

City University of New York (CUNY)

CUNY Academic Works

Open Educational Resources

Hostos Community College

2020

Cybersecurity-The Silk Road Market

Amy J. Ramson

CUNY Hostos Community College

[How does access to this work benefit you? Let us know!](#)

More information about this work at: https://academicworks.cuny.edu/ho_oers/7

Discover additional works at: <https://academicworks.cuny.edu>

This work is made publicly available by the City University of New York (CUNY).

Contact: AcademicWorks@cuny.edu

CYBERSECURITY: SILK ROAD MARKET

These slides describe an account of how the Department of Justice through the FBI and DEA successfully brought the mastermind, Ross Ulbricht, behind the DARK WEB drug bazaar, SILK ROAD, to justice

Silk Road

Professor Amy Ramson, Esq.

This OER material was produced as a result of the PIT-UN network Challenge Grant – New America

Creative Commons License



This work is licensed under a
[Creative Commons Attribution-Noncommercial-Share Alike 4.0 License](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Ulbricht-head of the Silk Road market

- Ross Ulbricht was born on March 27, 1984
- Ulbricht created the **Silk Road website** in 2011
- Ulbricht earned millions of dollars in profits from the commissions collected on purchases
- Around January 2012, he adopted the username Dread Pirate Roberts referring to the pirate in the popular novel and film **The Princess Bride** that is passed to whom ever was wearing the mask
- In order to assure users that posts from by DPR were his own, DPR authenticated his posts using an electronic signature known as a PGP key.
- **See explanation of PGP key signature authentication on next slide**

PGP electronic signature authentication

- When sending digital signatures, PGP uses an algorithm that generates a hash (a mathematical summary) which is encrypted with the sender's private key
- The receiver uses the sender's public key to decrypt the hash code. A match of the hash code sent as the digital signature for the message verifies that the message has arrived securely from the sender

The Silk Road website

- Had a customer-friendly storefront similar to Amazon or E-Bay
- Was the dark web's largest black market, with \$1.2 billion in sales and nearly a million customers
- Sold drugs, fake passports, driver's licenses and illegal service providers, such as hit men, hackers, and forgers

Silk Road Market website image from Newsweek

Silk Road
 anonymous market

messages 1 | orders 0 | account \$0.00

Search

Shop by Category

Drugs 2,399

- Cannabis 341
- Dissociatives 65
- Ecstasy 209
- Opioids 156
- Other 144
- Precursors 12
- Prescription 526
- Psychedelics 427
- Stimulants 273

Apparel 114

Art 7

Books 743

Collectibles 12

Computer equipment 19

Custom Orders 26

Digital goods 310

Drug paraphernalia 89

Electronics 20

Erotica 319

Fireworks 2

Food 3

Forgeries 58

Hardware 2

Home & Garden 7

Jewelry 48

Lab Supplies 5

Lotteries & games 29

Medical 5

5x - 10mg Dexedrine (Pure Dextroamphetamine)
\$4.94

2 x 0,25 mg Xenax (Alprazolam)
\$1.50

Malena charas hand rubbed Indian hash 100g
\$75.83

1 Gram OG KUSH OIL 81% THC 90% TOTAL
\$4.13

14 grams (1/2 Ounce) of Nebula JWH-122
\$2.63

3.5g Crystal Meth Ice Shards
\$31.92

20 x 25mg Cialis
\$2.57

III...Psilocybe-Cubensis-Chocolate...III
\$18.15

100 x Orange Star Very high MDMA content 180mg
\$105

100x 200mg White XTC 'Speakers'
\$200

3g Methylone Crystals - \$50-Lab Grade
\$50

15mg Adderall Extended Release (1 Capsule)
\$15

Purchases were made using Bitcoins

- Bitcoin is decentralized, operating apart from governmental currencies or central banks
- Anyone who downloads the Bitcoin software becomes part of the Bitcoin network
- Bitcoins are similar to cash because they allow vendors and customers to be anonymous
- Bitcoins were transferred between anonymous accounts, which had no identifying information about the account user
- The transaction history of each Bitcoin is logged in a blockchain which prevents a person from spending the same Bitcoin twice
- The blockchain automatically “self-updates” when a Bitcoin transaction takes place

Read The Big Bitcoin Heist in Vanity Fair magazine

<https://www.vanityfair.com/news/2019/11/the-big-bitcoin-heist>

- Criminals broke into a data center in Iceland and stole 550 Bitcoin computers, with motherboards, graphics cards, and power accessories worth \$500,000
- But essentially, “The criminals stole the digital presses used to print money in the age of cryptocurrency”.
- The value of the computers was immense because the machines could mine Bitcoins which would provide a continuous stream of virtual encrypted and untraceable money for the burglars

TOR

- Users of Silk Road's had to use Tor software to reach its servers.
- "Tor" or The Onion Router is an **Internet networking protocol**
- Using Tor's software makes it difficult, to ascertain the user's webmail, search history, see social media posts and most other online activity including the user's country because their devices' IP address is stripped

Federal law enforcement involved

- Different federal agencies had started working on the case
- But the US Department of Justice's Federal Bureau of Investigation and Drug Enforcement Agency solved it
- FBI-The lead federal agency for investigating cyber attacks by criminals, overseas adversaries and terrorists
- DEA-The principal agency dealing with drug trafficking and distribution within the United States

Investigation by two divisions of US Attorney's Offices

- Two divisions of the Department of Justice: the U.S. Attorney's Offices for the District of Maryland and the Southern District of New York investigated
- Law enforcement agents knew that the Dread Pirate Roberts had created and managed the site, but they did not know DPR's actual identity.

US Attorneys office

- The United States Attorneys serve as the nation's principal litigators under the direction of the Attorney General.
- There are 93 United States Attorneys stationed throughout the United States, Puerto Rico, the Virgin Islands, Guam, and the Northern Mariana Islands, United States and one in Washington D.C.
- Attorneys are appointed by the President with the advice and consent of the United States Senate.

United States Attorneys continued

United States Attorneys conduct the trial work in which the United States is a party

The United States Attorneys have three statutory responsibilities:

- the prosecution of criminal cases brought by the Federal Government;
- the prosecution and defense of civil cases in which the United States is a party; and
- the collection of debts owed the Federal Government which are administratively uncollectible

Technology versus privacy

- Innovations in electronic surveillance technology have outpaced constitutional and statutory protections, leaving areas where there are currently no controls on the use of new surveillance devices and/or no legal interpretations
- This current case brought up some of those questions with regard to the 4th amendment but it did not provide definitive answers

Defense argument: Violation of 4th amendment rights

The Fourth amendment to the Constitution:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Fourth Amendment argument

- The government viewed this case as the illegal sale of drugs and other nefarious services
- The defendant claimed that the government is violating privacy in the digital sphere through 14 searches and seizures of Ulbricht's computers, equipment, and online accounts

Examples of 4th amendment violations defense alleged

1. Tracing of Ulbricht's alleged servers in Iceland with no warrant
2. Requesting Comcast for information related to Ulbricht's alleged IP address in San Francisco.
3. Use of Ulbricht's home Internet routing data which helped the government match Ulbricht's online activity with DPR's use of Silk Road
4. Warrants that were "general warrants" that allowed the government to obtain a lot of private data while the 4th amendment requires that law enforcement obtain particular places or persons.

For instance: On the day of Ulbricht's arrest, the government obtained a warrant to seize Ulbricht's laptop and searched it for a wide variety of information related to Silk Road and information that would identify Ulbricht as Dread Pirate Roberts.

Example of alleged 4th amendment violation: Pen/Trap orders

- On September 2013, the government obtained five “pen/trap” orders. See 18 U.S.C. §§ 3121-27 (“Pen/Trap Act”).
- The orders allowed law enforcement to collect IP addresses for Internet traffic to and from Ulbricht’s home router and other devices that connected to Ulbricht’s home router
- No probable cause or warrant is needed for these

Searches and Seizures

- A great deal of the evidence against Ulbricht came from the government's search of his laptop and his home after the arrest.
- The government recovered DPR's private PGP key on Ulbricht's laptop. The public PGP key did not change during the site's life span, meaning that DPR used the same private key to sign his posts throughout the time that he administered Silk Road
- On the day of Ulbricht's arrest, the government obtained a warrant to seize Ulbricht's laptop and searched it for a wide variety of information related to Silk Road and information that would identify Ulbricht as Dread Pirate Roberts.

Arrest of Ulbricht

- Ulbricht was arrested in a San Francisco public library on October 1, 2013
- The arrest was successfully orchestrated to catch Ulbricht in the act of administering Silk Road as DPR.
- Federal agents observed Ulbricht enter the public library, and a few minutes later Dread Pirate Roberts came online in the Silk Road staff chat.
- Der-Yeghiayan, under the undercover administrator username Cirrus, initiated a chat with DPR, asking him to address some flagged messages from users because this would “force [Ulbricht] to log in under . . . his Dread Pirate Roberts account” in the Silk Road marketplace, as well as in the staff chat software.”

The arrest continued

- Once Der-Yeghiayan knew that DPR had logged onto the flagged message page, he signaled another agent to arrest Ulbricht
- Once arrested agents seized his laptop. The chat that Der-Yeghiayan had initiated with Dread Pirate Roberts was open on Ulbricht's screen.

Trial

- Ulbricht's trial lasted three weeks, from January 13 through February 4, 2015.
- Judge Forrest handled the complex and combative trial.
- Ulbricht was found guilty of drug trafficking and other crimes associated with his creation and operation of an online marketplace Silk Road

The Federal Sentencing Guidelines

- The Sentencing Guidelines are rules for judges in sentencing defendants who are convicted in the US federal court system
- Their goals is to ensure uniformity among all defendants
- Although they are not mandatory, judges must consider them and, if they depart from the Guidelines, they must explain why

How the Federal Sentencing Guidelines operate

- The Federal Sentencing Guidelines operate upon a point system, from 1 to 43, with the higher points leading to longer sentences
- There is a “baseline” number of points allocated for each crime to which extra points for enhancements are added.
- Enhancements are conditions that make the crime worse, for example use of a firearm possession in furtherance of drug trafficking and many more
- The total of the baseline number plus the enhancement is the offense level, a number ranging between 1 and 43 is the offense level
- The sentence is calculated by matching the “offense level” to months of imprisonment necessary for that crime in the sentencing table

SENTENCING TABLE
(in months of imprisonment)

Offense Level	Criminal History Category (Criminal History Points)					
	I (0 or 1)	II (2 or 3)	III (4, 5, 6)	IV (7, 8, 9)	V (10, 11, 12)	VI (13 or more)
Zone A	1	0-6	0-6	0-6	0-6	0-6
	2	0-6	0-6	0-6	0-6	1-7
	3	0-6	0-6	0-6	2-8	3-9
	4	0-6	0-6	2-8	4-10	6-12
	5	0-6	0-6	1-7	4-10	6-12
	6	0-6	1-7	2-8	6-12	9-15
	7	0-6	2-8	4-10	8-14	12-18
	8	0-6	4-10	6-12	10-16	15-21
Zone B	9	4-10	6-12	8-14	12-18	18-24
	10	6-12	8-14	10-16	15-21	21-27
	11	8-14	10-16	12-18	18-24	24-30
Zone C	12	10-16	12-18	15-21	21-27	27-33
	13	12-18	15-21	18-24	24-30	30-37
Zone D	14	15-21	18-24	21-27	27-33	33-41
	15	18-24	21-27	24-30	30-37	37-46
	16	21-27	24-30	27-33	33-41	41-51
	17	24-30	27-33	30-37	37-46	46-57
	18	27-33	30-37	33-41	41-51	51-63
	19	30-37	33-41	37-46	46-57	57-71
	20	33-41	37-46	41-51	51-63	63-78
	21	37-46	41-51	46-57	57-71	70-87
	22	41-51	46-57	51-63	63-78	77-96
	23	46-57	51-63	57-71	70-87	84-105
	24	51-63	57-71	63-78	77-96	92-115
	25	57-71	63-78	70-87	84-105	100-125
	26	63-78	70-87	78-97	92-115	110-137
	27	70-87	78-97	87-108	100-125	120-150
	28	78-97	87-108	97-121	110-137	130-162
	29	87-108	97-121	108-135	121-151	140-175
	30	97-121	108-135	121-151	135-168	151-188
	31	108-135	121-151	135-168	151-188	168-210
	32	121-151	135-168	151-188	168-210	188-235
	33	135-168	151-188	168-210	188-235	210-262
	34	151-188	168-210	188-235	210-262	235-293
	35	168-210	188-235	210-262	235-293	262-327
	36	188-235	210-262	235-293	262-327	292-365
	37	210-262	235-293	262-327	292-365	324-405
	38	235-293	262-327	292-365	324-405	360-life
	39	262-327	292-365	324-405	360-life	360-life
	40	292-365	324-405	360-life	360-life	360-life
	41	324-405	360-life	360-life	360-life	360-life
	42	360-life	360-life	360-life	360-life	360-life
	43	life	life	life	life	life

US Department of Probation's involvement in sentencing

- A probation officer interviews the defendant and produces a presentence report for the judge to use in sentencing.
- The PSI contains details on the defendant's offense; the defendant's criminal history; the defendant's family history, education, employment record, military service, finances, and health; information about victim impact and potential restitution; recommendation of a sentence
- Judges rely on these recommendations

Sentencing

- Ulbricht's sentencing hearing took place on May 29, 2015. The district court (federal trial court) decided that Ulbricht's offense level was 43—the highest possible offense level under the Sentencing Guidelines—and that his criminal history category was I.
- The high offense level largely resulted from the massive quantity of drugs trafficked using Silk Road, as well as several enhancements, including one for directing the use of violence
- Due to the high offense level, the Guidelines advisory sentence range was life in prison also recommended by the US Probation Office