or gain (positive) in the welfare of one party resulting from an activity of another party. In the above countermeasures there exist some externalities that will be explained in this section. The externalities of underground forums mainly come from the harm that is carried out on the society and partly also the economy, resulting from the illegal trades on cybercriminal markets.

There are three different possible external effects of trades of physical and digital goods on underground forums.

1. Harm to the society by the drug abuse resulting from the sales of drugs, those can be deaths as mentioned for the case of AlphaBay, addictions and the costs of healthcare that come with it.
2. Harm to the society by the weapons sold online. If a person gets shot because one illegally bought a weapon from an underground forum this would be a negative externality. For example, in 2016 the 18-year old Ali Sonboly shot nine people dead in Munich, Germany with a weapon he bought on the dark web [8].
3. Harm to the society by distribution of malware bought on the dark web. If one buys malware and distributes it to create for example DDoS attacks, the effect on the user would also be a negative externality. Those could also attack the infrastructure of companies, leading to a negative effect on the economy.

2.4 Cost-benefit distribution of the countermeasure amongst the actors

The following table identifies the distribution of costs and benefits of the identified countermeasures to the actors. As the report by McAfee states, defenders still lack the incentive to do more because they underestimate the risk whilst cybercriminals are incented to do more, because their rate of return is increasing as the market grows [9]. As elaborated in our second assignment, the purpose of the countermeasure strategy to infiltrate the forums is to reduce the illegal drugs-related transactions and result in a positive impact on the society. It can be concluded, that whilst law enforcement organizations hold the costs to infiltrate the forums, the society and economy benefits from their actions. Since they are national organizations, it is their duty to protect the society and economy and their resulting benefit is an outcome of their work.

Table 1: Costs and Benefits Actor Countermeasures

Actor	Countermeasure	Cost	Benefit
Dutch National Police	Inflating forums to arrest forums owners, sellers, and/or buyers.	Manpower with expertise on cybercriminal markets	Reducing digital crime
LE of other countries	Information sharing	Manpower, the involvement of multiple countries makes it difficult to cooperate, thus they need to meet frequently and come to agreements.	Improves international, national and regional security
General Intelligence and Security Service	Conducting threat intelligence analytics	Manpower, conducting analytics is time consuming, because false positives also must be treated.	Ensures national security

3 Metric Variance

In previous assignments, we have defined a metric that measures the number of sales posts in several underground forums per month normalized for total number of internet users. This data was analysed for three different countries: the Netherlands, Germany, and the United States. In these results, shown as Figure 1, indicated that compared to both Germany and the United States, the Netherlands has a higher rate of forum sales posts.

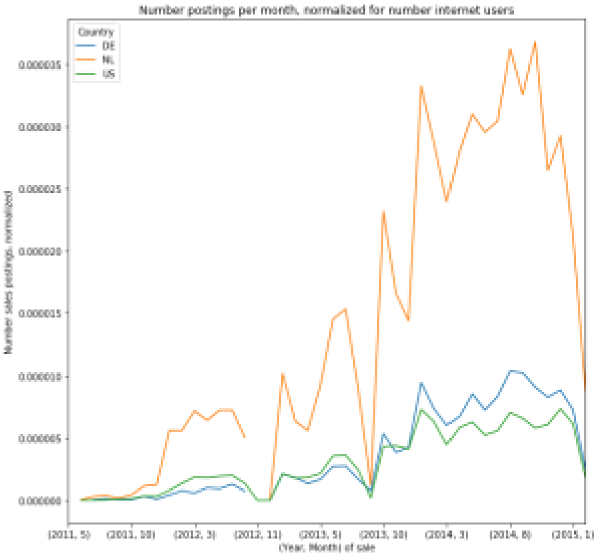

Figure 1: Number postings per month, normalized

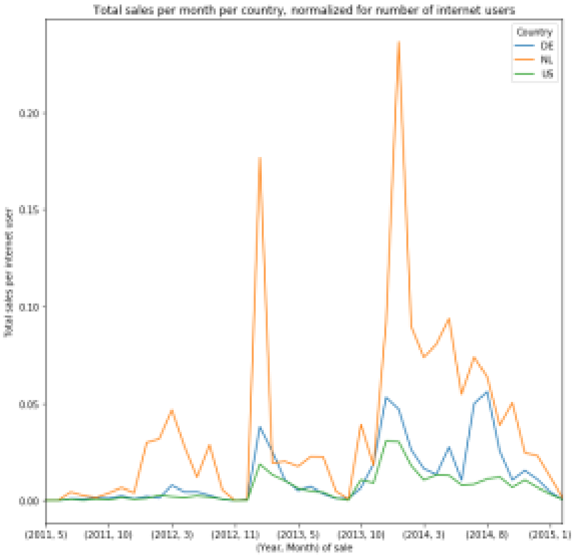

Figure 2: Total sales per month, normalized

However, rate of forum posts may not indicate total sales of goods on these forums. Posts from the Netherlands were shown to have higher total sales value as well, this data also being normalized for total number of internet users. Results for the total sales amount can be found in Figure 2. At the same time, the data for the United States and Germany are much closer in value.

In this section, the variance seen in these related metrics will be explained. First, several factors that may contribute to variance will be explored. Second, one of these factors will be selected for further analysis, including data collection and statistical analysis.

3.1 Factors Potentially Explaining Variance

One factor that may contribute to number of postings on underground forums has already been accounted for in the final version of the metrics described earlier: that of the number of internet users in a country. We initially theorized that because internet connectivity is required to post on cybercriminal forums, it is a contributing factor. By normalizing the metrics for total number of internet users, that factor can be accounted for. In the case of the three countries selected, Germany and the United States have very similar rates of internet use, at 88 percent and 88.5 percent of total population, respectively. At the same time, the Netherlands boosts a 93.7 percent connectivity [10]. These differences served to increase, albeit only by a small amount, the variance between the Netherlands and both the United States and Germany. As a note, this relationship could be studied further in factor analysis by comparing number of posts with countries with more widely varying internet connectivity. However, that is out of scope of this analysis.

After accounting for total number of internet users in a country, there are several other factors that may contribute to the remaining variance. These include:

- Drug usage in a certain country. As there may be different levels of drug usage in different countries, it may be possible that this also affects the number of people from the country trading drugs online.
- Drug and other laws in a country - this will affect what is available for sale in the first place
- The law enforcement budget relative to the size of the country, and especially the budget targeted specifically for cybercrime.
- The priority, focus, or strategy of law enforcement in a country.

3.2 Selected Factor Analysis

Further analysis will be completed for two factors: law enforcement budget and drug usage in a country. These factors lead to the two following hypotheses that will be tested:

H1: A higher law enforcement budget leads directly to lower number of sales on cybercriminal forums.
H2: More drug use in a country leads to higher sales on cybercriminal forums.

Law Enforcement Budget

Monies used to address cybercrime in the United States will be represented by the U.S. Department of Justice (DoJ) budget. This department includes a focus on cybercrime. The table, below, indicates the yearly published budget for the DoJ.

Table 2: DoJ Annual Budgets

Year	**Budget**
2011	27.2 billion [11]
2012	28.2 billion [11]
2013	27.1 billion [12]

2014	27.6 billion [13]

From the Netherlands, the annual budget of the Dutch Ministry of Security and Justice will be used. The information found did not indicate the specific budget allocation to cyber security, possibly attributed to the language barrier between this author and Dutch national government documents.

Table 3: Dutch Ministry of Security and Justice Annual Budget

Year	**Budget**
2011	5.99 billion [14]
2012	11.4 billion [15]
2013	11.2 billion [16]
2014	11.8 billion [17]

There was a restructuring between 2011 and 2012 and the role of the Ministry of Security and Justice expanded to include the National Police, which represents the large increase in budget between those years. For further analysis, we will use an average of the years from 2012 to 2015 for the 2011 number, as the budget has remained relatively constant over that time period. This will give us an approximation of the 2011 budget if it included all elements of the other budgets for the Ministry of Security and Justice.

In Germany, data will be used from the Ministry of the Interior. This ministry is responsible for civilian protection and is the head of several agencies involved in information and technology security. Like the Ministry of Security and Justice in the Netherlands and the Department of Justice in the United States, its role is larger than cybersecurity alone, but information was not found specifically referencing cybersecurity budget.

Table 4: German Ministry of Interior Annual Budget

Year	**Budget**
2011	4.25 billion [18]
2012	4.16 billion [19]
2013	4.06 billion [20]
2014	4.06 billion [21]

The effects of law enforcement budget can be normalized in multiple ways to account for the impact of size of the country under analysis:

- Normalize budget over total GDP of the country
- Normalize budget over population of the country

Statistical analysis will be completed involving this data to determine if there is a statistically significant relationship between law enforcement budget and number of sales on cybercriminal forums. The data is plotted in Figure 3. This chart displays the relationship between total sales on underground forums, normalized for number of internet users, and justice ministry budget, normalized for country population.

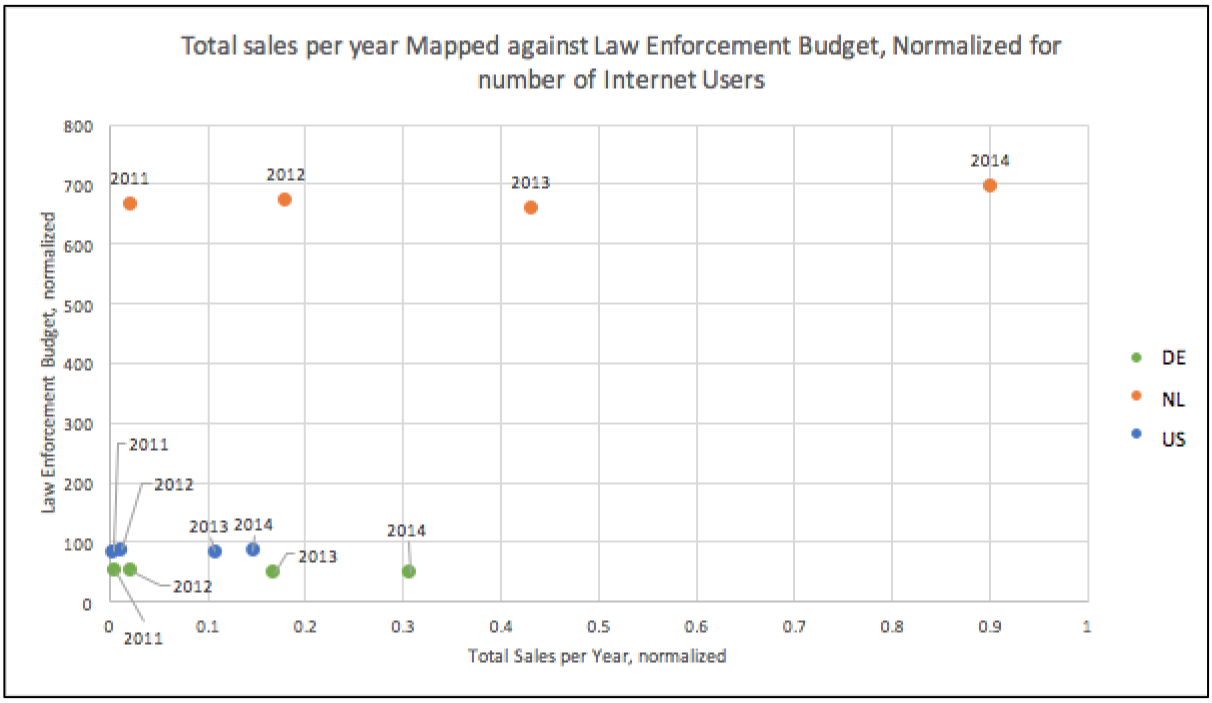

Figure 3: Comparison of Total sales per year on cybercriminal markets and law enforcement budget

Correlation of this data is 0.55, indicating a relatively moderate positive correlation between total sales on cybercriminal forums and justice ministry budget. This information indicates that a larger law enforcement budget does not lead to a reduction in sales on cybercriminal forums. The Netherlands, which has the highest budget for a justice ministry, also has the highest sales on these cybercriminal forums. So, the higher rate of sales on underground forums in the Netherlands is likely attributable to another cause than the amount spent in law enforcement. To refine this analysis further, a more accurate total for the amount each country spends specifically on addressing the issue of sales on cybercriminal forums should be considered.

Drug Use

As the security metric is concerned with drug sales online, this implied that there is a market of the buying and selling of these drugs. Since drug usage can vary per country, it may very well be possible that this explains part of the variance of the transactions online. In this section, we will look at the drug usage of a country as an explanatory factor for the online drug profits made from selling from those countries.

As an indicator for drug usage in a country, one can look at questionnaires such as held by the World Drug Report [22]. Since this data does not encompass all years (data is usually given per 5 years) and is split into different types of drugs, we will look at the data around the year 2014 and specifically for amphetamines. The year was chosen as it contains data on the countries we are interested in and is contained within our data on underground forums.

Amphetamines are chosen as this drug contains data for all countries and is illegal in all of them. This would not be the case for cannabis usage which is legal in the Netherlands. We will assume that the amphetamines category is a proxy variable for the total drug usage in the country. The amphetamine category was selected because specific drug usage might also have an influence on the average drug usage numbers. Furthermore, average numbers of drug use do not exist in this dataset, so additional assumptions would have to be made in combining statistics for multiple categories of drug usage in the analysis.

Table 5 shows the percentages of amphetamine usage under 15- to 65-year9-old people.

Table 5: Amphetamine use for people aged 15 to 65

Country	**Year**	**Drug usage**
Germany	2015	1,10
The Netherlands	2014	1,30
The United States	2014	1,70
Denmark	2013	0,60
Belgium	2013	0,50
Canada	2015	0,25

Looking at the dataset, the following numbers are the total sales (profits) for the sale of stimulants in the year 2014, normalized by the internet users of the specific country:

Table 6: Amphetamine use normalized over total number of internet users

Country	**Profits**
Germany	0,093
The Netherlands	0,166
The United States	0,028
Denmark	0,003
Belgium	0,054
Canada	0,035

To analyse the relation, a linear regression will be used to see what the correlation between the two variables (total sales and drug usage) is. Figure 4 shows the data points and the linear regression line. On X-axis is the drug usage in the country, on the Y-axis the total sales per country normalized for internet users.

Looking at the result of the linear analysis, we can state that the best fitting line between the data points has a slope of 0,039. However, given the P-value of 0.476, this result is not statistically significant. This means we cannot reject the null hypothesis.

Table 7: Results of statistical analysis of drug use correlation to cybercriminal market sales

	Estimate	Standard Error	t-Statistic	P-Value
x	0.0390135	0.0496291	0.786101	0.475763

To conclude, although it appears that the drug usage is correlated with transactions on the cybercriminal markets, the result is not statistically significant. More data is needed to reduce the error of our low data sample. This may turn out to be actually be an explanatory factor.

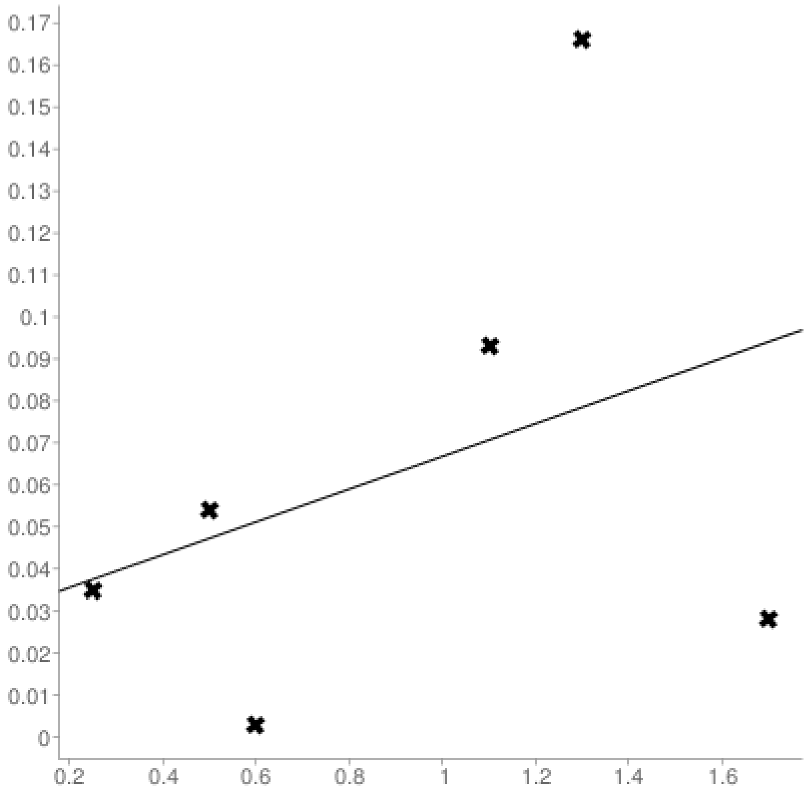

Figure 4: Correlation between drug use and sales on cybercriminal markets

3.3 Limitations and Future Work

With respect to the law enforcement budget, the factor analysis does not account for the influence of multilateral dollars spent, only direct expenditures by a specific country. And as stated earlier, it also does not capture money directly spent on combating the issue of cybercriminal forum sales. To understand the relationship between law enforcement spending and sales on underground forums, more data collection about money spent, both directly and indirectly, to combat cybercriminal forum activity, will be required. Furthermore, the law enforcement factor analysis does not consider potential effects of longer-term law enforcement investments and investigations that do not necessarily have a direct impact on cybercriminal activity reduction.

On the drug usage front, several assumptions were made with regards to the choosing of a year and specific drug. These choices may affect the outcome of the analysis. In the following research, it may be possible to look at a more general drug usage indicator instead of a specific drug. This may be combined with data on more countries to do a better regression analysis as the dataset is currently rather limited.

4 Conclusions

Overall, the main countermeasure identified in this paper is to infiltrate underground forums to combat illegal trades. Related to this countermeasure the Dutch National Police, Law Enforcement agencies of other countries and the General Intelligence and Security Service are involved and are pursuing their interest of gathering and sharing information to prosecute cybercriminal activities. To execute the countermeasure comes with both costs and benefits to those actors.

After identifying relationships and actions of various actors fighting against cybercriminal activity on underground forums, the metric covering total sales on underground forums for a country was analysed to determine factors that may explain variance in the metric for different countries. It was determined that law enforcement budget has little direct influence on total sales on cybercriminal forums. In the case of drug usage, it appears that this may be correlated with the total sales, however this result is not statistically significant. It is suspected that this is due to the few data points used and with more data the error can be reduced.

5 References

[1] Nederlands Politie, “Underground Hansa Market taken over and shut down | politie.nl,” 2017. [Online]. Available: https://www.politie.nl/en/news/2017/july/20/underground-hansa-market-taken-over-and-shut-down.html. [Accessed: 22-Oct-2017].

[2] HSD Foundation, “Ten New Cyber Teams to Combat Cybercrime at Dutch National Police,” *Security Talent*, 13-Jan-2017.

[3] Centraal Planbureau, “Cyber Risk Assessment (CSRA) for the Economy,” Den Haag, 2017.

[4] S. Gibbs and L. Beckett, “Dark web marketplaces AlphaBay and Hansa shut down,” *The Guardian*, 20-Jul-2017.

[5] Europol, “INFORMATION SHARING ON COUNTER TERRORISM IN THE EU HAS REACHED AN ALL-TIME HIGH,” 30-Jan-2017.

[6] C. Bing, “How the FBI relies on dark web intel firms as frontline investigators,” *CyberScoop*, 13-Apr-2017.

[7] Algemene Inlichtingen en Veiligheidsdienst, “Samenwerking,” *Cyberdreiging*, 2017. [Online]. Available: https://www.aivd.nl/onderwerpen/cyberdreiging/samenwerking. [Accessed: 22-Oct-2017].

[8] P. Thompson, “The handgun used by Munich killer was a converted replica which had been bought on the ‘dark web’ and was originally from Slovakia, say investigators,” *Daily Mail*, Munich, 24-Jul-2016.

[9] McAfee, “The Economic Impact of Cybercrime and Cyber Espionage,” 2013.

[10] Internet Live Stats, “Internet Users by Country (2016),” 2016. [Online]. Available: http://www.internetlivestats.com/internet-users-by-country/. [Accessed: 08-Oct-2017].

[11] U.S. Department of Justice, “FY 2012 Budget and Performance Summary,” Washington, D.C., 2012.

[12] U.S. Department of Justice, “FY 2013 Budget and Performance Summary,” Washington, D.C., 2013.

[13] U.S. Department of Justice, “FY 2014 Budget and Performance Summary,” Washington, D.C., 2014.

[14] Tweede Kamer, “Vaststelling begroting Ministerie van Justitie (VI) voor het jaar 2011,” Den Haag, 2011.

[15] Tweede Kamer, “Vaststelling begroting Ministerie van Veiligheid en Justitie (VI) voor het jaar 2012,” Den Haag, 2012.

[16] Tweede Kamer, “Vaststelling begroting Ministerie van Veiligheid en Justitie (VI) voor het jaar 2013,” Den Haag, 2013.

[17] Tweede Kamer, “Vaststelling begroting Ministerie van Veiligheid en Justitie (VI) voor het jaar 2014,” Den Haag, 2014.

[18] Der Bundestag, “Haushaltsgesetz 2011,” Berlin, 2011.

[19] Der Bundestag, “Haushaltsgesetz 2012,” Berlin, 2012.

[20] Der Bundestag, “Haushaltsgesetz 2013,” Berlin, 2013.

[21] Der Bundestag, “Haushaltgesetz 2014,” Berlin, 2014.

[22] United Nations Office on Drugs and Crime, “World Drug Report 2017,” 2017.