Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market

van Wegberg, Rolf; Verburgh, Thijmen

Publication date
2018

Document Version
Final published version

Published in
Evolution of the Darknet Workshop at the Web Science Conference (WebSci 18)

Citation (APA)
van Wegberg, R., & Verburgh, T. (2018). Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market. In Evolution of the Darknet Workshop at the Web Science Conference (WebSci 18) (pp. 1-5). Association for Computing Machinery (ACM).

Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market*

Rolf van Wegberg
Delft University of Technology / TNO
r.s.vanwegberg@tudelft.nl

Thijmen Verburgh
TNO
thijmen.verburgh@tno.nl

ABSTRACT

In the summer of 2017, an international policing effort - named Operation Bayonet - led by the Federal Bureau of Investigation (FBI) and the Dutch National High Tech Crime Unit (NHTCU) targeted two prominent online anonymous markets. On the one hand, the FBI succeeded in the take-down of AlphaBay, on the other hand the NHTCU took over, operated and shut down Hansa Market. By coordinating these efforts and planning these actions sequentially, both agencies expected users active on AlphaBay to make their way to Hansa Market - which at that moment was in complete control and operated by the NHTCU. To assess the effects of Operation Bayonet, we leverage measurements of the user-base of current market leader, and then safe haven: Dream Market. We investigate the effects of the operation on all newly registered vendors on Dream Market (*n=220*) during and shortly after Operation Bayonet by mapping their individual and historic characteristics to discern migration patterns and changes in vendor behavior.

Compared to 'simple' take-downs, like the AlphaBay take-down, the effects of the Hansa Market shut down on vendors seem remarkably different. Vendors do not just simply move on after the Hansa Market shutdown. Few simply migrate, some take precautions like changing their username and/or PGP-key, but many start over with a clean slate - erasing their past reputation completely - and are truly 'Lost in the Dream'.

CCS CONCEPTS

• **Security and privacy → Economics of security and privacy**;

KEYWORDS

Online anonymous markets, Police interventions, Operation Bayonet, Crime displacement

ACM Reference Format:
Rolf van Wegberg and Thijmen Verburgh. 2018. Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market. In *Proceedings of Workshop on the Evolution of the Darknet (WEBSCI).* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

In a coordinated effort, two leading online anonymous markets - AlphaBay and Hansa Market - were taken down by the Federal Bureau of Investigation (FBI) and the Dutch National High Tech Crime Unit (NHTCU) during Operation Bayonet [1]. The FBI managed to take down AlphaBay, while the NHTCU infiltrated and operated Hansa market for nearly a month as administrator and thereafter shut down Hansa Market for good. The unexpected and unannounced implosion of AlphaBay, left buyers and vendors in uncertainty and despair as the FBI - contrary to previous take-downs - remained completely silent about their involvement. Many AlphaBay users sought refuge to Hansa Market - which at that moment was operated by the NHTCU. Hence, the police agencies were in a perfect position to not only disrupt the ecosystem by creating distrust amongst users on these anonymous markets, but also collect valuable data on thousands of them. As the police agencies changed their intervention strategy distinctively, the question arises: did this intervention in turn result in a change in user strategy? Can we identify changes in behavior of vendors forced to migrate in the aftermath of Operation Bayonet?

In this paper we use measurements of the user-base of Dream Market to investigate the effects of the operation on all newly registered vendors on Dream Market (*n=220*) during and shortly after Operation Bayonet. To measure changes in user behavior, we identify where these vendors migrated from and observe changes in their 'appearance', i.e. a change in username or PGP-key. First however, we briefly look into Operation Bayonet itself.

In that operation, the FBI took down Alphabay on July 5th 2017 and the Dutch police forces took down Hansa on July 21st 2017, while informing the world that they had been in full control of the site for 27 days. [2] In a bold move, the NHTCU had also been able to turn off the encryption of personal messages on Hansa, which allowed them to monitor personal information, like street-addresses, passing through the site. On the day of the Hansa take-down, the FBI announced to be responsible for the take-down of AlphaBay a month before. The FBI were able to seize multiple AlphaBay servers and arrest Alexandre Cazes - allegedly one of the administrators of Alphabay, known as Alpha02 - on July 5th 2017 in Thailand. Meanwhile, the planning of the Hansa take-down started long before and originated from a tip about the server's location. This tip led to a yearlong investigation, ultimately ending in the arrest of the administrators in Germany and the police being able to mirror the confiscated servers in Lithuania.

[*] Parts of the analysis in this paper have been previously made public through a TNO-factsheet outlining the initial findings in this paper.

[1] See https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

[2] See https://www.politie.nl/en/news/2017/july/20/underground-hansa-market-taken-over-and-shut-down.html and https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

WEBSCI, 2018
© 2018 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

2 FROM TAKE-DOWNS TO INFILTRATION

Leveraging the insights of previous take-downs - like the Silk Road 1.0 and 2.0 cases - we know that the typical result of a 'simple' take-down is that users migrate to other markets and simply carry on with their illegal business [6]. Researchers from Carnegie Mellon University [10] studied the overall trade-volume on online anonymous markets in the ecosystem before, during and after both the Silk Road take-downs. Although the trade-volumes changed after both take-downs, they increased instead of decreased, reflecting a ecosystem that not merely recovers from an intervention but continues to grow regardless. Noteworthy are the insights of the sociologist Ladegaard [8] linking the media coverage of both take-downs to this increased sales-volume. Aside from any multiplication effect by extensive media coverage, take-downs often result in a so-called waterbed-effect, or the displacement of crime. In that sense we can draw upon the insights from crime displacement theory in the physical world and assess them in a digital environment [2]. Previously, Decary-Hetu [4] studied the effectiveness of interventions aimed at the warez scene - the hacker community specialized in distributing pirated material, like pirated movies - and concluded that crime displacement was one of the primary results of these interventions. Police agencies nowadays seem determined however, to break with this tradition and changed their intervention strategies to tackle precisely this unwanted side-effect.

As Law Enforcement Agencies (LEA) became aware of the existence of online anonymous markets as a prominent meeting and trading place for criminals [9], several operations were launched to shut down this innovative criminal business. There are several ways the police has taken action [7]. Foremost, they have used traditional investigation methods, such as infiltration on the marketplace and intercepting physical packages. Increasingly, this traditional policing is combined with technical investigation methods, such as pursuing a strategy to triangulate server locations of these markets. In the last decade, two 'successful' and major operations can be identified, namely Operation Marco Polo and Operation Onymous. Operation Marco Polo started in 2011 and ultimately resulted in the take-down of Silk Road 1.0 and the arrest of its main administrator Ross Ullbricht - who was arrested while being logged in on Silk Road as 'Dread Pirate Roberts' - in 2013. [3] Over the course of the operation, LEA executed multiple (pseudo)buys and infiltrated the marketplace by using new and flipped user-accounts. They achieved the take-down by a combination of technical advances and traditional policing, such as making use of their infiltrated positions. Less detailed information is available on Operation Onymous - which was a coordinated operation between police forces from 17 countries coordinated by Europol in 2014. It resulted in the take-down of large numbers of sites - some being online anonymous markets. At least the markets Cloud 9, Hydra & Silk Road 2.0 were shut down by Operation Onymous. [4]

Although these interventions are perceived as impactful, it is important to know exactly which type of impact interventions specifically aimed at online anonymous markets, have. This would allow LEA to not only review past interventions, but also to create evidence-based interventions. Before deciding on any course of action, LEA can identify and weigh the favorable and less-favorable effects of specific interventions. These foreseeable effects of potential future interventions contribute to an informed decision how and where to successfully intervene to achieve the desired effect. In order to develop such evidence-based interventions, there is a need for a methodology in measuring the effects of interventions. Success in one area - taking down an online anonymous market - might lead to less success in another: actually lowering crime across the ecosystem. This dilemma in online interventions is reflected in the balancing act between aiming for a desistance effect, in which vendors would stop selling and the criminal activity ceases to exist, and showing force by taking down markets and just see displacement of crime taking place. Crime displacement is an effect that is frequently encountered in policing online crime [4]. In the case of online anonymous markets, it can be described as buyers and vendors moving on from one marketplace to the next, if one becomes unavailable - due to police interventions or an exit-scam [5]. Ironically, given the anonymous yet transparent nature of these markets, measuring this displacement has become easier as well. Current methodologies investigating the effect of online anonymous market interventions primarily look into the number of listings, number of users and sales-volume in order to determine effect sizes. This paper however, applies a new methodology to measure the impact of the different aspects of Operation Bayonet by not only looking into crime displacement, but also capturing specific vendor migration patterns and changes in vendor behavior during and immediately after the intervention.

3 MEASUREMENTS ON DREAM MARKET

To observe the initial effects - in terms of crime displacement - of Operation Bayonet, we study the user-base of another market: Dream Market, who became market leader right after Operation Bayonet. This market was established at the end of 2013 and has grown steadily ever since, making it a suitable market for our analysis as we can lever a baseline of pre Operation Bayonet operation.

From 2014 onwards we have scraped the forum of Dream Market, extracting - next to forum posts - its (number of) users. We made daily scrapes between January 2014 and September 2017. We use the (number of) users on the Dream Market forum as a proxy for the (number of) users in the Dream Market community. Being active on a forum is not compulsory for trading on a market - so not all vendors are automatically registered on the forum - but is rather incentivized by the nature of online anonymous markets. Building a solid and verifiable reputation as a respectable vendor or honest buyer on a market, goes hand in hand with being active on a forum [5]. Specifically for vendors, reputation is an important part of doing business on an anonymous market. Dealing with all sorts of questions on the forum - ranging from product requests, to mishandled or seized shipments of drugs - be it addressed to individual vendors or not, helps grow ones reputation. That way, vendors apply similar tactics as in the legal economy: companies use approachable 'helpdesks' to increase the brand's reputation. Moreover, users connect their status on the market, to their status

[3] See https://krebsonsecurity.com/2013/10/feds-take-down-online-fraud-bazaar-silk-road-arrest-alleged-mastermind/

[4] See https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network

[5] An exit-scam is the sudden shut down of a market by its administrators, who take off with all funds in escrow. This could be severial millions worth of funds.

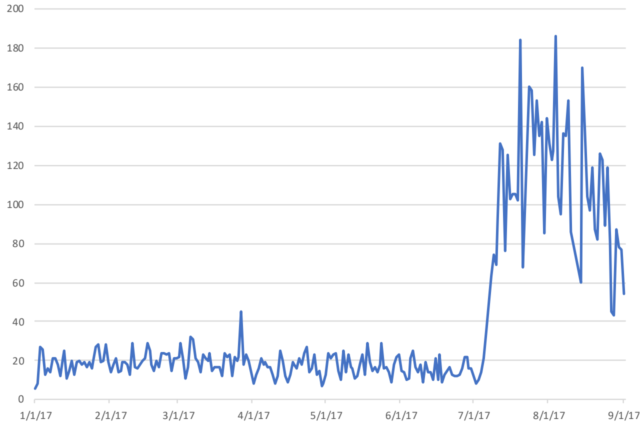

Figure 1: Daily new users on Dream Market in 2017

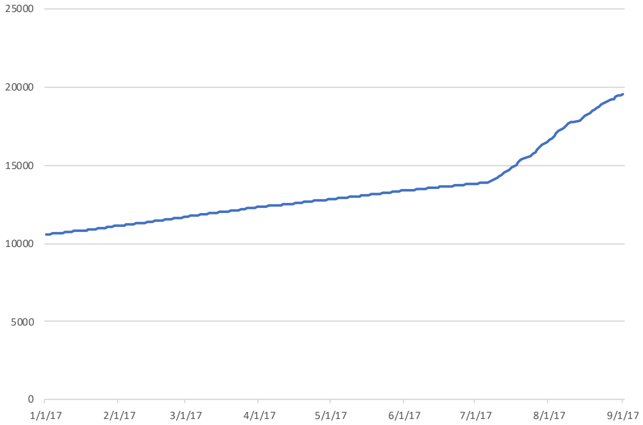

Figure 2: Users on Dream Market in 2017

on the forum, i.e. a vendor on the market is recognizable as such on the forum. Meaning that we can discriminate between vendors and buyers via their respective status on the forum.

In each snapshot, i.e. scrape, we collect - among other things - the usernames and registration dates of active buyers and vendors from their individual user pages. Note that acquiring accurate registration dates - and not derived from first seen vendor activity in a certain scrape - is only possible through forums. Parsing the information on these pages gives us an aggregate of the total number of users. We can calculate the daily influx of users by taking the registration date as a time stamp and cumulate all new registrations on a certain date. The accuracy of the scraped information does not hinge completely on regular interval scrapes - which can prove difficult some days - because we can collect information, e.g. the registration date of a user, in retrospect from the individual user page. All in all, we are confident that our scraped data gives an accurate picture of the lower bound of users active in the Dream Market community between January 2014 and September 2017.

At the beginning of 2017 we measured that on Dream Market around 10,000 users were active. In terms of daily influx in the year 2017, Dream Market saw about 20 new users registering per day. That changed significantly from July 2017 onwards. From that moment on, Dream Market started taking in more than 60 new users per day, with some days where even 180 new users registered (Figure 1). As a consequence, Dream Market nearly doubled its user base to almost 20,000 users in only nine months' time (Figure 2). Looking at the exact timing of this sudden rise in daily influx in July 2017, we can state that Operation Bayonet - where AlphaBay went down on July 4th 2017 and Hansa Market was shut down on July 20th 2017 - was probably the direct cause. Due to this rise in new users, Dream Market became the leading online anonymous market right after the operation. [6]

However, looking at the user-base of AlphaBay - according to US Attorney General Jeff Sessions over 40,000 vendors were selling to more than 200,000 buyers [7] - and Hansa Market - which had marginal presence in the ecosystem - prior to their take-down, certainly not all users migrated to Dream Market. Yet, the increase of users is consistent with earlier take-down effects. To properly assess the detailed effects of Operation Bayonet on vendors migrating to Dream Market, we specifically look at all newly registered vendors on Dream Market (*n=220*) between July 1st and September 1st 2017. We investigate their background in terms of earlier presence on online anonymous markets. That way, we can identify specifics in crime displacement, i.e. vendor migration patterns to Dream Market, during and shortly after Operation Bayonet. Given the nature of the Hansa Market infiltration and take-down, we expect less linkable vendor migration from Hansa Market to Dream Market.

4 MIGRATION PATTERNS

After obtaining the usernames of all vendors (*n=220*) that registered on Dream Market between July 1st and September 1st 2017, we used online anonymous market search engine *Grams*[8] to map specific (historic) characteristics of these vendors, for instance on which markets they were previously active. The search engine allowed 'informed customers' to track down vendors of products and services to assess their track record using previous sales and accompanied feedback. In turn, this allowed us to investigate the newly registered vendors on Dream Market and analyze their past and present behavior, i.e. their behavior before and after the intervention. *Grams* made it possible to search for vendors using either their username or PGP-key. For each vendor we executed a *Grams*-search with their Dream Market-username. The output of this search always was at least the combination 'username-market' of that user on Dream Market. Hence, we were able to validate our initial assumption that all 220 newly registered vendors were indeed active on the market and were not merely active on the forum. Next, the output of Grams would show us any other 'username-market' combinations that either use the same username or are connected through the same unique PGP-key. That way, we determined where the vendor migrated from: AlphaBay, Hansa Market, or that the vendor was active on both markets before migrating to Dream Market.

[6] See https://dnstats.net
[7] See https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

[8] On December 12th 2017 the administrator of Grams placed a message on Reddit announcing the discontinuation of Grams later that week. Fortunately, we finished our analysis before *Grams* became unavailable.

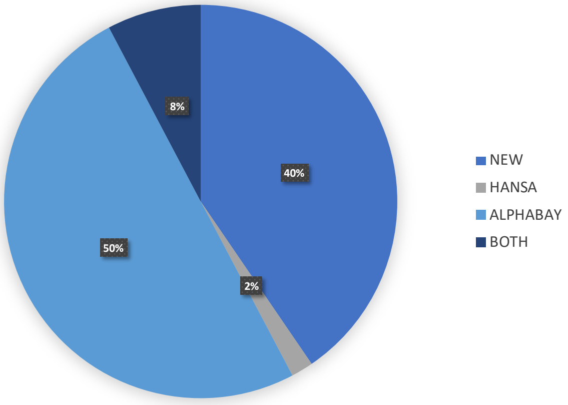

Figure 3: Breakdown of newly registered vendors on Dream Market (*n=220*)

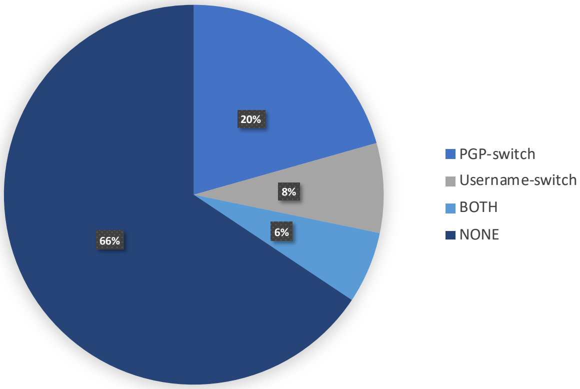

Figure 4: Breakdown of evasive strategies of migrated vendors to Dream Market (*n=131*)

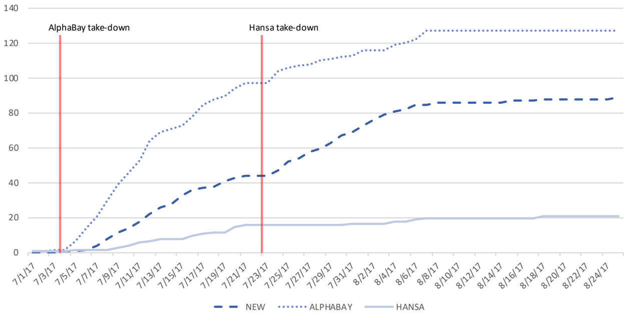

Figure 5: Cumulative number of newly registered vendors on Dream Market per origin on date (*n=220*)

Figure 3 shows the breakdown of newly registered vendors on Dream Market. First, we can observe that many vendors migrating to Dream Market came from AlphaBay (40%). Curiously, the migration path from Hansa Market to Dream Market is near absent (2%). The latter is particularly interesting given the one major difference between the two take-downs in Operation Bayonet. Where AlphaBay was a take-down like many other, the Hansa take-down followed on nearly a month of complete control. This breakdown shows that there is a striking difference in migration patterns directly after that take-down. Second and rather unexpected, many of the newly registered vendors are completely 'new' and are without any previous reputation or track-record. This can mean two things: 1) real 'new' vendors picked this exact moment to start their online business and chose to do so on Dream Market or 2) vendors that were previously active on AlphaBay, Hansa or other markets took the rather drastic measure to completely start over - throwing away months or even years' worth of reputation and changing their identity by switching username and PGP-key. To investigate the effects of Operation Bayonet further, we look closer at the migrated vendors, so the 131 users that were active on AlphaBay, Hansa or both, as the question arises: did they put any effort into evasive measures after both take-downs?

5 VENDOR BEHAVIOR

To measure changes in vendor behavior in the group of migrated vendors (*n=131*) we turn to the online anonymous market search engine *Grams* again. Using the search engine, we identified vendors that changed usernames, but stuck to their PGP-key, or vendors that stuck to their username but changed PGP-keys. Because of the fact *Grams* uses both usernames and PGP-key to connect vendors, we leverage this output to see if the Dream Market username is the same as other usernames on other markets but has a different PGP-key. Or that the Dream Market username is different from earlier used usernames, but all have the same PGP-key connected to it. Figure 4 shows that two-thirds of the migrated users did not take any noticeable evasive measures. However, we can see that respectively 20% of users changed their PGP-keys, 8% changed their usernames and 6% did both. We were able to identify a handful of newly registered vendors on Dream Market who tried to start over completely - by changing both their username and PGP-key - but failed in some respect. For instance, they used the same e-mail address to register their new PGP-key as they used to register their old ones. Allowing us to deduce that these vendors at least tried to start over completely and provided us with the understanding that others might have successfully did so.

Both the number of evasive measures and the share of 'new' vendors, are a strong indicator that this intervention has more than meets the eye. Knowing that a username and PGP-key are valuable assets in an anonymized setting - like underground markets - users do not change PGP-keys or usernames unless they really have to [1, 5]. Looking beyond the influx of users to Dream Market, one could see a scenario of a 'panicking' community or at least a community wherein vendors feel forced try to change their identity, be it with a new username, new PGP-key or even start over completely.

6 LONGITUDINAL ANALYSIS

We can assess this scenario even further by looking at these elements, i.e. the migration pattern and evasion measures, longitudinally. That way, we can see if the behavior of these vendors after the AlphaBay take-down differs from the Hansa take-down - where the police infiltrated, disabled encryption on personal messages

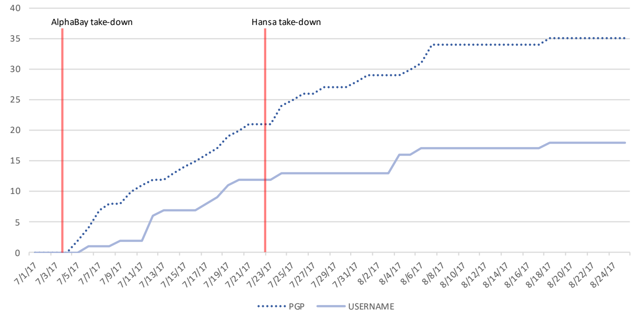

Figure 6: Cumulative number of evasive measures by newly registered vendors on Dream Market on date (*n=53*)

and could see everything being said and done for three weeks without arising any suspicion. We expect that a 'simple' take-down would result in similar vendor behavior as reported by earlier studies [3, 6, 10]: migrate and carry-on. As the Hansa Market take-down coincided with the public statement of NHTCU that they operated the market for more than three weeks, and have gathered information about the true identity of potentially thousands of users, we hypothesize that this would result in a different vendor response compared to 'simple' take-downs.

Figure 5 shows the cumulative number of newly registered vendors during our period of analysis in July and August 2017. Noticeably, the influx of AlphaBay migrants starts steep - right after the take-down on July 4th. The number of AlphaBay migrants stays relatively stable from the last week of July onwards. Even more interestingly, the number of 'new' vendors increases whilst the number of Hansa migrants stagnates at precisely the same time, namely around the 22nd of July: right after the Hansa Market take-down. This again builds to the scenario of a community seeking refuge to completely new identities, right after the Hansa take-down.

Looking at the evasive measures (Figure 6), this scenario finds more support. Right after the Hansa take-down, the username-switch stagnates. In turn, migrating vendors apparently turn to a more drastic measure: starting over.

7 DISCUSSION

In this paper we presented a new methodology to discern the different effect-types of online anonymous markets interventions. By taking into account the (longitudinal) changes in behavior on a vendor-level, i.e. specific migration patterns and changing vendor behavior - we were able to see beyond the waterbed-effect for the first time.

We have to stress however, that the methodology and measurements in this paper have some limitations. First, our methodology is partly based on a third-party search engine to make connections between vendors across markets. Leaning on that defunct service to identify changing vendor behavior, in terms of migration patterns and evasive measures, means that replicating our findings - using that same service - has become rather impossible. Second, our measurements contain data on users of the Dream Market forum - not the market - for a long period of time before, but only depict a relatively short window after, Operation Bayonet. This could mean that we only witness the first and not final effects of this intervention. Third, as we employ a novel methodology to measure changes in vendor behavior, we cannot compare these results one-on-one with previous research efforts into police interventions. Hence, more research efforts therefore should be taken to a) investigate the long-term effects of this intervention in terms of crime displacement and changes in vendor behavior, b) how to identify migration patterns of vendors across markets and c) leveraging the before mentioned research efforts to investigate previous and/or future interventions using this novel methodology to better compare the effects of these respective operations.

Notwithstanding these limitations, if we apply our methodology to measure the effects of Operation Bayonet on migrating vendors to Dream Market, we see the first signs of a game-changing police intervention. Compared to 'simple' take-downs, like the AlphaBay take-down, the Hansa Market take-down stands out - in a positive way the police might add, as users do not just move along after the Hansa Market shutdown. Few simply migrate, some take evasive measure - like changing their username and/or PGP-key - but many start with a clean slate on Dream Market. This may sound as a minor detail, but the opposite is the case. When a vendor starts over he/she loses their track-record, reputation and customer-base. Like a Michelin star restaurant moving cities, whilst changing its name, website and phone-number: nobody will recognize the fancy restaurant from before and the chef will likely be forced to start (re)building a reputation from scratch. We have to see if the effects of this innovative intervention hold in the long run, but for now the initial effects are remarkable in the light of earlier interventions aimed at online anonymous markets.

REFERENCES

[1] Judith Aldridge and Rebecca Askew. 2017. Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy* 41 (2017), 101–109. https://doi.org/10.1016/j.drugpo.2016.10.010

[2] Kj Kate J. Bowers and Shane D. Sd Johnson. 2003. Measuring the geographical displacement of crime. *Journal of Quantitative Criminology* 19, 3 (2003), 275–302. https://doi.org/10.1023/A:1024909009240

[3] Nicolas Christin. 2013. Traveling the silk road: a measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web*. 213–224. https://doi.org/10.1145/2488388.2488408

[4] David Décary-Hétu. 2014. Police Operations 3.0: On the Impact and Policy Implications of Police Operations on the Warez Scene. *Policy & Internet* 6, 3 (2014), 315–340. https://doi.org/10.1002/1944-2866.POI369

[5] David Décary-Hétu and Benoit Dupont. 2013. Reputation in a dark network of online criminals. *Global Crime* 14, 2-3 (2013), 175–196. https://doi.org/10.1080/17440572.2013.801015

[6] D. Décary-Hétu and L. Giommoni. 2017. Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change* 67, 1 (2 2017), 55–75. https://doi.org/10.1007/s10611-016-9644-4

[7] Alice Hutchings and Thomas J. Holt. 2017. The online stolen data market: disruption and intervention approaches. *Global Crime* 18, 1 (2017), 11–30. https://doi.org/10.1080/17440572.2016.1197123

[8] Isak Ladegaard. 2017. We Know Where You Are, What You Are Doing and We Will Catch You. *The British Journal of Criminology* (2017). https://doi.org/10.1093/bjc/azx021

[9] Rutger Leukfeldt, Edward Kleemans, and Wouter Stol. 2017. The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. *American Behavioral Scientist* (2017), 000276421773426. https://doi.org/10.1177/0002764217734267

[10] Kyle Soska and Nicolas Christin. 2015. Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *24th USENIX Security Symposium (USENIX Security 15)* (2015), 33–48. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/soska