oiioiioii Oxford Internet Institute
oiioiioii University of Oxford
oiioiioii

UNIVERSITY OF
OXFORD

The Economic Geography of Darknet Marketplaces

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

www.oii.ox.ac.uk/research/projects/economic-geog-darknet
@OiiDarknet

September 8, 2017

The "Darknet": Anonymisation with Tor

oiioiioii Oxford Internet Institute
oiioiioii University of Oxford
oiioiioii

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
2

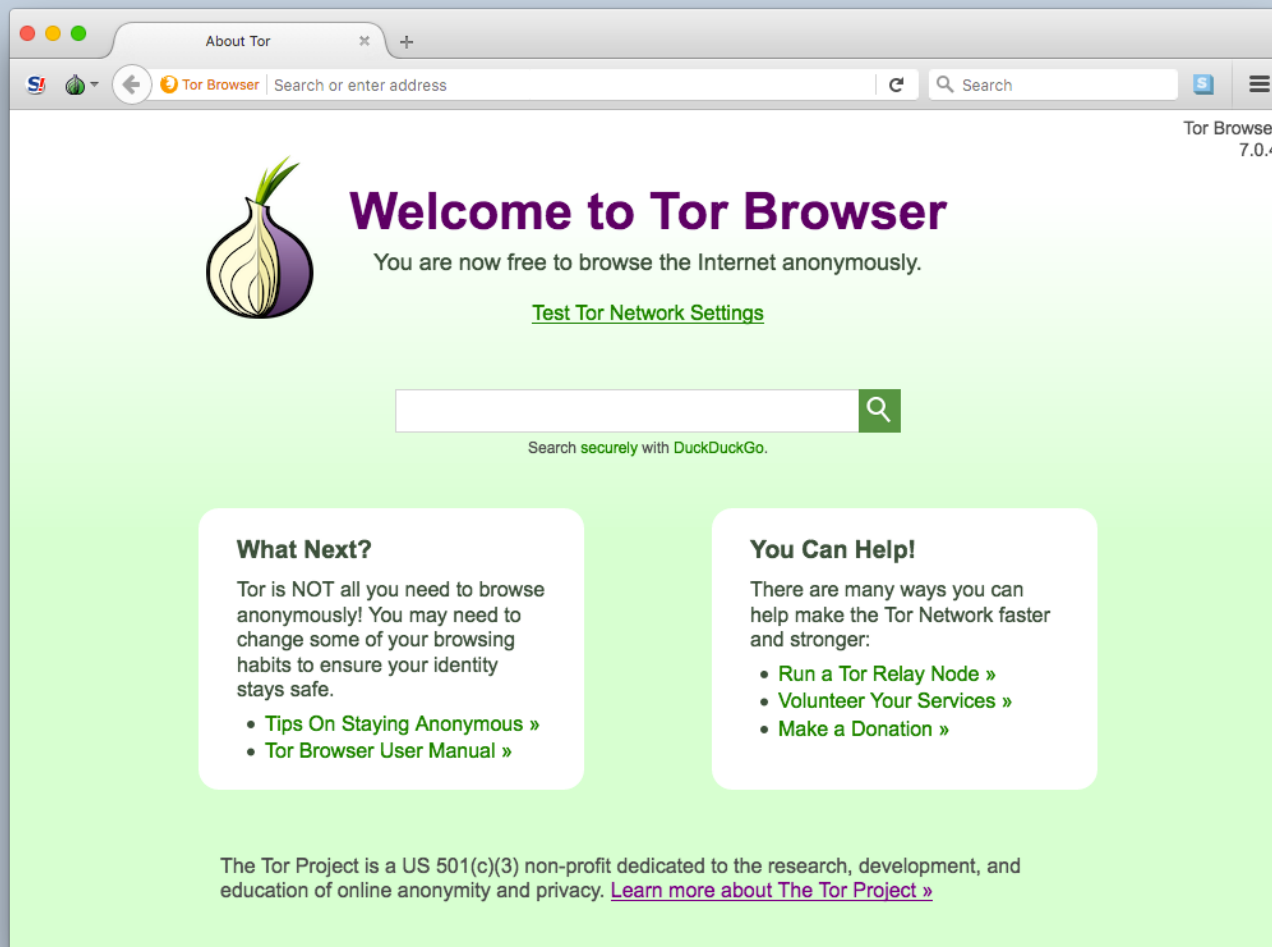# Darknet Markets: Platforms for Illicit Trades

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
3

The Oxford Internet Institute (OII) at the University of Oxford

https://www.oii.ox.ac.uk/

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
4
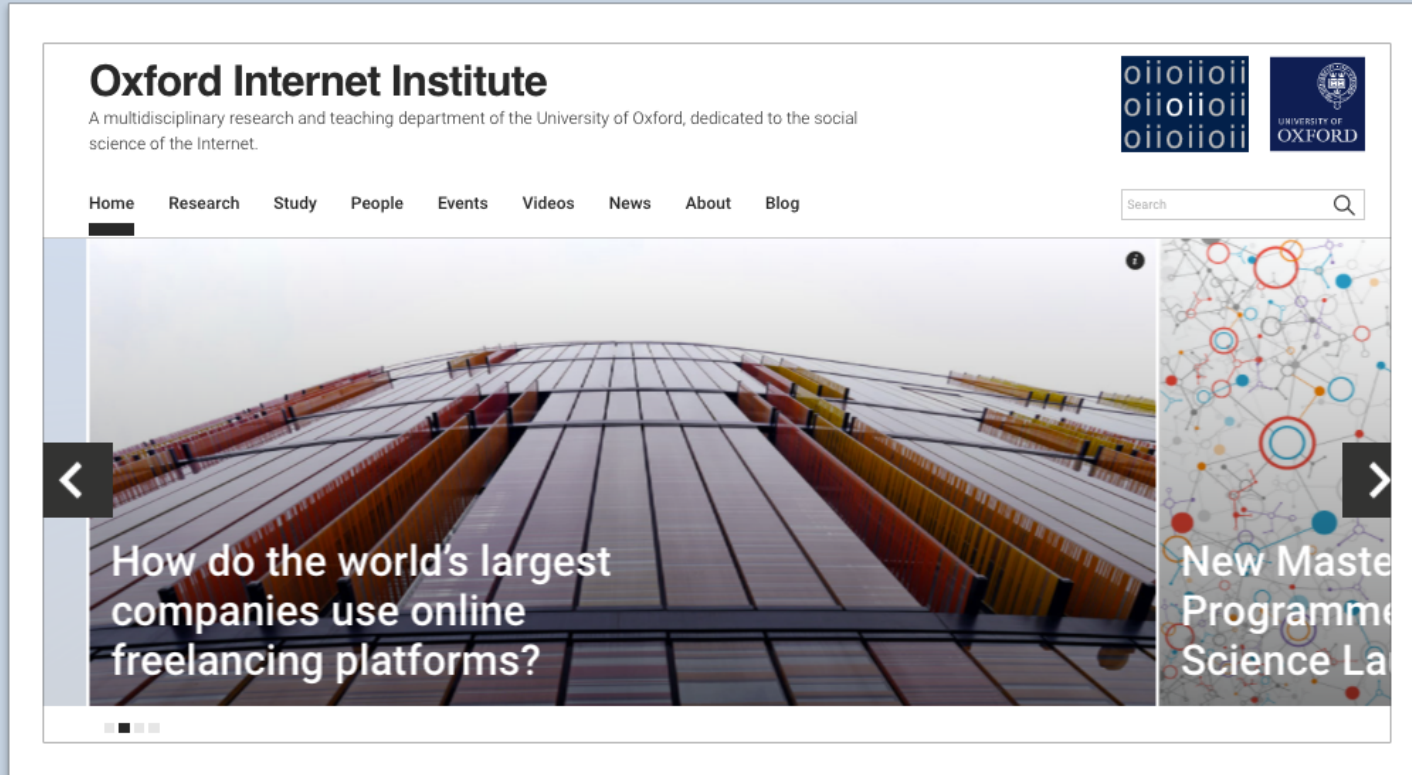
What is the Economic Geography of Darknet Markets?

- Economic Geography: what drives economic activity in certain places but not others?

- For example, we might want to ask:
    - What is the number of heroin sellers in every country?
    - What is the geography of the online weapons trade?
    - How widely distributed is the trade of new psychoactive substances (NPS)?

- We are **now building a reusable data set** at the country level
- Mapping, visualising, analysing the data
- **We plan to open it up to the public!**

Our Research Approach

- Primarily we seek to understand the social phenomenon.

- This is **independent academic research**, we have no ties to law enforcement or platform operators. The project is funded by Google and the Alan Turing Institute, who do not influence the work.

- This is **data-centric** and **quantitative** work, rather than ethnographic. Observational studies, based on readily-available public information. Primarily we scrape catalogue and trading data at large scale, and then analyse and visualise it.

- **We are not collecting information about individuals.** Can't see individual trades, only information that is shown on market platforms such as product metadata, buyer feedback, and vendor profiles.

oiioiioii Oxford Internet Institute
oiioiioii University of Oxford
oiioiioii
oiioiioii

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
6

A Survey of the Largest Markets

A Survey of the Largest Markets

#	Market	Address	Type	Live?	Scraper done?	Parser done?	Needs login?	Needs invite?	Sequential IDs?	Full listings?	Stable ordering?	Listing dates?	Sales counter?	Feedback dates?	(Vendor-fb counter?)	Stated	%	Actual	Sta/Act	Language?	Comments
1			Market	y	y	y	y		y	n	y	y	y	y	(y)	347,081	58.74%	136,152	39%		Navigation counters seem to i
2			Market	y			y		n	y	n	n	n	y	y	86,366	14.62%				Hard to scrape: no sequential
3			Market	y	y	y	y		n	y	y	n	n	y	y	51,381	8.70%	8,224	16%		No sequential IDs, but access
4			Market	y	y	y	n		y	y	y	n	n	y	y	39,083	6.61%	62,978	161%		Sequential IDs! No sales coun
5			Market	y	y	y	n	y	y	y	y	n	n	y	y	27,718	4.69%	34,741	125%	Finnish, English	Invite link via DNML. Feedbac
6			Market	y			y		y	y	y	n	n	(n)	n	23,946	4.05%				Sequential IDs, can get a full l
7			Market	y			n		y	?	?	n	n	y	n	6,000	1.02%			Russian	Items listed by vendor/shop, b
8			Market	y			y		n							1,719	0.29%			English/German	Won't be easy to scrape... no
9			Market	y			y									1,696	0.29%				
10			Market	y			y									1,257	0.21%				
11			Market	y			y									905	0.15%				
12			Market	y			y									905	0.15%				
13			Market	y			y									819	0.14%				
14			Market	y			y									633	0.11%				
15			Market	y			n									490	0.08%				
16			Market	y			y									411	0.07%			Italian	
17			Market	y			y									187	0.03%				
18			Market	y			y									184	0.03%				
19			Market	y			y									111	0.02%			French	
20			Market	n													0.00%				
21			Market	y			y	y									0.00%				Invitation requested
22			Market	y			y	y									0.00%				
23			Market	y													0.00%			French	(Stuck on registration)
24			?	n													0.00%			French	Down for maintenance
25			Forum	n													0.00%				

The table header groups: columns "Full listings?" through "(Vendor-fb counter?)" fall under **Constraints**; columns "Stated", "%", "Actual", "Sta/Act" fall under **Catalogue size**.

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

oiioiioii Oxford Internet Institute
oiioiioii University of Oxford
oiioiioii

UNIVERSITY OF OXFORD

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017

8

Extracting Product Metadata
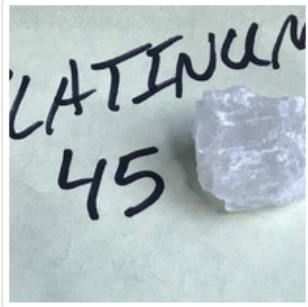
You can browse products and vendors without logging in. For making purchases you'll need to **register an account.**

10 grams of Grade A+ Crystal Methamphetamine - USA DOMESTIC Glass

342.79 EUR (0.088284 BTC)

25 pcs in stock

(3)

United States → Worldwide

This is top grade uncut and touched off the brick crystal methamphetamine. Smokes clean and burns clear. 100% satisfaction. Listing is for a 10 gram sack of glass shards.

Stealth shipping always ensured with a 1 time reship if you do not receive your package. We will be posting bulk sale opportunities once people order a few grams and realize the quality of this product.

USA domestic ships the day of if ordered Monday - Fri and will be delivered in 4 days max.

- Great communation. Great stealth. On time delivery. Decent product (over weight also) :) . Thanks for your gift, bub. I will be back. (28.8.)   (€100+ · 3+)
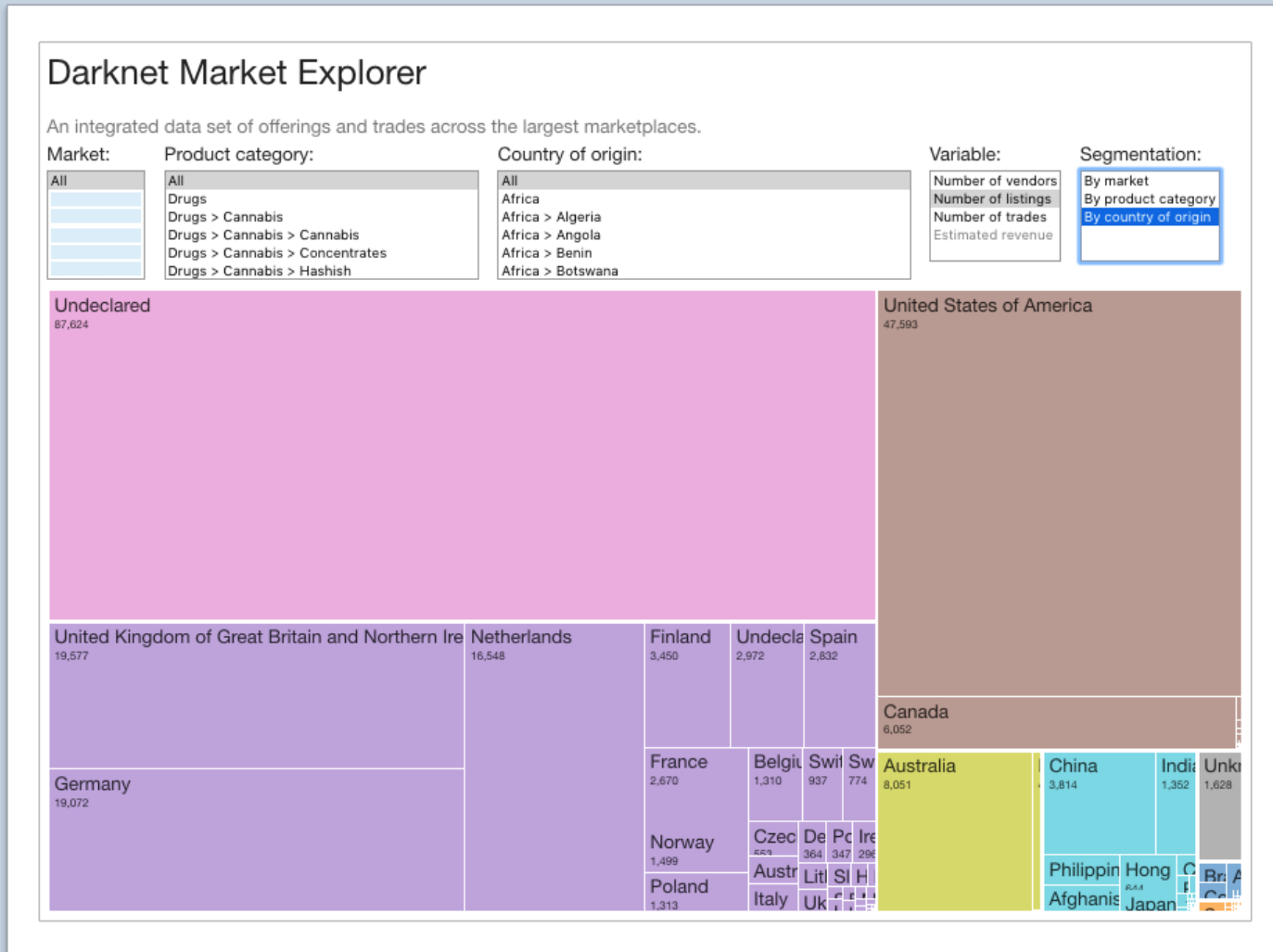
Shipping fee 5.9 EUR (Domestic Priority + Stealth/ Tracki) is included in price shown above. Other shipping options can be selected at additional cost. You only pay for shipping once when you order multiple pieces of a single product or other products from same vendor

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
9

Collecting the Data Across Markets…

- In total we collected **~250k listings** across the markets we observed.

- According to our estimates, this accounts for **80-90% of the global offerings** on darknet markets at the time of data collection

Market	Title	Vendor	ISO3	CC
	2 OZ Crystal Methamphetamines 56 Grams		USA	NA
	3g Power Plant (★★★ Qualitat) - Free Shipping		DEU	EU
	Anavar - 50mg Winstrol - 50mg Anadrol - 50mg		USA	NA
	BudgetBudsExpress Shatter Pack 56g		USA	NA
	Modvigil 200mg - Generic Provigil Modafinil 2...		USA	NA
	AsiaMoviePass - [PORN LIFETIME ACCOUNT]		Undeclared	Undeclared
	seduce-fast-food-girl XXX PC Game		Undeclared	Undeclared
	100 HIGH QUALITY DOUBLE DOSED 4MG YELLOW R039 ...		CAN	NA
	Rapidgator Premium Account		ndeclared	Undeclared
	The Designers Guide to the Cortex M Processor ...		Undeclared	Undeclared
	CANNABIS OIL AND TOP MEDICAL MARIJUANA STRAINS...		Undeclared	Undeclared
	10 x Orange Rolls Royce 200MG		NLD	EU
	Unknown		Unknown	Unknown
	LSD - 1 Trip (200 µg)	Neuropols	DEU	EU
	Digital Counting Scale Grain Kitchen Jewelry B...		USA	NA
	XTC Pillen 210mg 500st		DEU	EU
	XANAX (ALPRAZOLAM) 1 mg x 100 by PFIZER-		HUN	EU
	Special OFFER - 14g - MDMA 84% Dutch Import 10...		GBR	EU
	Videosz\n		Undeclared	Undeclared
Unaps	GHRP2, 10mg/vial, Bio Peptide, 100% Quality	anhav100	Undeclared	EU

A First Market Overview, by Geography

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
11
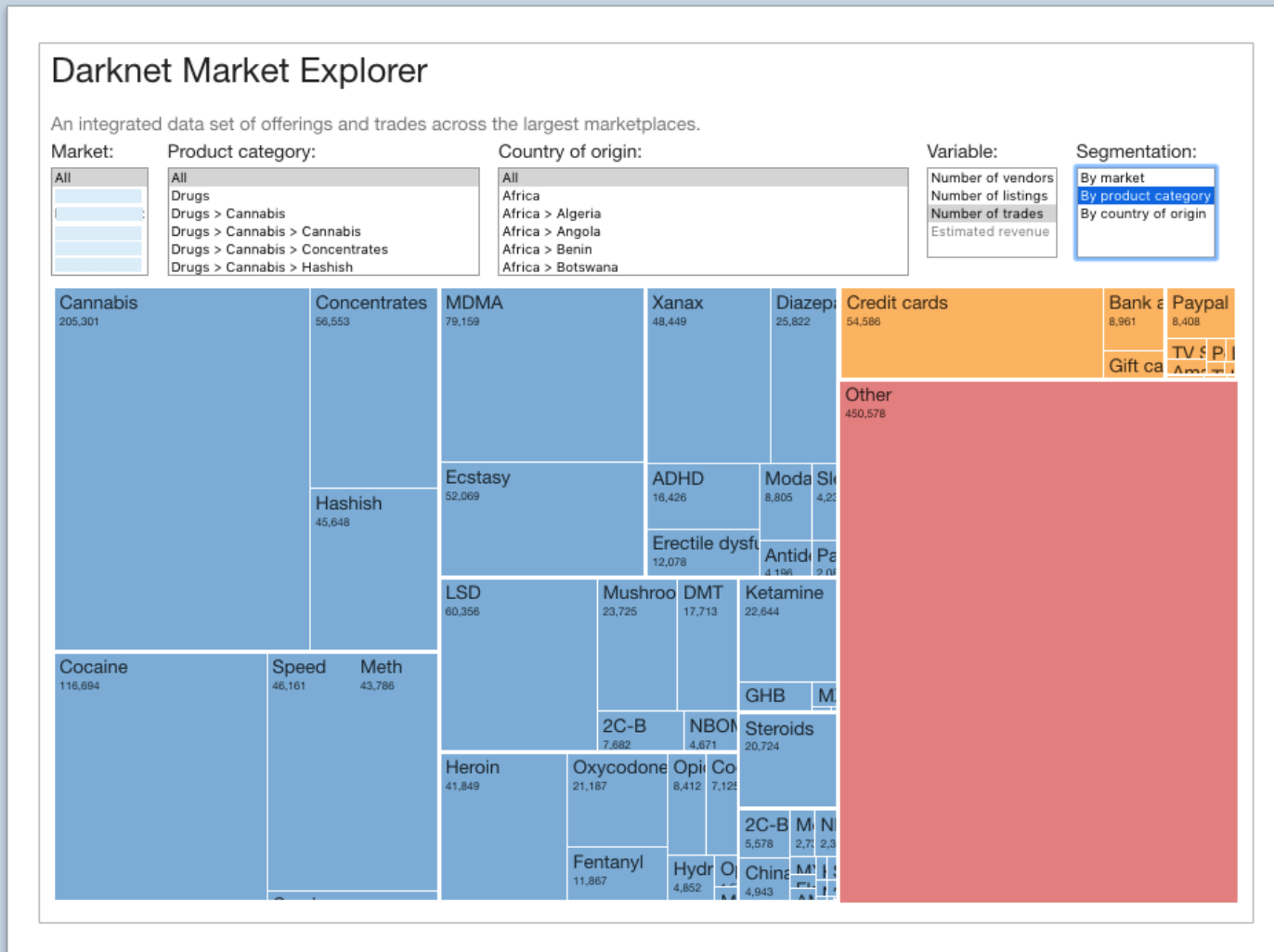
Developing a Simple Product Taxonomy

- Drugs: **Cannabis** (Marijuana, Concentrates, Hashish), **Dissociatives** (GBL, GHB, Ketamine, MXE, MXP, PCP), MDMA, Ecstasy, **New Psychoactive Substances** (2C-B, 2C-E, 2C-I, 4-MEC, AMT, China White, DMAA, Flakka, Kratom, M1, MXE, MXP, Mephedrone, NBOMe, Spice/K2), **Opioids** (Codeine, Fentanyl, Heroin, Hydrocodone, Morphine, Opioid detoxification, Opium, Oxycodone), **Pharmaceuticals** (ADHD, Antidepressants, Diazepam, Erectile dysfunction, Modafinil, Painkillers, Sleeping pills, Xanax), **Psychedelics** (2C-B, DMT, LSD, Mushrooms, NBOMe), **Steroids**, **Stimulants** (Cocaine, Crack, Meth, Speed).

- Information goods: **Accounts** (Amazon, Ebay, Paypal, Porn, TV & Cable, TV Streaming, Uber), **Malware** (Botnets, Malware, Ransomware), **Money** (Bank drops, Credit cards, Gift cards).

- Physical goods: Weapons (Ammunition, Explosives, Hand weapons, Long-range weapons).

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
12

Developing a Simple Product Taxonomy

Oxford Internet Institute
University of Oxford

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
13

Buyer Reviews as Indicators of Activity

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
14

Estimating Trading Activity over Time

Daily sales feedback volume

Legend:
- Total
- Stated origin
- Undeclared origin

X-axis: Mon, 2017-03-06 · Mon, 2017-03-13 · Mon, 2017-03-20 · Mon, 2017-03-27 · Mon, 2017-04-03 · Mon, 2017-04-10 · Mon, 2017-04-17 · Mon, 2017-04-24 · Mon, 2017-05-01 · Mon, 2017-05-08 · Mon, 2017-05-15 · Mon, 2017-05-22 · Mon, 2017-05-29
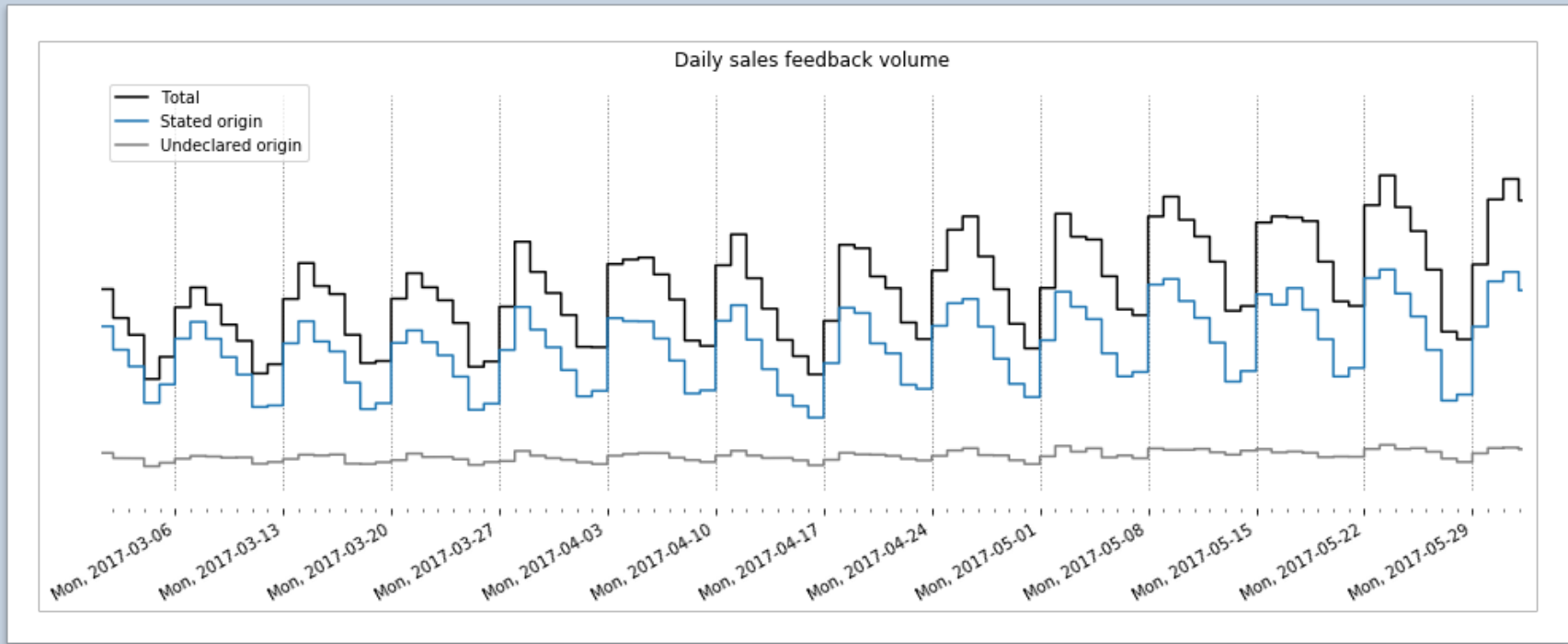
Where are Which Goods Traded?

Drugs > Cannabis

Total reviews
- 1 - 19
- 20 - 199
- 200 - 1999
- 2000 - 19999
- 20000 - 104580
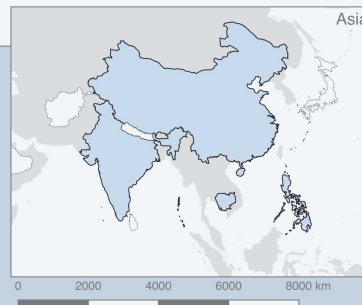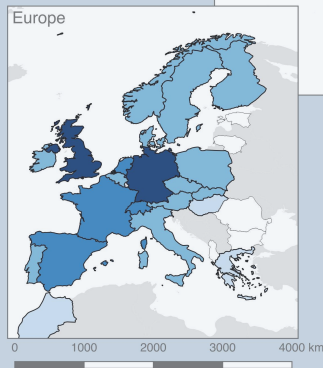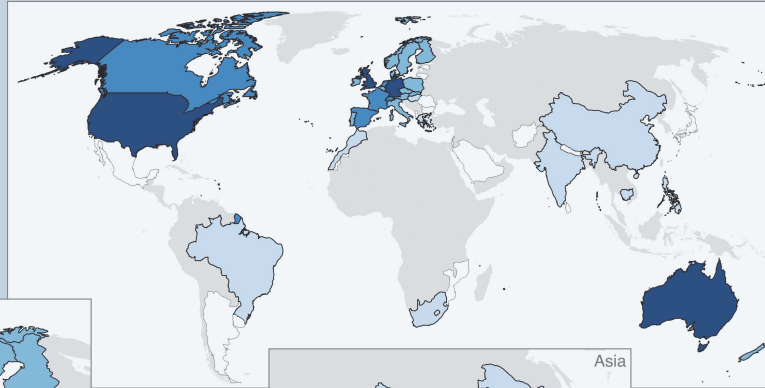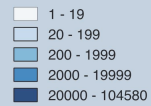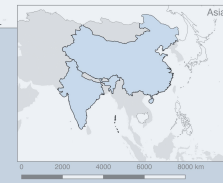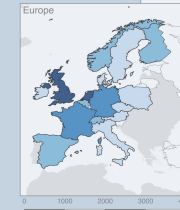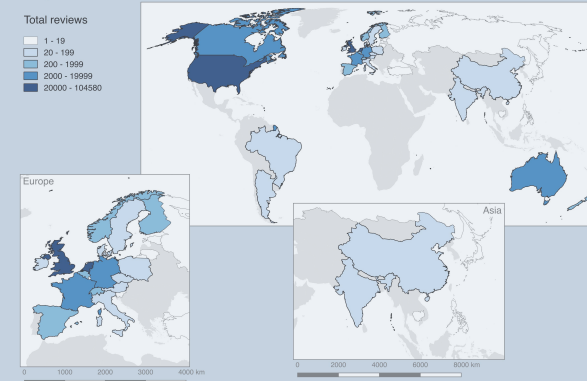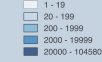
Europe

Asia

Drugs > MDMA

Total reviews
- 1 - 19
- 20 - 199
- 200 - 1999
- 2000 - 19999
- 20000 - 104580

Europe

Asia

Drugs > Psychedelics

Total reviews
- 1 - 19
- 20 - 199
- 200 - 1999
- 2000 - 19999
- 20000 - 104580

Europe

Asia

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
16
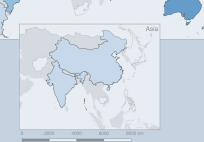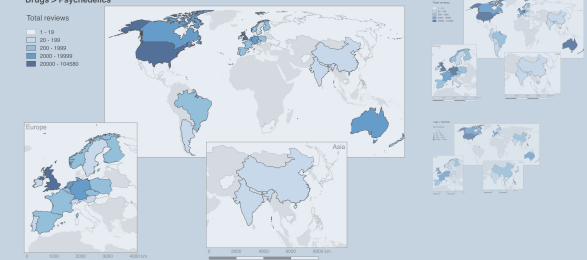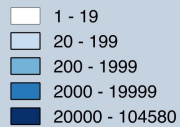
A Focus on Recreational Drugs for the English-speaking West (1/3)

Drugs > Cannabis

Total reviews
- 1 - 19
- 20 - 199
- 200 - 1999
- 2000 - 19999
- 20000 - 104580
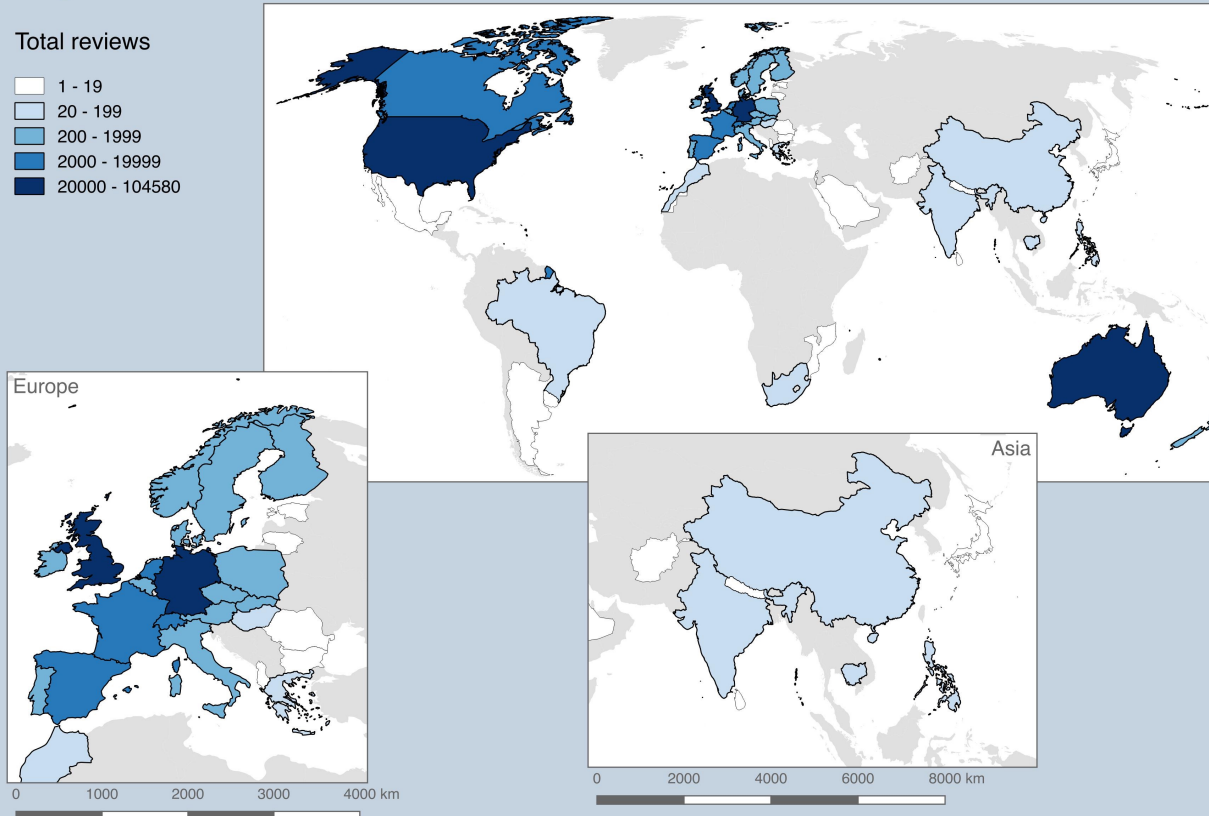
Europe

Asia

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
17

A Focus on Recreational Drugs for the English-speaking West (2/3)

Drugs > MDMA

Total reviews

- 1 - 19
- 20 - 199
- 200 - 1999
- 2000 - 19999
- 20000 - 104580

Europe

Asia

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
18

A Focus on Recreational Drugs for the English-speaking West (3/3)

Drugs > Psychedelics

Total reviews

- 1 - 19
- 20 - 199
- 200 - 1999
- 2000 - 19999
- 20000 - 104580

Europe

Asia

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
19

Some Weapons Trading, but not a Lot

Physical > Weapons

Total reviews

- 1 - 19
- 20 - 199
- 200 - 1999
- 2000 - 19999
- 20000 - 104580

Europe

Asia

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
20
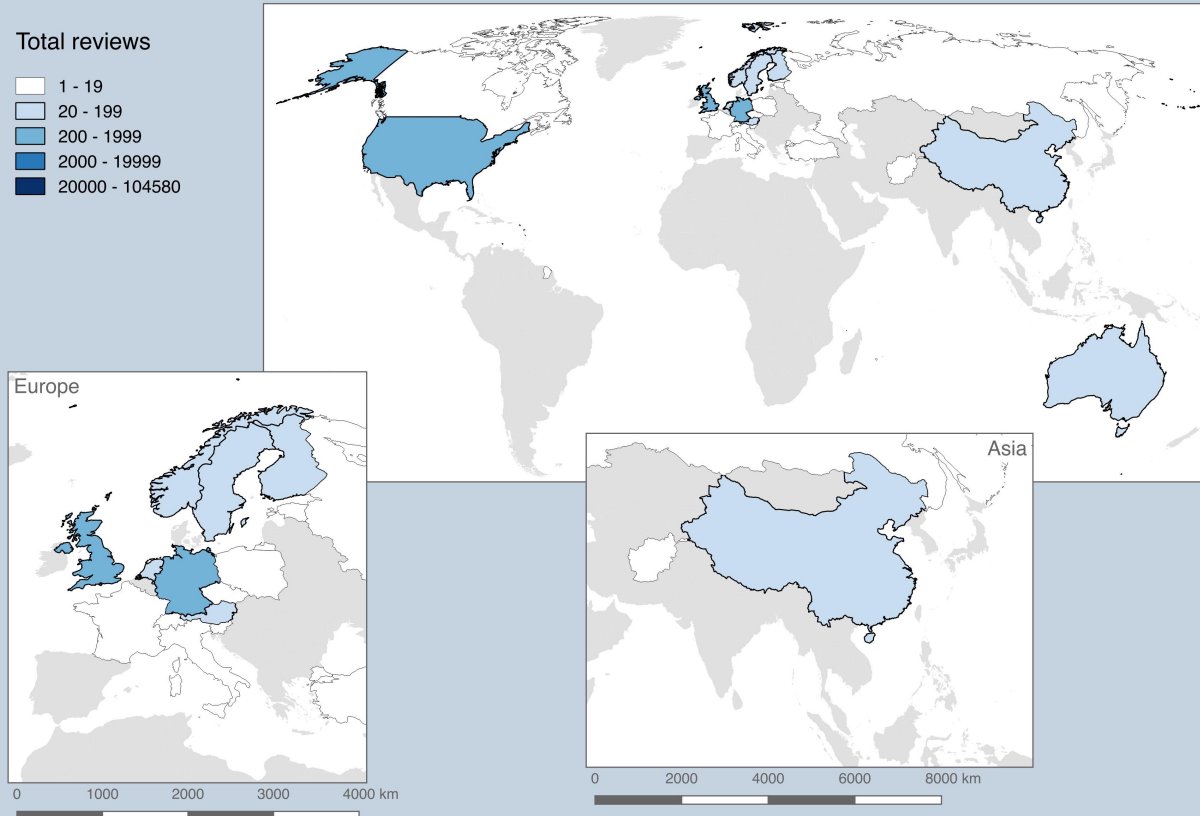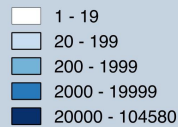
~5 Countries Provide Most of the Inventory

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
21
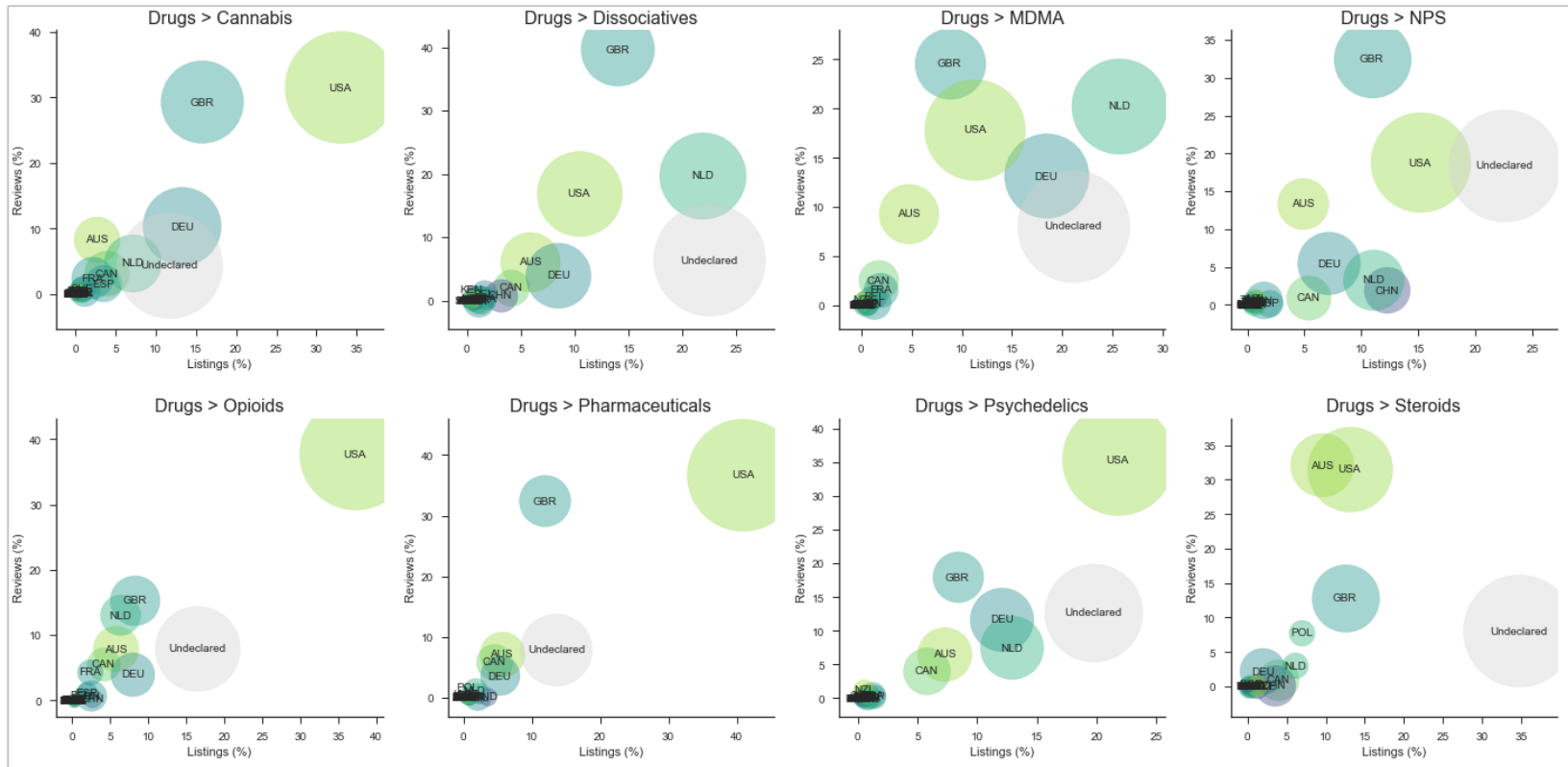
Cocaine Production in South America…

Flows of cocaine from/to countries or regions

→ Main trafficking
→ Other trafficking
Most frequently mentioned countries of provenance for individual drug seizure cases

0   1,000   2,000 km

Source: UNODC, responses to annual report questionnaire and individual drug seizure database.
Notes: The trafficking routes represented on this map should be considered broadly indicative and based on data analyses rather than definitive route outlines. Such analyses are based on data related to official drug seizures along the trafficking routes as well as official country reports and responses to annual report questionnaires. Routes may deviate to other countries that lie along the routes and there are numerous secondary flows that may not be reflected.
The boundaries shown on this map do not imply official endorsement or acceptance by the United Nations. Dashed lines represent undetermined boundaries. The dotted line represents approximately the Line of Control in Jammu and Kashmir agreed upon by India and Pakistan. The final status of Jammu and Kashmir has not yet been agreed upon by the parties. The final boundary between the Sudan and South Sudan has not yet been determined.

http://www.unodc.org/wdr2016/

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
22

… While Cocaine Vendors on Darknet Markets are Situated in Buyer Locations

Drugs > Stimulants

Total reviews
- 1 - 19
- 20 - 199
- 200 - 1999
- 2000 - 19999
- 20000 - 104580

Europe

Asia

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
23
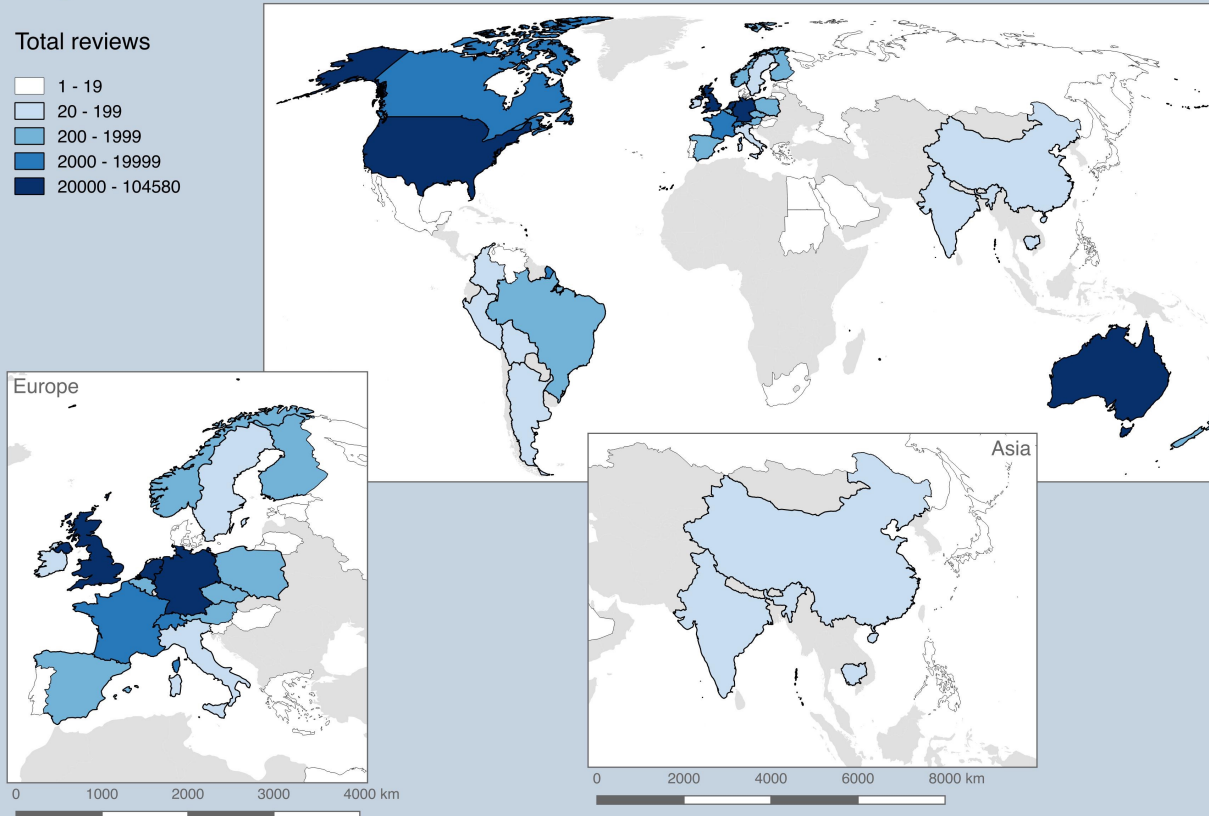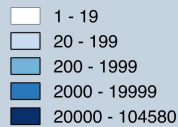
Opium Production in Mexico, Afghanistan

http://www.unodc.org/wdr2016/
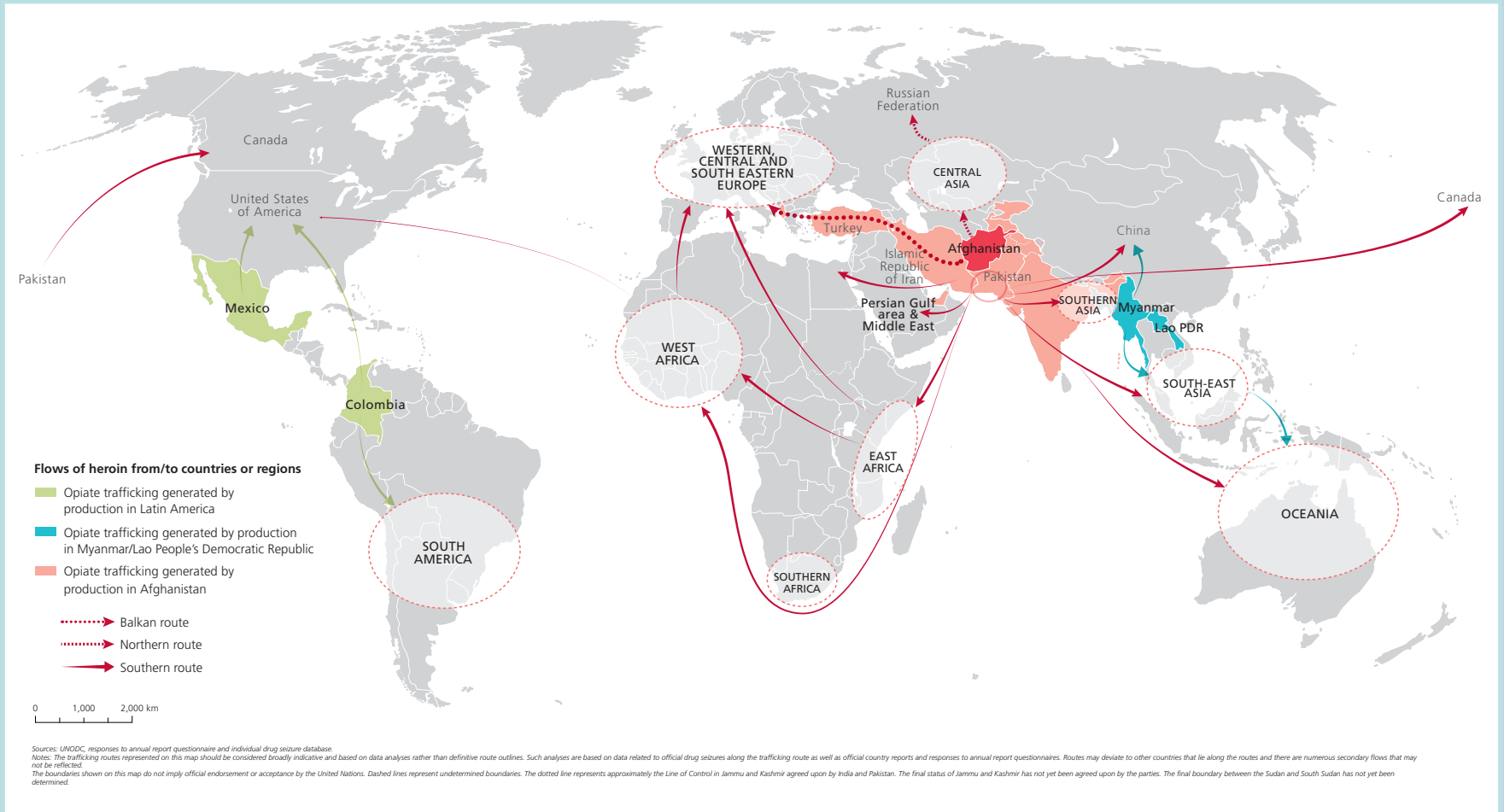
… While Most Opiates on Dark Markets are Sold from Consumer Countries

Drugs > Opioids

Total reviews

- 1 - 19
- 20 - 199
- 200 - 1999
- 2000 - 19999
- 20000 - 104580

Europe

0   1000   2000   3000   4000 km

Asia

0   2000   4000   6000   8000 km
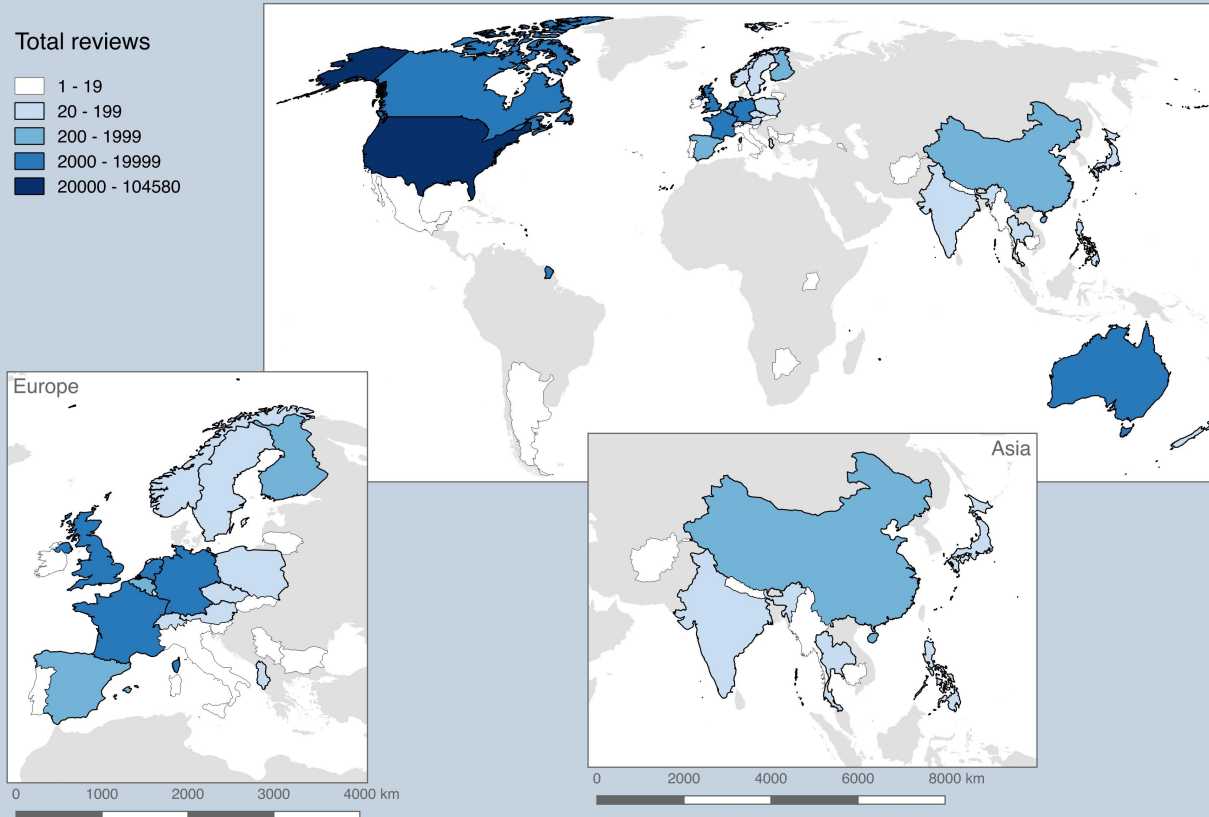
New Psychoactive Substances (NPS)

Drugs > NPS

Total reviews
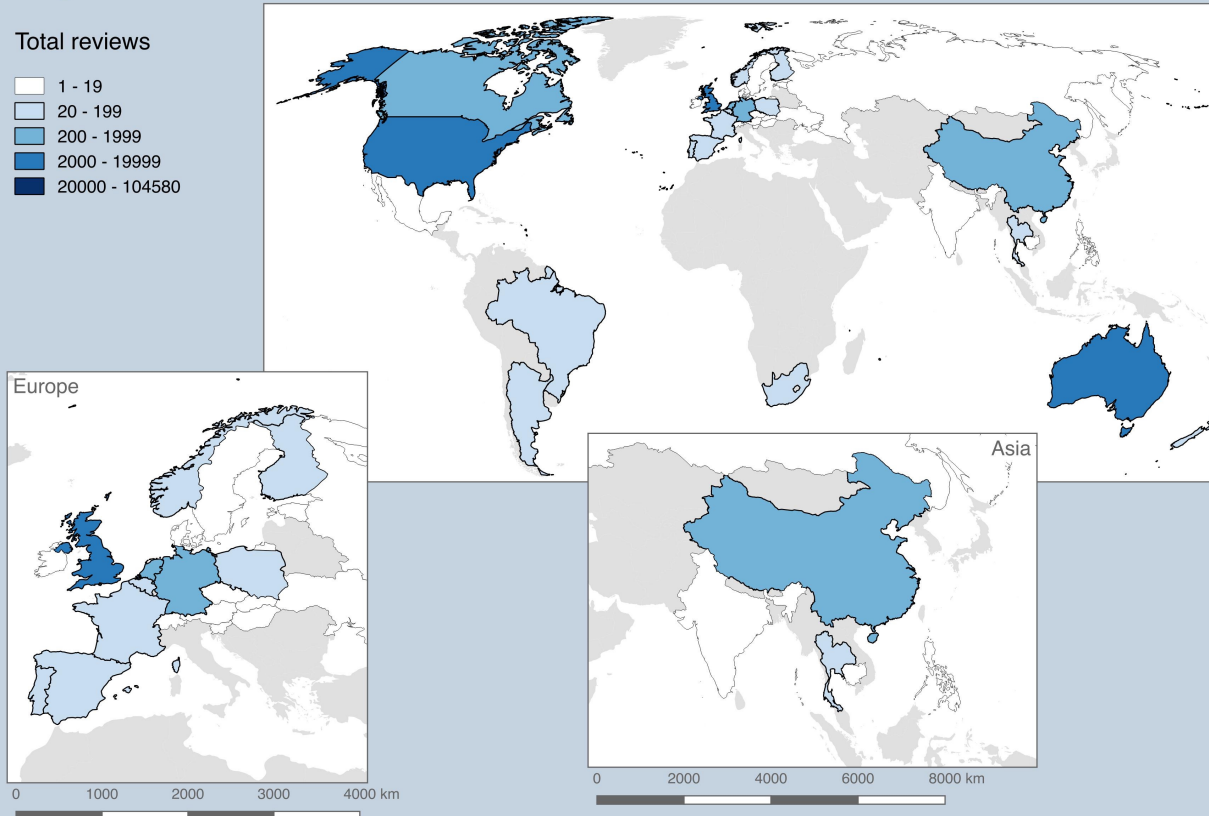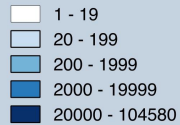
- 1 - 19
- 20 - 199
- 200 - 1999
- 2000 - 19999
- 20000 - 104580

Europe

Asia

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
26

No Need to Declare Country of Origin for Digital Information Goods: No Risk of Border Checks

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
27
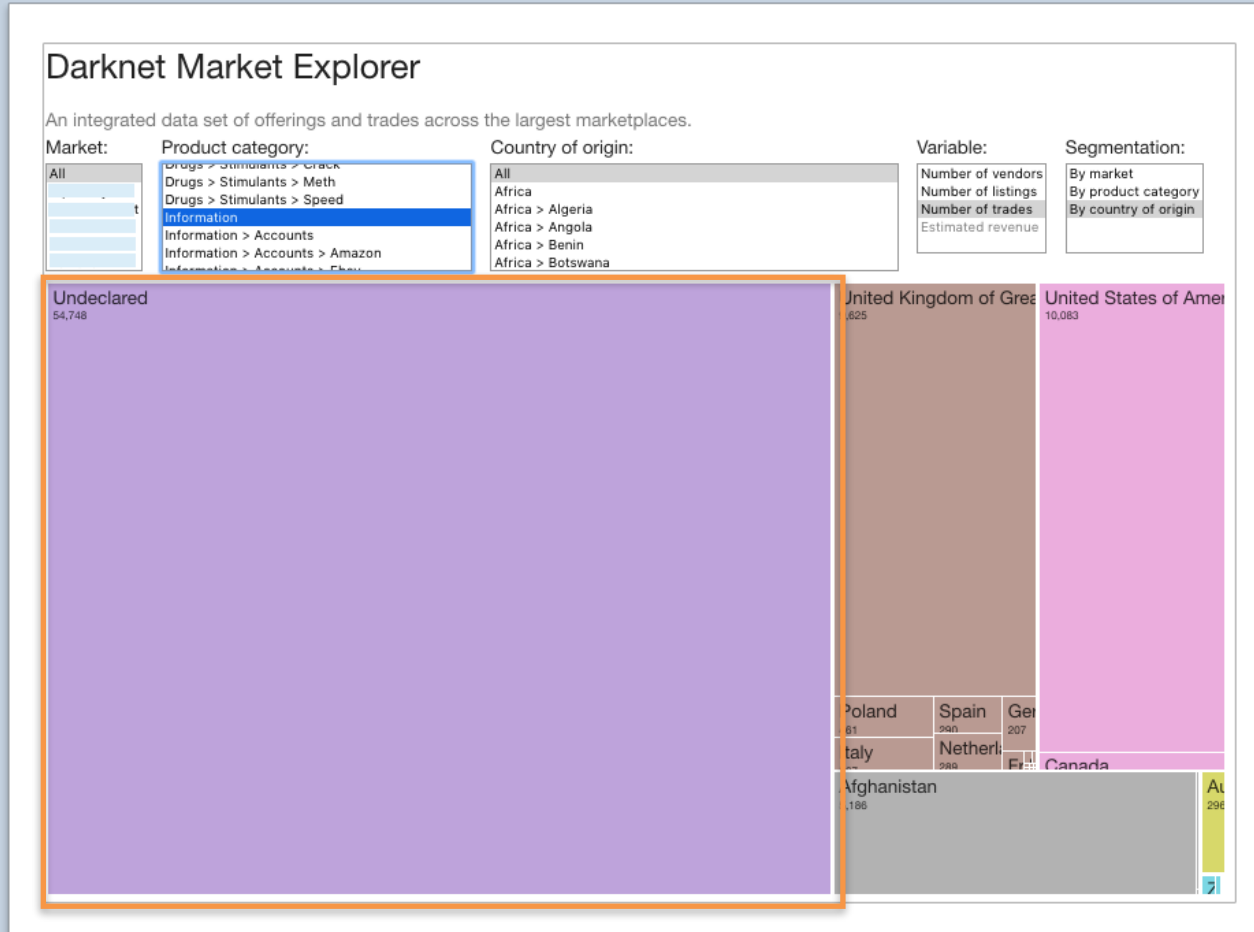
Some Technical Details

- ## Many use curl and other basic crawlers

- ## This has now become less practical
  - An order of magnitude **more listings**
  - Need to carefully control **request rate**
  - Many intermittent **failure modes**: non-trivial retry logic
  - May need to **interrupt and resume** later
  - May want better **alerting** options

Alec Muffett
@AlecMuffett

OII Speaker: "We use Curl…"
OII Funders: "NOT DARK ENOUGH"
S: "<um> DarkCurl™"
F: "Nope"
S: "DarkWebCyberScrapers!"
F: "Now you're talking…"

at country resolution. Martin will give a brief introduction to darknet markets in general, and show a current overview of the largest markets. He will then describe the OII's darknet market scraping technology, and talk about our research, highlighting some of our key findings to date. Product inventories, regional specialisation, small-time buyers and bulk traders, … our

6:27 am - 25 Aug 2017

5 Retweets 13 Likes

twitter.com/alecmuffett/status/901073569366634496

- ## Additionally, we only wanted a specific subset of the data: catalogues and trading indicators. No forum discussions, etc.

- ## We ended up using Scrapy. It's great!

When your study population is taken down by the law...

oii oii oii
oii oii oii   Oxford Internet Institute
oii oii oii   University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
29

Alphabay and Hansa Takedowns in July

Alphabay: 5th July

Hansa: 20th July

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
30
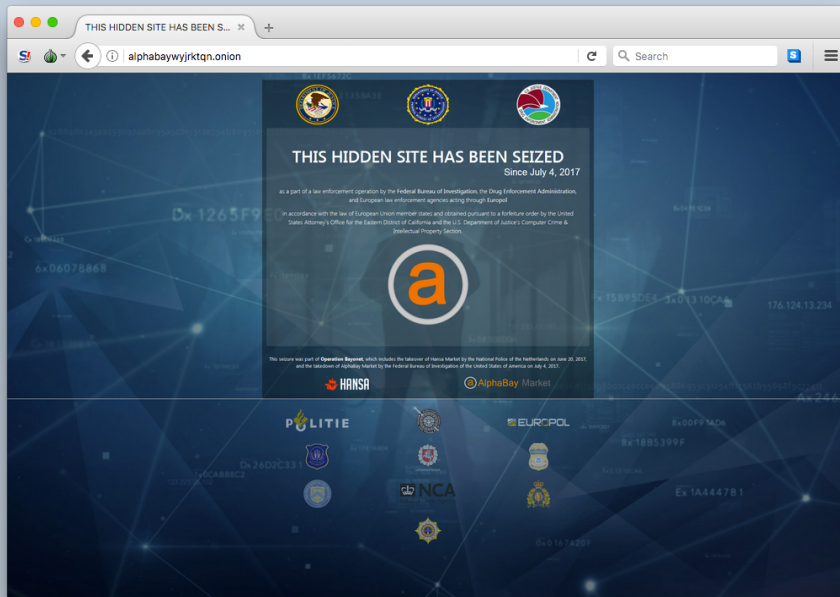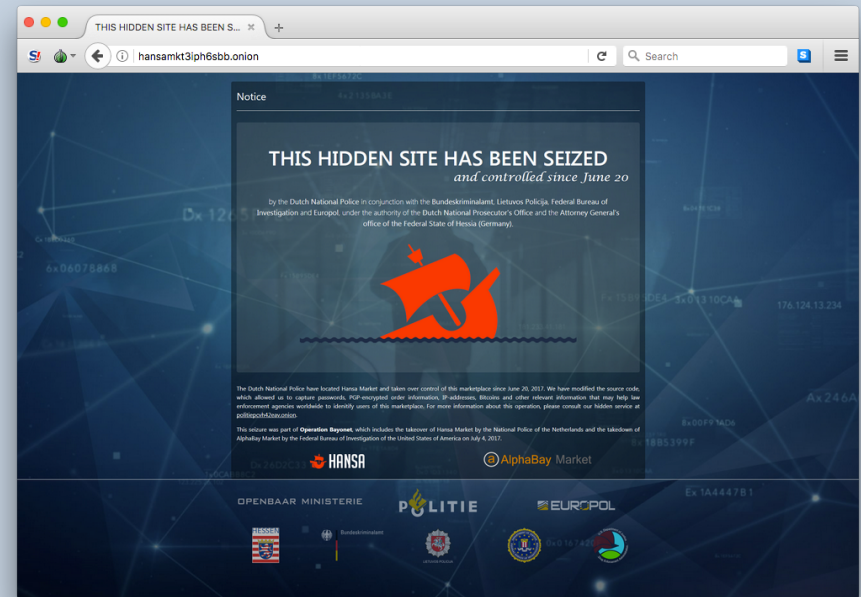
A Multi-stage Covert Attempt to Undermine Trust in Darknet Markets

FBI, DEA, Dutch National Police, Europol working together:

1. Covertly took over Hansa
2. Closed Alphabay on 5th July, the largest market at the time
3. As trading activity moved to Hansa: **secretly collected passwords and chat logs**
4. Took down Hansa on 20th July

The stated intention: to **harm trust in widely used markets**.

MASSIVE BLOW TO CRIMINAL DARK WEB ACTIVITIES AFTER GLOBALLY COORDINATED OPERATION

THIS NEWS/PRESS RELEASE IS ABOUT **DRUG TRAFFICKING**
View all crime areas ▶

20 July 2017
Press Release

Takedown of AlphaBay and Hansa will lead to hundreds of new investigations in Europe

Months of preparation and coordination have resulted today, 20 July 2017, in the takedown of two of the largest criminal Dark Web markets, AlphaBay and Hansa.

Two major law enforcement operations, led by the **Federal Bureau of Investigation (FBI)**, **the US Drug Enforcement Agency (DEA)** and **the Dutch National Police**, with the support of **Europol**, have shut down the infrastructure of an underground criminal economy responsible for the trading of over 350 000 illicit commodities including drugs, firearms and cybercrime malware. The coordinated law enforcement action in Europe and the US ranks as one of the most sophisticated takedown operations ever seen in the fight against criminal activities online.

"This is an outstanding success by authorities in Europe and the US," **Rob Wainwright**, the Executive Director of Europol, said today, while appearing alongside the US Attorney General, Acting FBI Director and Deputy Director of the US Drug Enforcement Administration (DEA), at a special press conference in Washington DC. "The capability of drug traffickers and other serious criminals around the world has taken a serious hit today after a highly sophisticated joint action in multiple countries. By acting together on a global basis the law enforcement community has sent a clear message that we have the means to identify criminality and strike back, even in areas of the Dark Web. There are more of these operations to come," he added.

Dimitris Avramopoulos, European Commissioner for Migration, Home Affairs and Citizenship, said: "The Dark Web is growing into a haven of rampant criminality. This is a threat to our societies and our economies that we can only face together, on a global scale. The take-down of the two largest criminal Dark Web markets in the world by European and American law enforcement authorities shows the important and necessary result of international cooperation to fight this criminality. I congratulate the American and Dutch authorities for their successful work, as well as Europol for centrally supporting this endeavour. Our fight against criminal activities online and offline will continue and intensify."

Julian King, EU Commissioner for the Security Union, said: "This latest success demonstrates not just the growing threat posed by increasingly sophisticated criminal enterprises exploiting the largely unregulated space occupied by the internet but also the vital role of international cooperation among law enforcers, the private sector, national authorities and international organisations in making all of us safer from global, borderless menaces."

https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-w

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of Darknet Marketplaces
@OiiDarknet
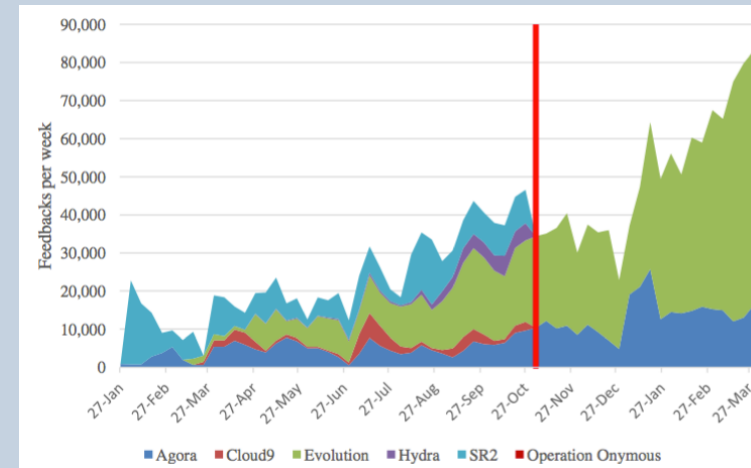
August 31, 2017
31

Ouch… impact for our research?

- **Having your data source suddenly disappear** is a worry for any long-term data scraping process…

- However in this case: opportunity to move beyond a simple observational study to a **quasi-experiment**. We can observe what happens in the overall marketplace after the external intervention.

- In this case: **how resilient are these marketplaces** to interference by law enforcement? Does trade actually go down, or simply move elsewhere?
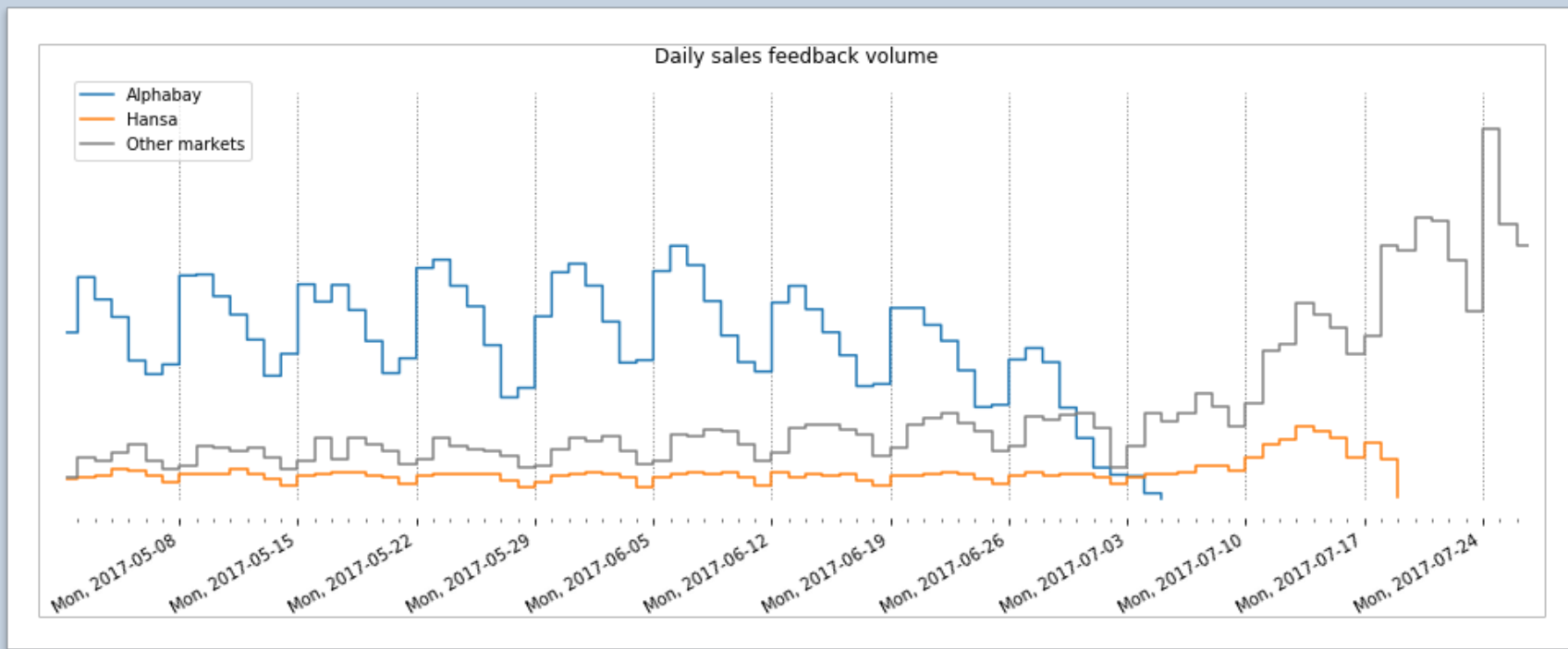
  Was it an effective deterrent?

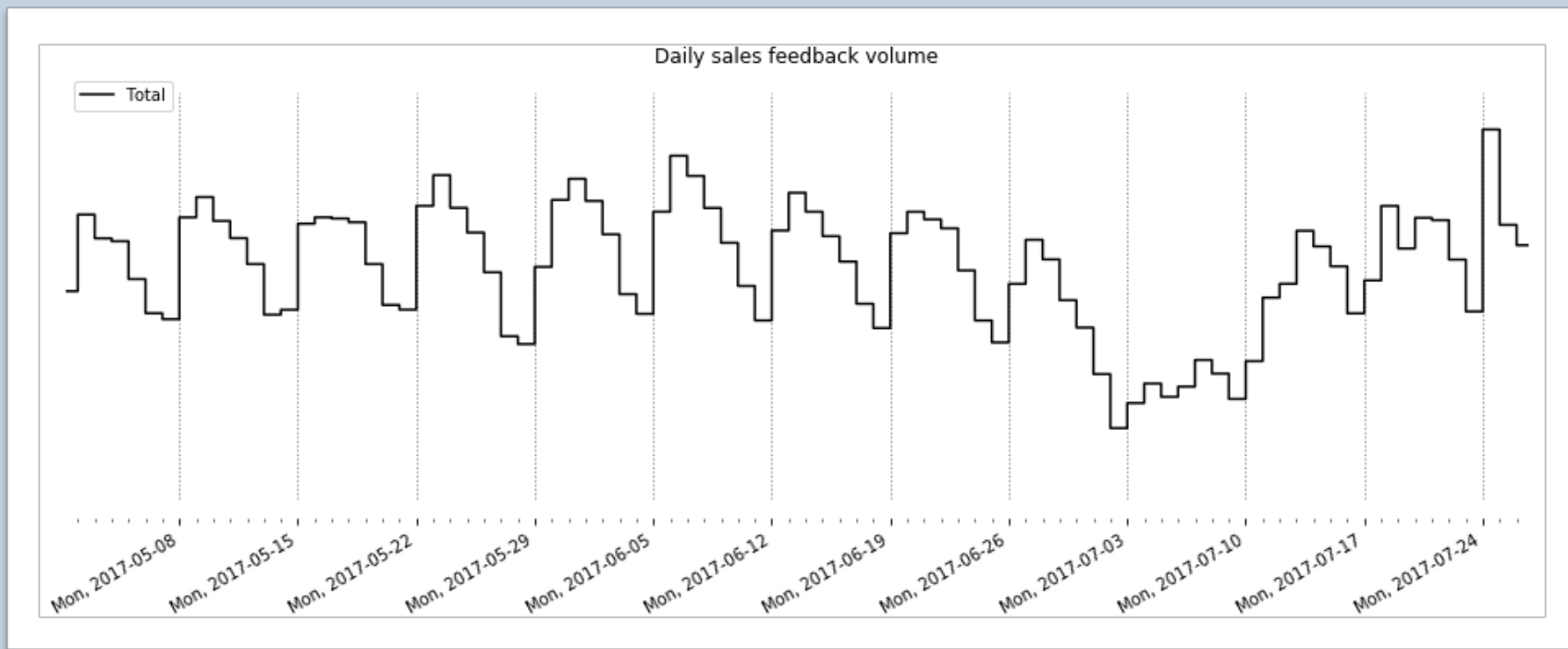# Prior Experience Suggests: Takedown Deterrent Might Not Last

- Décary-Hétu & Giommoni (2016), "*Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous*"

- Initial effect:
  - **Most vendor accounts retired**, few moved to new markets.
  - Drop in overall sales.

- Within 1-2 months:
  - New vendor accounts appeared.
  - Product prices did not change.
  - **Overall sales increased!**

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
33

After Alphabay and Hansa Takedowns: Buyers Simply Moved to Other Markets

Daily sales feedback volume

- Alphabay
- Hansa
- Other markets

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
34

After Alphabay and Hansa Takedowns: Buyers Simply Moved to Other Markets

Daily sales feedback volume

Oxford Internet Institute
University of Oxford

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

In closing, some security-related matters…

oii oii oii Oxford Internet Institute
oii oii oii University of Oxford
oii oii oii

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
36

The Basic Infrastructure Proposition of These Markets

- **Electronic currency** to avoid identification

- **Buyer reviews** to establish trust

- Market resilience through **redundant market platforms** developed by independent actors

- An "**open innovation**" approach to iterative improvement

- Some **self-policing** to avoid raising too much attention. E.g. markets typically ban child porn. Some also ban fentanyl, weapons, etc.

But Also a Popular Target for Scams

- Dark markets have wide appeal, but a **high technical barrier** to entry. This yields opportunities for scams.

- Most recently: a **tutorial site** with instructions on **how to use darknet markets**. High pagerank, so people would find it easily.

- … it sent people to a **fraudulent mixing service**.

MOTHERBOARD

GONE PHISHING

Image: Flickr/Mr TGT. Composition: Author

An Elaborate Darknet Phishing Scam Is the Top Google Result for Basic Bitcoin Tutorials

JORDAN PEARSON
Aug 30 2017, 6:13pm

"This is probably the best phishing scam I've ever seen."

SHARE   f   TWEET   🐦

As far as online scams designed to steal money and information go, a site called darknetmarkets.org is very impressive and equally scary—not least because Google is currently serving it as a top search result for Bitcoin tutorials.

Darknetmarkets.org, for all intents and purposes, is a "real" website. Its logo looks to be made of chopped-up cocaine, and the site is filled with legitimate-seeming resources for anybody looking to buy drugs on the darknet. News articles populate its homepage, and the site features how-tos on topics like using "mixing" services to hide your Bitcoin transactions from the authorities. A sidebar contains links to the "top" sites to buy drugs on the darknet. If you search Google for "how to mix bitcoins," darknetmarkets.org comes up as the number one result.

https://motherboard.vice.com/en_us/article/d33ey7/an-elaborate-darkne

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
38

And Frequent Scams by Market Operators

- **Exit scams** and other market manipulations: a big incentive to take the money and run.

- Operators and moderators may **abuse their privileged positions**.

- A common approach: **occasional transgressions**. Not enough to undermine trust in the market itself.

- In other cases, **scammers can operate freely** on markets without interference by admins.

Oxford Internet Institute
University of Oxford

UNIVERSITY OF OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017
39

Risk for Operators: Information Leaks Can Lead to Arrests

- Information security is hard. Market operators may not have sufficient **opsec experience**.

- Increasing law enforcement efforts to take down markets and big vendors.

- Common occurrence: **reused identities**, e.g. email addresses or aliases.

  (But also suggestions that such instances can be the result of parallel construction efforts by law enforcement agents.)

ANDY GREENBERG SECURITY 11.07.14 06:00 AM

GLOBAL WEB CRACKDOWN ARRESTS 17, SEIZES HUNDREDS OF DARK NET DOMAINS

Jeeves privacy. Photo: Josh Valcarcel/WIRED JOSH VALCARCEL/WIRED

When "Operation Onymous" first came to light yesterday, it looked like a targeted strike against a few high value targets in the Dark Web drug trade. Now the full scope of that international law enforcement crackdown has been revealed, and it's a scorched-earth purge of the Internet underground.

On Friday, the European police agency Europol along with the FBI and the Department of Homeland Security announced that the operation has now arrested 17 people in as many countries and seized hundreds of Dark Web domains associated with well over a dozen black market

https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

Insecure Dev Practices are Common

Reasons: went offline with user's money probably due to the discovery of many XSS bugs, a private message leak and their test server being exposed on the clearnet
PGP key:

Notes: removed August 22, 2017

- A lot of **insecure coding practices** by inexperienced developers. Frequent XSS/ injection vulnerabilities. (I've looked at a lot of markup. Impression: often not professional web developers.)

- **IP leaks: real or fake?** Recent reports that a market was leaking an IP address. A basic opsec transgression.

  Some suggest: maybe a decoy?

Market Complaint Accusation
Regarding ████████ IP address exposure... I already pointed it out 9 months ago. And, it's a red herring.
submitted 1 month ago by ████████

I reported on this 9 months ago.

See for yourself:

I find it hilarious how much news is out there today about some other guys "discovery" - I already found it. And, ████████ still exists. *it's a red herring*. ████████ did it on purpose to mislead people. He's probably getting a laugh out of all the news being generated all over it. People only now care because the AB and Hansa takedowns. If it was a real finding, LE would have taken them down long ago because you know they on this subreddit 24/7.

Do Operators Even **Audit** their Platforms?

- An **inherent tension** between operator anonymity and common security practices: open code, external audits, …

- Some markets introduced **bug bounties**.
  https://darkwebnews.com/darknet-markets/darknet-markets-bug-bounties/

- A key moment to start paying attention: **when a big platform gets taken down**. People will flood to a smaller one. That market may not yet have spent time auditing their code.

A final request…

- Please *send me term lists for more software categories: hacking tools, keyloggers, …*

  Who catalogues such tools?

Oxford Internet Institute
University of Oxford

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

UNIVERSITY OF OXFORD

Economic Geography of
Darknet Marketplaces
@OiiDarknet

Thank You! Questions?

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

**The Economic Geography of Darknet Marketplaces
Oxford Internet Institute**

www.oii.ox.ac.uk/research/projects/economic-geog-darknet
@OiiDarknet

oii oii oii   Oxford Internet Institute
oii oii oii   University of Oxford

UNIVERSITY OF
OXFORD

Martin Dittus, @dekstop
Joss Wright, @josswright
Mark Graham, @geoplace

Economic Geography of
Darknet Marketplaces
@OiiDarknet

August 31, 2017

44