

Technical Note: Characterising the online weapons trafficking on cryptomarkets

Rhumorbarbe D., Werner D., Gilliéron Q., Staehli L., Broséus J., Rossy Q.

Ecole des Sciences Criminelles, University of Lausanne, Lausanne, Switzerland.

Abstract

Weapons related webpages from nine cryptomarkets were manually duplicated in February 2016. Information about the listings (i.e. sales proposals) and vendors' profiles were extracted to draw an overview of the actual online trafficking of weapons. Relationships between vendors were also inferred through the analysis of online digital traces and content similarities.

Weapons trafficking is mainly concentrated on two major cryptomarkets. Besides, it accounts for a very small proportion of the illicit trafficking on cryptomarkets compared to the illicit drugs trafficking. Among all weapon related listings (n = 386), firearms only account for approximately 25% of sales proposal since the proportion of non-lethal and melee weapons is important (around 46%). Based on the recorded pseudonyms, a total of 96 vendor profiles were highlighted. Some pseudonyms were encountered on several cryptomarkets, suggesting that some vendors may manage accounts on different markets. This hypothesis was strengthened by comparing pseudonyms to online traces such as PGP keys, images and profiles descriptions. Such a method allowed to estimate more accurately the number of vendors offering weapons across cryptomarkets. Finally, according to the gathered data, the extent of the weapons trafficking on the cryptomarkets appear to be limited compared to other illicit goods.

Keywords: Darknet markets ; Firearms ; Ammunition ; Digital traces ; Forensic intelligence ; Internet traces

1 Introduction

Following the major development of the Internet, communication and information technology provided a broad range of opportunities to diversify illicit trafficking. Cryptomarkets – marketplaces on the Dark web hosting illegal trafficking activities – are among the examples of phenomenon that emerged a few years ago [1]. The first cryptomarket, Silk Road, was mainly dedicated to the trafficking of illicit drugs [2]. Ever since its closure in 2013, many other marketplaces were developed and other illicit goods such as counterfeit products, stolen data, counterfeit or falsified ID documents or firearms, are also offered for sale [3,4]. The media regularly points out the question of firearms trafficking online [5–8], sometimes implying that it accounts for an important part of online illicit trading. However illicit drugs are, by far, the most popular illicit goods proposed on cryptomarkets implying that academic research is essentially focused on the trafficking of this products on cryptomarkets (see for example [9–13]). Most of the research concerning weapons trafficking is about non-online markets [14,15]. Nevertheless, the relationship between weapons trafficking and online trading has been studied, but from very specific perspectives, such as the use of social media in Libya [16]. Thus, to the best of our knowledge, academic literature does not provide much information about weapons trafficking on the Dark web. The only scientific study conducted so far was published in a recent report by the RAND Corporation. It addresses questions such as the size and scope of market, the revenue generated as well as considering both vendor shops and cryptomarkets [17]. The Armory – a market closely related to Silk Road – was opened in 2012 and closed after a few months of activity since it was not generating a lot of transactions [2]. Since then, the pieces of information related to weapons trafficking on the Dark web mostly originate from online news or discussion websites. For example, it seems that the name “The Armory” is still in use, which leads to debates on forums since scam is apparently a common practice in the online firearms trading [18,19]. An interview of a so-called Armory administrator is also available [20], but information from such sources needs to be carefully considered. Indeed, the sensational media aspect of these sources may raise doubts about their reliability compared to properly documented and peer-reviewed academic resources. Despite the limited concrete research about weapons trafficking on the Dark web, their availability is regularly exposed, especially since the recent events in Europe [21]. The aim of this short communication is to explore the extent and the structure of weapons trafficking on the Dark web by drawing an overview of the weapons offered on cryptomarkets in early 2016 through the study of data extracted from these websites.

2 Methodology

Through different sources, a list of active cryptomarkets was established in February 2016. These sources include a bulletin by the NDARC [22], an independent researcher's website [23], the HiddenWiki platform [24] listing various .onion resources and the website DarkNet Stats [25] providing historical statistics about cryptomarket on the Dark web. Accounts were created on 22 marketplaces in order to access their respective listings (i.e. products listed for sale). Among them, 12 included a "Weapons" category and, since three of them had no listings in this category, we worked on a selection of nine cryptomarkets¹. Each selected cryptomarket was accessible via The Onion Router (TOR) and a randomly assigned VPN connection was also established before browsing these websites. The entire webpage – along with its pictures – of each listing appearing in the selected cryptomarkets' "Weapons" category was manually duplicated. The same method was used to duplicate the profile pages of the vendors offering these listings. Each webpage was consulted to extract the relevant information from the listings and profile HTML source codes which constitute the digital traces [26]. For the most important cryptomarkets in terms of weapons related listings (i.e. AlphaBay and Dream Market), Python scripts were used to parse the listings and profile pages and structure the information.

Since the listings classification was not necessarily consistent between cryptomarkets, every listing was classified manually according to its title — and its description when necessary. The listings were distributed between eight categories: *Firearms*, *Ammunition*, *Non-lethal weapons*, *Melee weapons*, *Digital material*, *Explosives and CBRN*, as well as a category *Others* and a category *Custom listings* including the listings specifically requested by a buyer (see Table 1 for examples of product in each category). Listings not related to weapons – probably misclassified at the time of its publication by the vendor – were excluded from further analyses. Finally, possible relationships between vendors were then investigated, either manually by reading the description of the listings and the profile pages, or by using a dedicated software (i.e. IBM i2 Analyst's Notebook 8.9.7). When a public PGP key appeared on a vendor's profile page, it was extracted and imported into a certificate manager to obtain the username and e-mail address given when the key was generated.

3. Results

3.1. Overview of the market

Overall, a total of 425 listings were highlighted. However, 39 of them appeared to be misclassified since they were not belonging to any weapons related category. Table 1 shows the distribution of the 386 remaining listings.

Considering the 386 listings altogether, firearms are not the most frequently offered items on the studied cryptomarkets (around 25%). Non-lethal weapons and melee weapons also account for an important part of the offered items – around 45% altogether

– despite the fact that they may not be so difficult to obtain in several countries. The term "custom" was included in 63 listings' title. For 22 of them, no indication about the offered item could be found in their title, nor in their description – hence their classification as Custom listings. However, the remaining 41 listings were classified more precisely. Interestingly, 39 of them were dedicated to the sale of firearms suggesting that this kind of items might be frequently traded on-demand. Regarding the Digital material category, 15 listings advertised other dedicated websites on the Dark web, among which several links were free while others had to be bought. Three sale proposals were dedicated to compilations of 3D printing files designed for weapons. The eight remaining listings concerned various tutorials or manuals about weapons or bomb making.

Only 10 listings included feedbacks of buyers (6 for firearms, 2 for melee objects, 1 for a non-lethal weapon and 1 for digital material). This results contrast with the usual number of feedbacks left after transactions for other products – i.e. illegal drugs – which is particularly high for prolific vendors [27,10]. Considering the limited numbers of listings and feedbacks, these results suggest that the number of sales is very low.

Table 2 shows that the population of vendors is composed of 96 profiles. Unlike the number of listings, firearms are the category showing the largest number of vendors (35% of the sellers). Both the number of listings and the number of vendors indicate that the illicit trafficking of weapons is essentially concentrated on the two main cryptomarkets, AlphaBay and Dream market, which concentrate more than 70% of the weapons related listings offered by 69 vendors.

¹ The selected markets are: Aflao marketplace (AFL), AlphaBay (ALB), Dr D's multilingual market (DDM), Dream market (DMA), French Darknet (FRE), The Real Deal (TRD), Oasis (OAS), Outlaw market (OUT), Valhalla (aka Silkkitie) (VAL).

Category	Cryptomarket									Total	Example of items
	ALB	DMA	VAL	FRE	DDM	AFL	OUT	TRD	OAS		
Non-lethal weapons	47	32	22		8					28.2% (n = 109)	Pepper sprays, telescopic batons, Taser, stun guns, tactical, self-defence pen
Firearms	66	14	1	5		6	6			25.4% (n = 98)	Semi-automatic pistols, rifles
Melee weapons	35	10	8	3	7				1	16.6% (n = 64)	Knives, blades, shuriken, knuckles
Digital material	15	10		1	1	2		5		8.8% (n = 34)	URL, tutorials, manuals
Ammunition	18	5		9						8.3% (n = 32)	Large variety of calibers from .22 LR to 12 Gauge
Custom listings	1	21								5.7% (n = 22)	Listings specifically created after a buyers' request
Explosives and CBRN	17	3					1			5.4% (n = 21)	Firecrackers, flares, military explosives, explosives devices, CBRN substances
Others	2	2	1		1					1.6% (n = 6)	Ballistic vest
Total	52.1% (n = 201)	25.1% (n = 97)	8.3% (n = 32)	4.7% (n = 18)	4.4% (n = 17)	2.1% (n = 8)	1.8% (n = 7)	1.3% (n = 5)	<0.5% (n = 1)	N = 386	

Table 1. Distribution of the weapons related listings.

There are 23 sellers offering weapons on these two crypto- markets. This represents 68% of the weapons dealers on the studied cryptomarkets. In general, a seller offers listings only in one category. However, on the two largest cryptomarkets, a significant number of vendors propose listings in more than one category (i.e. 41% of vendors on AlphaBay and 7% on Dream Market). Besides, on these cryptomarkets, respectively 66% and 77% of the vendors manage generally more than one listing related to weapons.

The number of vendors illustrated in Table 2 is based on the pseudonyms of vendors (i.e. vendors with 17 different pseudonyms are offering products in the Firearm category on AlphaBay). However, relationships might be highlighted between vendors when considering other information extracted from their profiles or listings. Such results allow to hypothesize that the number of different pseudonyms may not reflect the actual structure of the market since sellers may actually manage more than one account.

Category	Cryptomarket									Total
	ALB	DMA	VAL	FRE	DDM	AFL	OUT	TRD	OAS	
Firearms	17	5	5	1	3	3				34
Non-lethal weapons	14	5		3			1			23
Digital material	9	3	1			2	1		1	17
Melee weapons	8	3	3	3			1	1		19
Ammunition	7	2	2							11
Explosives and CBRN	7	2			1					10
Others	2	2		1			1			6
Custom listings	1	4								5
Total*	49.0% (n=47)	22.9% (n=22)	11.5% (n=11)	5.2% (n=5)	4.2% (n=4)	3.1% (n=3)	2.1% (n=2)	1.0% (n=1)	1.0% (n=1)	N = 96

*The total differs from the sum of each column since a vendor may offer several listings in more than one category.

Table 2. Number of vendors offering weapons related listings by cryptomarket and category.

3.2. Relations between vendor profiles

The combination of pseudonyms, PGP key, e-mail addresses and listings' images as well as profiles' descriptions highlights specific relationship patterns (see Fig. 1). The assumption that the profiles sharing the same pseudonym are managed by the same person – or group of persons – appears to be confirmed since PGP keys and the profiles' descriptions also match. In some cases, images may also strengthen the highlighted connections.

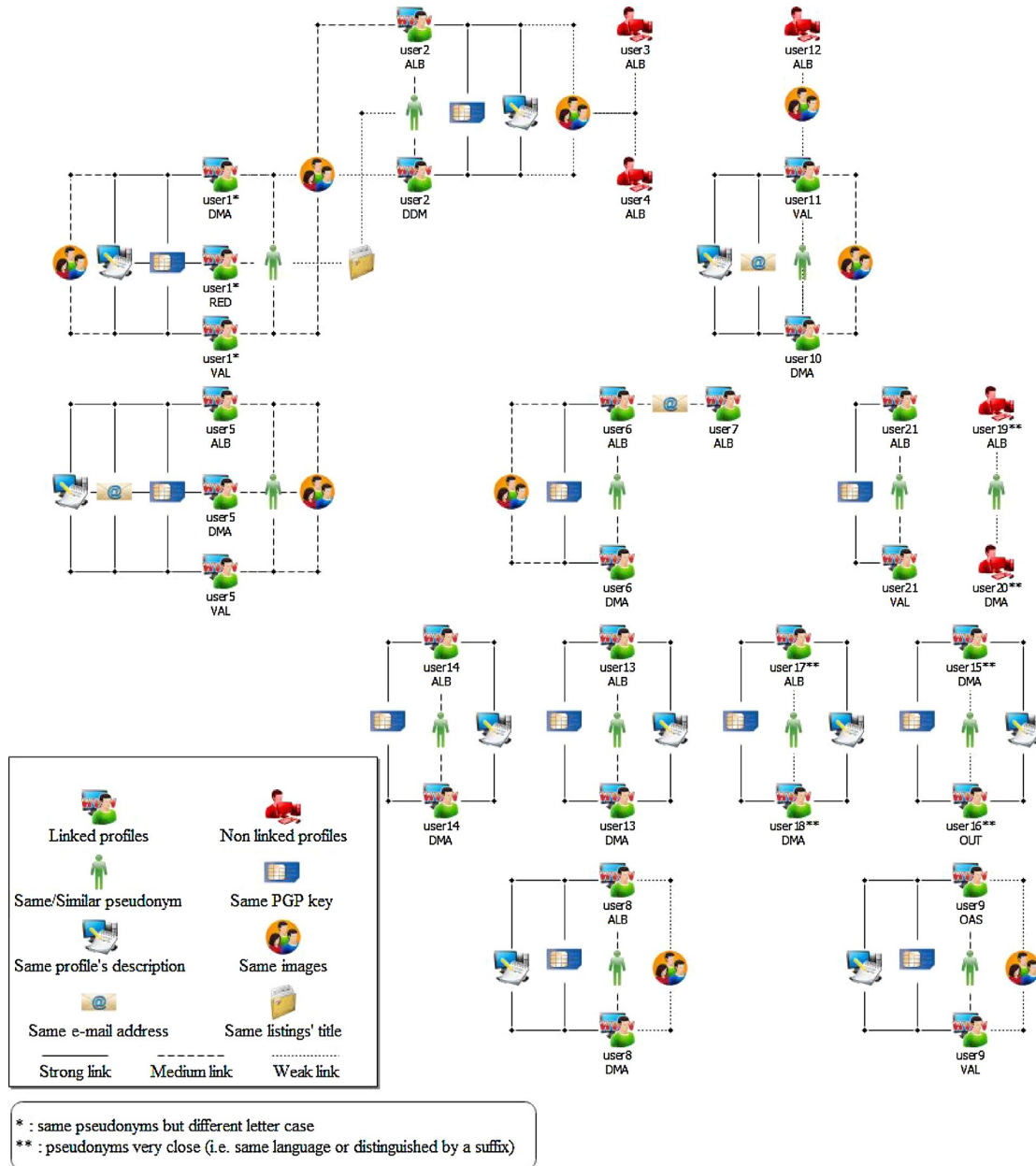


Figure 1. Relationships detected through the analysis of digital traces.

Relationships were highlighted between profiles sharing the same pseudonym, but also for profiles showing very similar pseudonyms (e.g. same pseudonyms but different letter case, pseudonyms in the same language or only distinguished by a suffix). As the pseudonym is directly related to a seller's reputation, identical pseudonyms allow to hypothesise a relationship between accounts. However, two different entities may also choose an identical pseudonym. Such a hypothesis needs other

information to be confirmed. Thus, PGP keys are of particular interest to draw links between vendor profiles since they are used not only to encrypt communication but also as a “proof of identity” [28]. E-mail addresses are retrieved in the descriptions, as well as in the metadata included in the PGP keys (retrieved through a certificate manager). Combining PGP Keys, e-mail addresses included in descriptions, usernames and e-mail addresses extracted from the PGP keys may strengthen pre-established links on the basis of the pseudonyms. Several links were also established on the basis of images sharing similar framing or features in the background. A large majority of these links correspond to the same profile on a cryptomarket.

Type of relation	Number of linked profiles		
	2	3	4
<i>Pseudonym</i>	11	2	
PGP key	9	2	
Description	8	2	
Image	6	1	2
E-mail	2	1	

Table 3. Number of relations highlighted by type of relation.

Table 3 show the number of links – and the number of linked profiles – according to the type of identifying information. Most of the relationships connect two vendor profiles, mainly through PGP keys and profiles descriptions. Links such as images or listings’ title tend to confirm the previously established relationships. It is worth noting that several relationships were established between profiles on the two main cryptomarkets – AlphaBay and Dream market – suggesting that the vendors intend to maximize their selling capacities by building a distribution channel on several markets, while taking care to keep the same identifiers (i.e. pseudonyms, PGP key, profile description) and sometimes the same listings’ images. Besides, cryptomarkets are subjected to disruptions (e.g. law enforcement operations, “exit scam”) impacting the number of vendors across marketplaces [29]. Maintaining a presence on several cryptomarkets may also prevent a loss of profit when a disruption occurs, which has also been observed regarding illicit drug trafficking [10].

4 General discussion and conclusions

The results obtained through this study allow to characterise the weapons trafficking on cryptomarkets. Even if the media emphasize the question of firearms selling on the Dark web, the overview drawn through the study of digital traces shows a relatively small weapons market compared to the illicit drug market. As described in the RAND report, more listings ($n = 811$) were highlighted on the 12 cryptomarkets studied in late 2016. However, this market is still considered as marginal, as illustrated by the calculation of the monthly revenue performed with this data [17]. Furthermore, this market appears to be concentrated on two cryptomarkets and might be extended to other locations on the Dark web, as suggested by the links included in some listings, the dedicated websites highlighted by the RAND report [17] and the interview of The Armory administrator [20]. Besides, the analysis of digital traces extracted from active cryptomarkets suggests that this kind of market is not well-established compared to the illicit drugs market which is built on the reputation and the trustworthiness of vendors, assessed through the feedbacks left by previous buyers [30]. Hence the importance of the low number of feedbacks, what induce suspicion from buyers, especially since scam is frequent regarding this kind of trafficking [18,19]. Buying a firearm on a cryptomarket may also be thought as particularly risky because of mail delivery. A weapon is inevitably more difficult to conceal than illicit drugs sent in small quantities [13,8]. The online trafficking of firearms on cryptomarket is very limited compared to the extent of the traditional firearms trafficking which is characterized by large quantities of seized firearms and ammunition (see for example the data of the United Nation Office on Drugs and Crime [15]). Moreover, the large proportion of weapons not necessarily illegal in every country (i.e. non-lethal and melee weapons) offered on the cryptomarkets could explain the very few sales highlighted in this study [19]. Indeed, it may not be necessary to go through cryptomarkets to buy such items. When considering the relationship between firearms trafficking and communication technologies, the trading through social medias on the Internet – see the recently highlighted example in the Libyan context [16] – seems to be way more important than the trafficking on cryptomarkets.

Among the limitation of this overview, is the fact that finding some sales proposals online does not necessarily imply that a transaction has been completed. Only one of the studied cryptomarkets records the number of sales for a listing, implying that the general assessment regarding transactions should rely on feedbacks, which are universal across cryptomarkets.

Moreover, a listing can be edited (e.g. to change the title, description or categorization) while the number of sales is cumulated. Thus, the number of sales is not necessarily related to the item actually offered on the listing. Besides, only a few feedbacks were recorded. Using feedbacks to infer that a transaction occurred is a common practice to study the revenue of the vendors [31,17]. Indeed, customers are encouraged to leave a feedback after a transaction, it is a way to build trust between buyers and vendors and to prevent scams. The practice is well-known among the cryptomarkets community, especially regarding illicit drugs. The fact that only a few feedbacks were left about weapons listings suggests that only a few transactions for weapons were carried out. Finally, the possibility that these feedbacks are forged cannot be excluded, especially when vendors are starting a business. Thus, a valid evaluation of the number of effectively traded weapons is hazardous, even if our data allow to hypothesise that the extent of weapons trafficking on cryptomarkets is small.

On the other hand, the relatively small number of listings and vendors highlighted with this research is an advantage. Indeed, it allows a thorough study of the relationships between vendors'. Several digital traces turned out to be very informative to confirm linked assumed due to the similarity of vendors' pseudonyms. The results obtained through this research confirmed the potential of combining usernames, emails and PGP keys to highlight distribution channels [28]. Such analysis reveals that assessing the number of vendors according to the number of different pseudonyms might be misleading. On the contrary, the combination of different information may highlight the precise structure and the main actors of a specific trafficking across cryptomarkets. Using images comparison and a certificate manager to obtain the username and e-mail associated with a key may also provide information to improve the study of the structure. Such a process could be applied to other kind of trafficking in order to assess more precisely the number of vendors – or groups of vendors – offering illicit products on cryptomarkets. Finally, the results of this study suggest that firearms trafficking on cryptomarkets is often exaggerated by the media [7]. Firearms trafficking on cryptomarkets appears to be marginal, as evidenced by the number of highlighted sale proposals, vendors and transactions.

References

- [1] J. Martin, *Drugs on the Dark Net — How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*, Palgrave MacMillan, Basingstoke, UK, 2014, pp. 5– 24.
- [2] N. Christin, *Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace*, Proceedings of the 22nd International World Wide Web Conference, Rio de Janeiro, Brazil, 2013, pp. 213–224.
- [3] J. Van Buskirk, S. Naicker, R. Bruno, L. Burns, C. Breen, A. Roxburgh, *Drugs and the Internet Issue 7*, National Drug and Alcohol Research Center, Sydney, 2016 October 2016.
- [4] J. Broséus, D. Rhumorbarbe, M. Morelato, L. Staehli, Q. Rossy, *A geographical analysis of trafficking on a popular darknet market*, *Forensic Sci. Int.* 277 (2017) 88–102.
- [5] DeepDotWeb. *DeepDotWeb. Marketplace directory — The Armory, 2013–2016.* <https://www.deepdotweb.com/marketplace-directory/listing/the-armory-1/>. (Accessed 17 October 2016).
- [6] D. Miller, *Guns, Drugs, 950,000-volt Knuckle Duster Stun Guns, and Assassination Instruction Manuals: The Lethal Products Anyone Can Buy on Just One Website on the 'Dark Net'*, (2015) <http://www.dailymail.co.uk/news/article-2950373/Guns-drugs-950-000-volt-knuckle-duster-stun-guns-assas-sination-instruction-manuals-lethal-products-buy-just-one-website-Dark-Net.html>. (Accessed 22 February 2017).
- [7] B. Byrne, O. Schwartz, *How Criminals Can Buy Guns Illegally on the Dark Net*, (2016) <http://www.vocativ.com/267755/how-criminals-can-buy-guns-illegally-on-the-dark-net/>. (Accessed 22 February 2017).
- [8] B. Vitáris, *Do People Really Buy Weapons from Dark Web Markets?* (2016) <https://www.deepdotweb.com/2016/01/12/do-people-really-buy-weapons-from-dark-web-markets/>. (Accessed 24 February 2017).
- [9] K. Kruithof, J. Aldridge, D. Décary-Héту, M. Sim, E. Dujso, S. Hoorens, *Internet-facilitated Drugs Trade — An Analysis of the Size, Scope and the Role of the Netherlands*, RAND Corporation, Santa Monica, CA; Cambridge, UK, 2017 Available at http://www.rand.org/pubs/research_reports/RR1607.html. (Accessed 10 February 2017).
- [10] K. Soska, N. Christin, *Measuring the longitudinal evolution of the online anonymous marketplace ecosystem*, Proceedings of the 24th USENIX Security Symposium, Washington D.C., USA, 2015, pp. 33–48.
- [11] M.J. Barratt, J. Aldridge, *Drugs cryptomarkets [special issue]*, *Int. J. Drug Policy* 35 (2016) 1–96.

- [12] EMCDDA, The Internet and Drug Markets, Publications Office of the European Union, Luxembourg, 2016 Available at <http://www.emcdda.europa.eu/publications/insights/internet-drug-markets>. (Accessed 10 February 2017).
- [13] D. Rhumorbarbe, L. Staehli, J. Broséus, Q. Rossy, P. Esseiva, Buying drugs on a Darknet market: a better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data, *Forensic Sci. Int.* 267 (2016) 173–182.
- [14] UNODC, The Globalization of Crime — A Transnational Organized Crime Threat Assessment. Chapter 6 — Firearms, United Nations Office on Drugs and Crime, New York, 2010, pp. 129–141 Available at <https://www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html>. (Accessed 17 October 2016).
- [15] UNODC, Study on Firearms 2015 — A Study on the Transnational Nature of and Routes and Modus Operandi Used in Trafficking in Firearms, United Nations Office on Drugs and Crime, Vienna, 2015 160 pp. Available at <http://www.unodc.org/unodc/en/firearms-protocol/global-firearms-trafficking-study.html>. (Accessed 17 October 2016).
- [16] N. Jenzen-Jones, I. McCollum, Web traffick: analysing the online trade of small arms and light weapons in Lybia, Working Paper, Small Arms Survey, Geneva, Switzerland, 2017 Available at <http://www.smallarmssurvey.org/about-us/highlights/2017/highlight-wp26.html>. (Accessed 6 June 2017).
- [17] G. Persi Paoli, J. Aldridge, N. Ryan, R. Warnes, Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web, RAND Corporation, Santa Monica, CA, 2017 Available at https://www.rand.org/pubs/research_reports/RR2091.html. (Accessed 22 November 2017).
- [18] Reddit. Subreddits/r/onions — Comments. Is the armory legit, 2015. https://www.reddit.com/r/onions/comments/2rz0mk/is_the_armory_legit/. (Accessed 17 October 2016).
- [19] L.J. Moriarty, Criminal Justice Technology in the 21st Century, Third Edition, Charles C Thomas Pub Ltd., Springfield, IL, 2017 pp. 228–229.
- [20] S. Matthews, Vocativ. Q&A with a Deep Web Arms Dealer, (2014) <http://www.vocativ.com/tech/bitcoin/q-deep-web-arms-dealer/>. (Accessed 17 October 2016).
- [21] G. Weimann, Terrorist migration to the dark web, *Perspect. Terror.* 10 (3) (2016) 40–44.
- [22] J. Van Buskirk, A. Roxburgh, R. Bruno, L. Burns, Drugs and the Internet Issue 5, National Drug and Alcohol Research Center, Sydney, 2015 October 2015.
- [23] Gwern, Black-market Risks, (2016) <http://www.gwern.net/Black-market%20survival>. (Accessed 24 February 2016).
- [24] The Hidden Wiki. Tor .onion urls directories, 2016. <https://thehiddenwiki.org>. (Accessed 24 February 2016).
- [25] DarkNet Stats. DarkNet Stats, 2016. <https://dnstats.net>. (Accessed 23 February 2016).
- [26] D. Décary-Héту, J. Aldridge, Sifting through the net: monitoring of online offenders by researchers, *Eur. Rev. Org. Crime* 2 (2) (2015) 122–141.
- [27] J. Aldridge, D. Décary-Héту, Not an ‘eBay for Drugs’: The Cryptomarket Silk Road as a Paradigm Shifting Criminal Innovation, Social Science Research Network, 2014 Available at <http://ssrn.com/abstract=2436643>. (Accessed 10 March 2017).
- [28] J. Broséus, D. Rhumorbarbe, C. Mireault, V. Ouellette, F. Crispino, D. Décary-Héту, Studying illicit drug trafficking on Darknet markets: structure and organisation from a Canadian perspective, *Forensic Sci. Int.* 264 (2016) 7–14.
- [29] J. Van Buskirk, R. Bruno, T. Dobbins, C. Breen, L. Burns, S. Naicker, A. Roxburgh, The recovery of online drug markets following law enforcement and other disruptions, *Drug Alcohol Depend.* 173 (2017) 159–162.
- [30] M. Tzanetakis, G. Kamphausen, B. Werse, R. von Laufenberg, The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets, *Int. J. Drug Policy* 35 (2016) 58–68.
- [31] J. Aldridge, D. Décary-Héту, Hidden wholesale: the drug diffusing capacity of online drug cryptomarkets, *Int. J. Drug Policy* 35 (2016) 7–15.