The Language of Legal and Illegal Activity on the Darknet

Leshem Choshen*, Dan Eldad*,
Daniel Hershcovich*, Elior Sulem* and Omri Abend

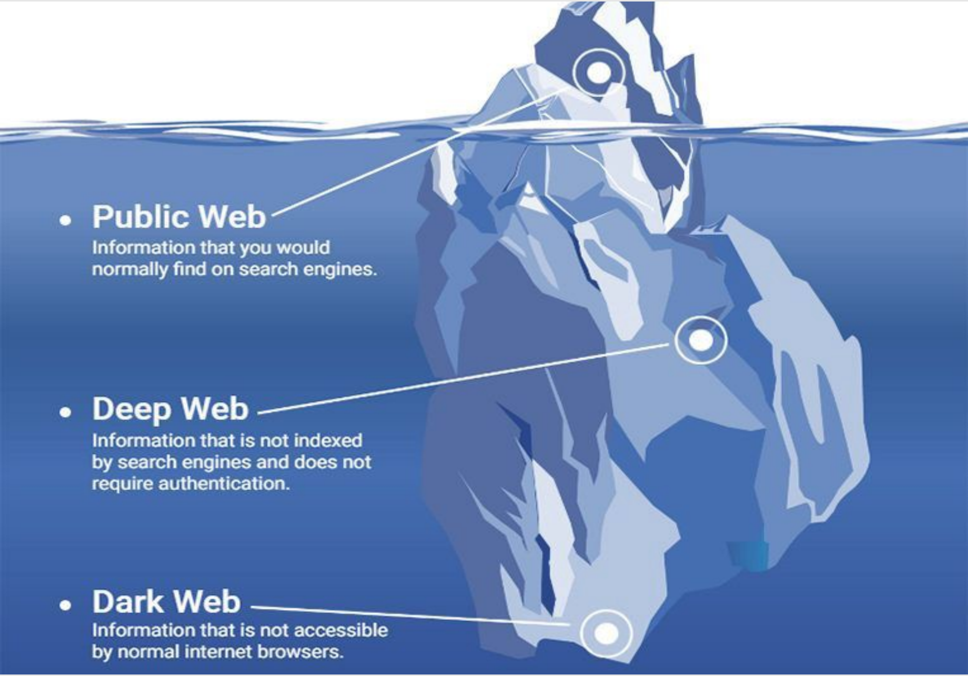
האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

ISRAEL SCIENCE FOUNDATION

THE FEDERMANN CYBER SECURITY CENTER
School of Computer Science and Engineering

Prime Minister's Office
National Cyber Bureau

July 31, 2019 *Equal contribution ACL 2019, Florence



Public Web
Information that you would normally find on search engines.
Deep Web
Information that is not indexed by search engines and does not require authentication.
Dark Web
Information that is not accessible by normal internet browsers.

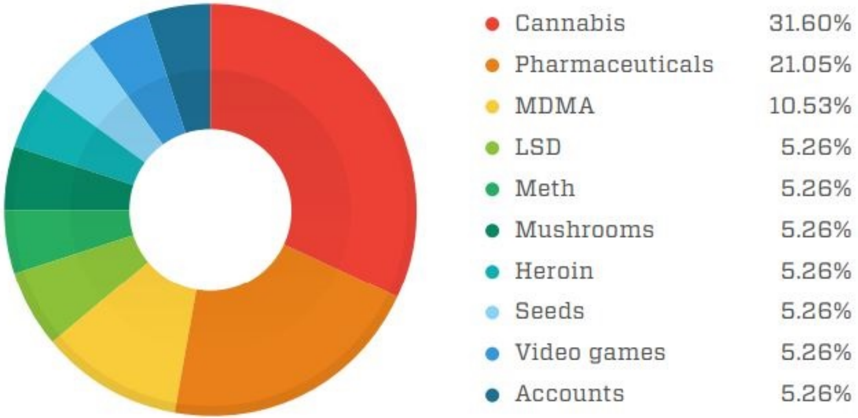
Darknet

Used interchangeably in this work:

- **Dark Web**
- **Darknet**
- **Tor** network (Tor: an encrypted browser)
- **Onion** network (.onion top-level domain)

Hosts: **onion services** (hidden services).

Darknet Markets



[1] Paganini (2015). "The Deep Web and Its Darknets".

Drugs

Finest organic cannabis grown by proffessional growers in the netherlands.
We double seal all packages for odor less delivery.
Shipping within 24 hours!

Product	Price	Quantity
1g Original Haze	15 EUR = 0.025 ฿	1_ X Buy now
5g Original Haze	65 EUR = 0.108 ฿	1_ X Buy now
1g Bubblegum	10 EUR = 0.017 ฿	1_ X Buy now
5g Bubblegum	45 EUR = 0.075 ฿	1_ X Buy now
1g Jack Herer	14 EUR = 0.023 ฿	1_ X Buy now
5g Jack Herer	60 EUR = 0.099 ฿	1_ X Buy now
1g Chronic	9 EUR = 0.015 ฿	1_ X Buy now
5g Chronic	40 EUR = 0.066 ฿	1_ X Buy now
1g Banana Kush	11 EUR = 0.018 ฿	1_ X Buy now
5g Banana Kush	45 EUR = 0.075 ฿	1_ X Buy now
1g Blue Cheese	9 EUR = 0.015 ฿	1_ X Buy now
5g Blue Cheese	40 EUR = 0.066 ฿	1_ X Buy now
1g Ice-O-Lator Hash, finest quality	35 EUR = 0.058 ฿	1_ X Buy now

Language of the Darknet

How well do **NLP tools** work on Darknet text?

spaCy

Language of the Darknet

How well do **NLP tools** work on Darknet text?

spaCy

Can we automatically **identify** illegal activity?

Language of the Darknet

How well do **NLP tools** work on Darknet text?

spaCy

Can we automatically **identify** illegal activity?

Disclaimer: variations among legal systems, societies and groups.

DUTA-10K

Dataset of 10367 Onion Services text pages [Al Nabki et al., 2019].

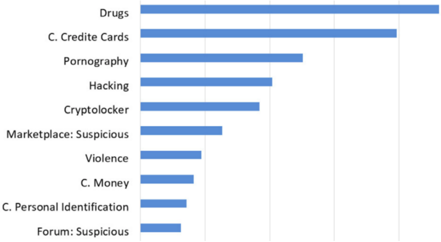
- Classified by monitoring needs of Spanish **law enforcement agencies**.
- 20% categorized as **illegal** and 48% as **legal** (32% unavailable).
- Of the illegal websites, 23% concern illegal **drugs**.

DUTA-10K

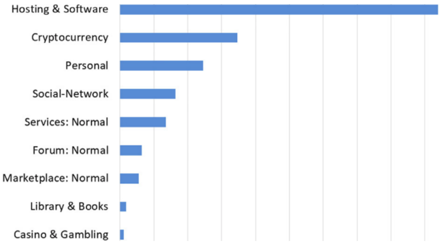
Dataset of 10367 Onion Services text pages [Al Nabki et al., 2019].

- Classified by monitoring needs of Spanish **law enforcement agencies**.
- 20% categorized as **illegal** and 48% as **legal** (32% unavailable).
- Of the illegal websites, 23% concern illegal **drugs**.

Distribution of categories:



Illegal



Legal

Control Data: eBay

Product descriptions acquired by searching for drug-related terms.
Do not sell actual drugs, but rather drug-related products.

Control Data: eBay

Product descriptions acquired by searching for drug-related terms.
Do not sell actual drugs, but rather drug-related products.

3 Layers Chip Style Herb Herbal Tobacco Grinder Weed Grinders

Description:

- Quantity: 1
- Type : Tobacco Crusher
- Feature: Stocked,Eco-Friendly
- Material: plastic
- Size: 42*26mm

Package include:

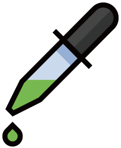
- 1PC Tobacco Crusher

Data

	Public Web	Dark Web
Legal	**eBay** (188 pages, 35,799 words)	**Legal Onion** (35 pages, 61,655 words)
Illegal		**Illegal Onion** (255 pages, 1,438,351 words)

Cleaning

- Remove non-linguistic content: buttons, encryption keys, URLs...
- Split to paragraphs, join to single lines, remove duplicates.
- Sampled 571 paragraphs from each, for comparable size.



```
Finest organic cannabis grown by proffessional growers in the netherlands.
We double seal all packages for odor less delivery. Shipping within 24 hours!
3 Layers Chip Style Herb Herbal Tobacco Grinder Weed Grinders
```

Vocabulary

Distance between word distributions

to	0.0486
the	0.4242
of	0.0162
is	0.0118
and	0.0102
...	
EUR	0.0094
cocaine	0.0041
Free	0.0041
drug	0.0035
1	0.0025
...	

Vocabulary

Distance between word distributions, measured by:

- Jensen-Shannon divergence
- L1 distance

Small "self-distances", found by splitting each in half

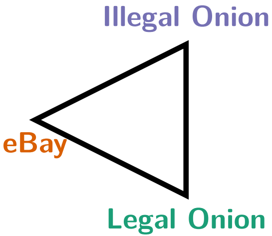
to	0.0486
the	0.4242
of	0.0162
is	0.0118
and	0.0102
...	
EUR	0.0094
cocaine	0.0041
Free	0.0041
drug	0.0035
1	0.0025
...	

Vocabulary

Distance between word distributions, measured by:

- Jensen-Shannon divergence
- L1 distance

Small "self-distances", found by splitting each in half, but the different domains are about equidistant.



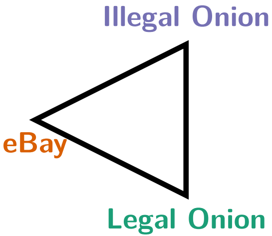
to	0.0486
the	0.4242
of	0.0162
is	0.0118
and	0.0102
…	
EUR	0.0094
cocaine	0.0041
Free	0.0041
drug	0.0035
1	0.0025
…	

Vocabulary

Distance between word distributions, measured by:

- Jensen-Shannon divergence
- L1 distance

Small "self-distances", found by splitting each in half, but the different domains are about equidistant.



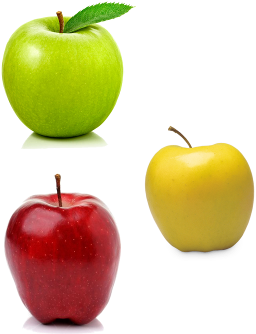
to	0.0486
the	0.4242
of	0.0162
is	0.0118
and	0.0102
...	
EUR	0.0094
cocaine	0.0041
Free	0.0041
drug	0.0035
1	0.0025
...	

Legal and illegal Onion should be considered different domains.

Characteristics of Darknet Data

Diverse: sub-domains are distinguishable.

Unique: distinguishable from other domains.



Named Entities and Wikification

NE extraction [spaCy] + Wikification [Bunescu and Pașca, 2006].

	% (of detected NEs) Wikifiable
eBay	38.6 ± 2.00
Illegal Onion	32.5 ± 1.35
Legal Onion	50.8 ± 2.31

By manual inspection, NE precision and recall are low for **Illegal Onion**. For example: slang words for drugs (e.g., "**kush**") falsely picked up as NEs.

$\Rightarrow$ Standard NLP is not suited for this domain.

Classes

We identified three domains. Two binary classification settings:

{ **eBay**, **Legal Onion** }

{ **Legal Onion**, **Illegal Onion** }

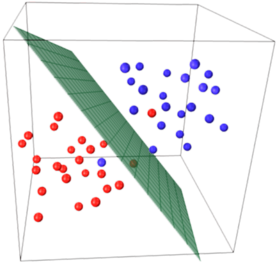
Classes

We identified three domains. Two binary classification settings:

{ **eBay**, **Legal Onion** }

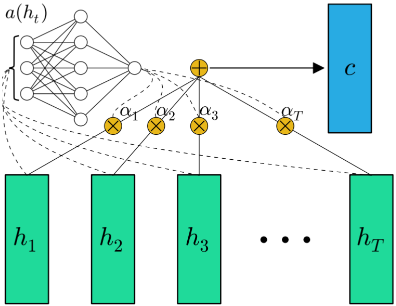
{ **Legal Onion**, **Illegal Onion** }

What are the linguistic features distinguishing them?



Classifiers

- NB: Naive Bayes (bag of words)
- SVM: Support Vector Machine
- BoE: sum/average GloVe + MLP
- seq2vec: BiLSTM + MLP
- attention: ELMo + BCN (self-attention)



Manipulations

To find what linguistic cues are used for classification.

Manipulations

To find what linguistic cues are used for classification. Conditions:

- Full original text
- Drop **content** words
- Drop **function** words
- Replace **content** words with their POS
- Replace **function** words with their POS

$$\{\text{ADJ, ADV, NOUN, PROPN, VERB, X, NUM}\}$$

Manipulations

To find what linguistic cues are used for classification. Conditions:

- Full original text
- Drop **content** words
- Drop **function** words
-
- Replace **function** words with their POS

{ADJ, ADV, NOUN, PROPN, VERB, X, NUM}

Generic	Viagra	(	Oral	Jelly	)	is	used	for	Erectile	Dysfunction
PROPN	PROPN	(	PROPN	PROPN	)	VERB	VERB	for	PROPN	PROPN

Manipulations

To find what linguistic cues are used for classification. Conditions:

- Full original text
- Drop **content** words
- Replace **content** words with their POS
- Drop **function** words
- Replace **function** words with their POS

$$\{\text{ADJ, ADV, NOUN, PROPN, VERB, X, NUM}\}$$

Generic	Viagra	(	Oral	Jelly	)	is	used	for	Erectile	Dysfunction
PROPN	PROPN	(	PROPN	PROPN	)	VERB	VERB	for	PROPN	PROPN

Welcome	to	SnowKings	Good	Quality	Cocaine	!
VERB	to	PROPN	PROPN	PROPN	PROPN	!

Results

eBay vs. **Legal Onion** drugs:

	full	drop content	drop function	pos content	pos function
NB	91.4	57.8	90.5	56.9	92.2
SVM	63.8	64.7	63.8	68.1	63.8
BoE_{sum}	66.4	56.0	63.8	50.9	76.7
$\text{BoE}_{\text{average}}$	75.0	55.2	59.5	50.0	75.0
seq2vec	73.3	53.8	65.5	65.5	75.0
attention	82.8	57.5	85.3	62.1	82.8

Results

Legal Onion vs. **Illegal Onion** drugs:

	full	drop content	drop function	pos content	pos function
NB	77.6	53.4	87.9	51.7	77.6
SVM	63.8	66.4	63.8	70.7	63.8
BoE_{sum}	52.6	61.2	74.1	50.9	51.7
$\text{BoE}_{\text{average}}$	57.8	57.8	52.6	55.2	50.9
seq2vec	56.9	55.0	54.3	59.5	49.1
attention	64.7	51.4	62.9	55.2	69.0

Darknet Forums

Can we generalize beyond drugs?

Darknet Forums

Can we generalize beyond drugs?

DUTA-10K also contain Legal Forums and Illegal Forums.
Multi-topic and user-generated.

Results

Legal Onion vs. **Illegal Onion** forums:

	full	drop content	drop function	pos content	pos function
NB	74.1	50.9	78.4	50.9	72.4
SVM	85.3	75.9	56.0	81.9	81.0
BoE_{sum}	25.9	32.8	21.6	36.2	35.3
$\text{BoE}_{\text{average}}$	40.5	42.2	31.9	48.3	53.4
seq2vec	50.0	48.9	50.9	28.4	51.7
attention	31.0	37.2	33.6	27.6	30.2

Results

Trained on **drugs**, evaluated on **forums** (**Legal Onion** vs. **Illegal Onion**):

	full	drop content	drop function	pos content	pos function
NB	78.4	63.8	89.7	63.8	79.3
SVM	62.1	69.0	54.3	69.8	62.1
BoE_{sum}	45.7	50.9	49.1	50.9	50.0
$\text{BoE}_{\text{average}}$	49.1	51.7	51.7	52.6	58.6
seq2vec	51.7	61.1	51.7	54.3	57.8
attention	65.5	59.2	65.5	50.9	66.4

Conclusion

Differences between legal and illegal Darknet sites include:
Vocabulary, shallow syntax (POS) and named entities.

Conclusion

Differences between legal and illegal Darknet sites include:
Vocabulary, shallow syntax (POS) and named entities.

Identified by:

- Word statistics: diverse and unique
- Wikification: works less well on illegal
- Predictive: simple classifiers work best

Conclusion

Differences between legal and illegal Darknet sites include:
Vocabulary, shallow syntax (POS) and named entities.

Identified by:

- Word statistics: diverse and unique
- Wikification: works less well on illegal
- Predictive: simple classifiers work best

https://github.com/huji-nlp/cyber

Conclusion

Differences between legal and illegal Darknet sites include:
Vocabulary, shallow syntax (POS) and named entities.

Identified by:

- Word statistics: diverse and unique
- Wikification: works less well on illegal
- Predictive: simple classifiers work best

https://github.com/huji-nlp/cyber

Thanks!

References I

Al Nabki, M. W., Fidalgo, E., Alegre, E., and Fernández-Robles, L. (2019).
ToRank: Identifying the most influential suspicious domains in the Tor network.
Expert Systems with Applications, 123:212–226.

Bunescu, R. and Pașca, M. (2006).
Using encyclopedic knowledge for named entity disambiguation.
In *Proc. of EACL*.