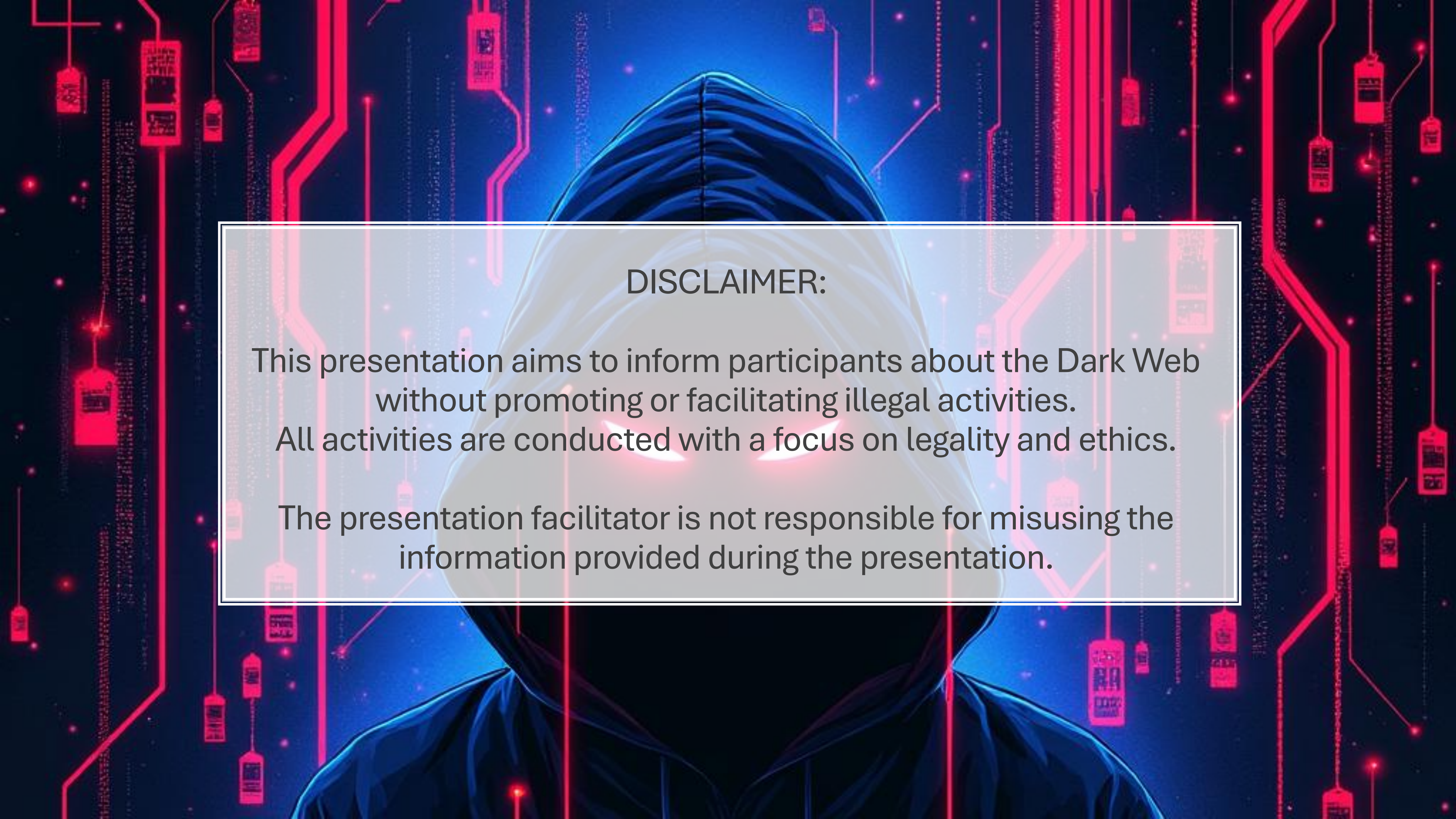
Exploring the Dark Web

Technology and Risks

Antonio Brandao

Cybersecurity Architect, BCNET

Jan 2025



DISCLAIMER:

This presentation aims to inform participants about the Dark Web without promoting or facilitating illegal activities.
All activities are conducted with a focus on legality and ethics.

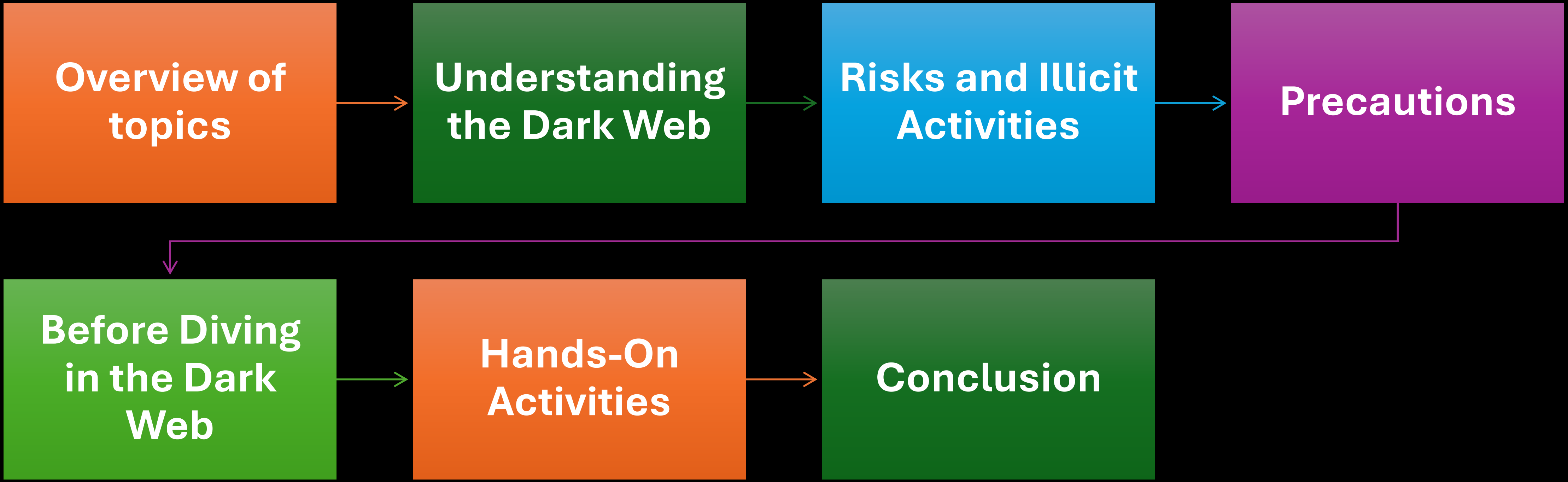
The presentation facilitator is not responsible for misusing the information provided during the presentation.

Disclaimer

The content and demonstrations presented in this session are strictly for **educational purposes** and are intended to promote awareness and understanding of online privacy, security, and the use of the TOR network.

- **You are hereby advised not to use the information provided to:**
  1. Engage in illegal activities.
  2. Access prohibited, restricted, or unauthorized material.
  3. Violate any laws, regulations, or ethical guidelines.
- **By participating in this session, you agree to:**
  - Use the knowledge and techniques responsibly and lawfully.
  - Ensure compliance with the policies and regulations of your organization, jurisdiction, and governing authorities.
  - The presenter and affiliated parties disclaim any liability for the misuse of the information or tools demonstrated. Always consult applicable laws and regulations before implementing or experimenting with any technology.

Agenda



Overview of topics

Understanding the Dark Web

Risks and Illicit Activities

Precautions

Before Diving in the Dark Web

Hands-On Activities

Conclusion

Introduction to the Dark Web

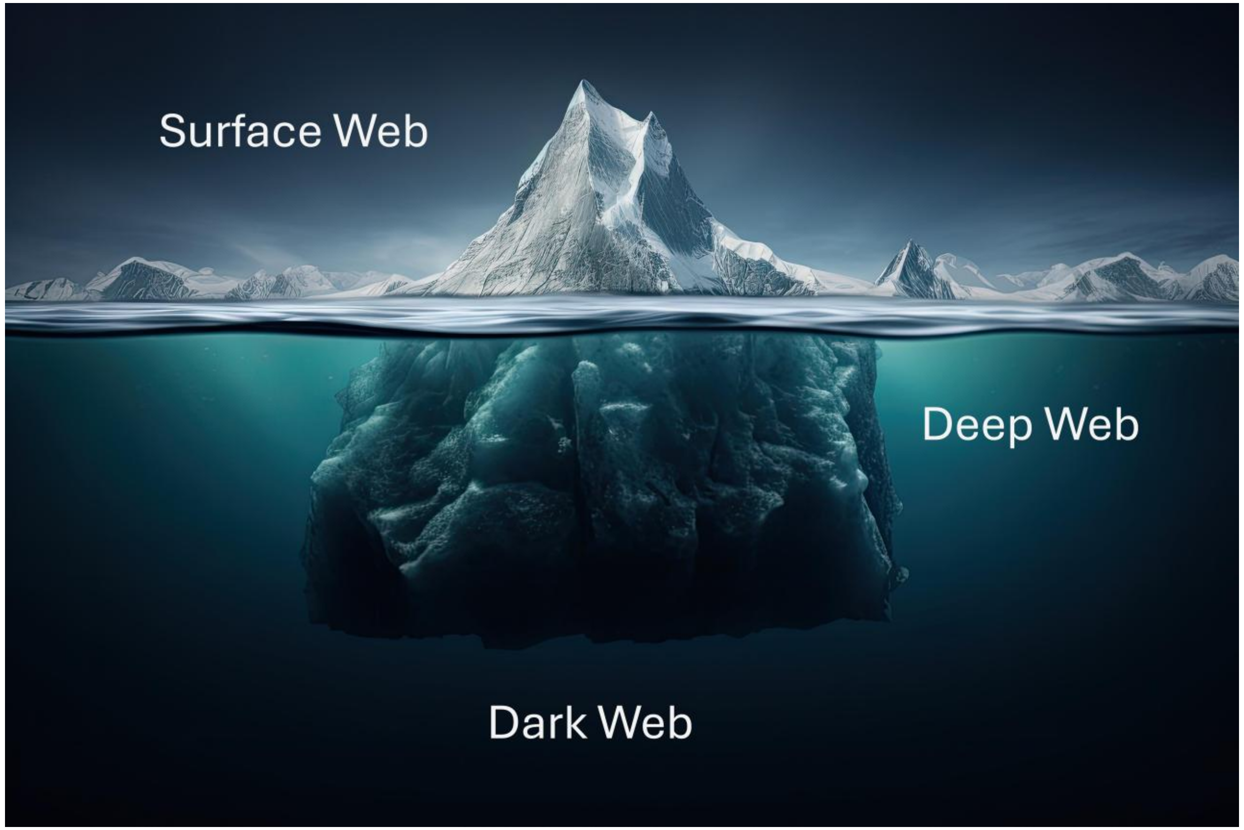
- Definition of the Surface, Deep, and Dark Web

Understanding The Dark Web

- **Surface Web: Publicly indexed content**. The Surface Web, also known as the Visible Web or Indexed Web, consists of all websites and web pages indexed by standard search engines like Google, Bing, and Yahoo.

- **Deep Web: Non-indexed content like databases**. The Deep Web encompasses all online content that is not indexed by standard search engines. This includes any web pages behind paywalls that require authentication or are dynamically generated in response to a user's query.

- **Dark Web:** The Dark Web is a subset of the Deep Web that is intentionally hidden **and requires specific software**, configurations, or authorization. It operates on overlay networks that use the Internet but require specialized protocols for access.



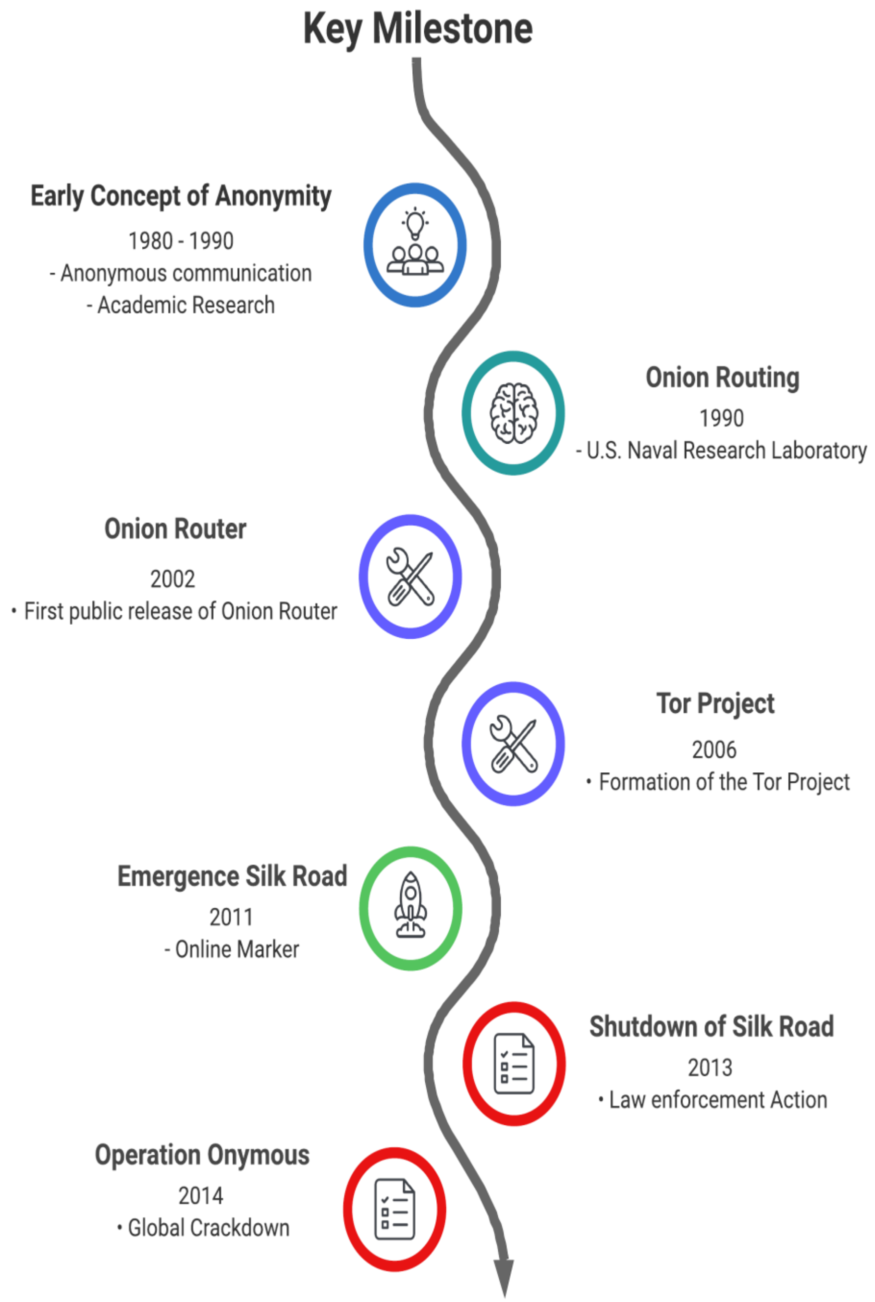
Understanding The Dark Web

History and Evolution

Early concepts of anonymous communication

Development of Onion Routing and the Tor network

Key milestones (e.g., Silk Road, Operation Onymous)



Key Milestone

Early Concept of Anonymity
1980 - 1990
- Anonymous communication
- Academic Research

Onion Routing
1990
- U.S. Naval Research Laboratory

Onion Router
2002
• First public release of Onion Router

Tor Project
2006
• Formation of the Tor Project

Emergence Silk Road
2011
- Online Marker

Shutdown of Silk Road
2013
• Law enforcement Action

Operation Onymous
2014
• Global Crackdown

Understanding The Dark Web

The Tor Network:

- How it works (onion routing)

Alternative networks:

- I2P
- Freenet

Understanding The Dark Web

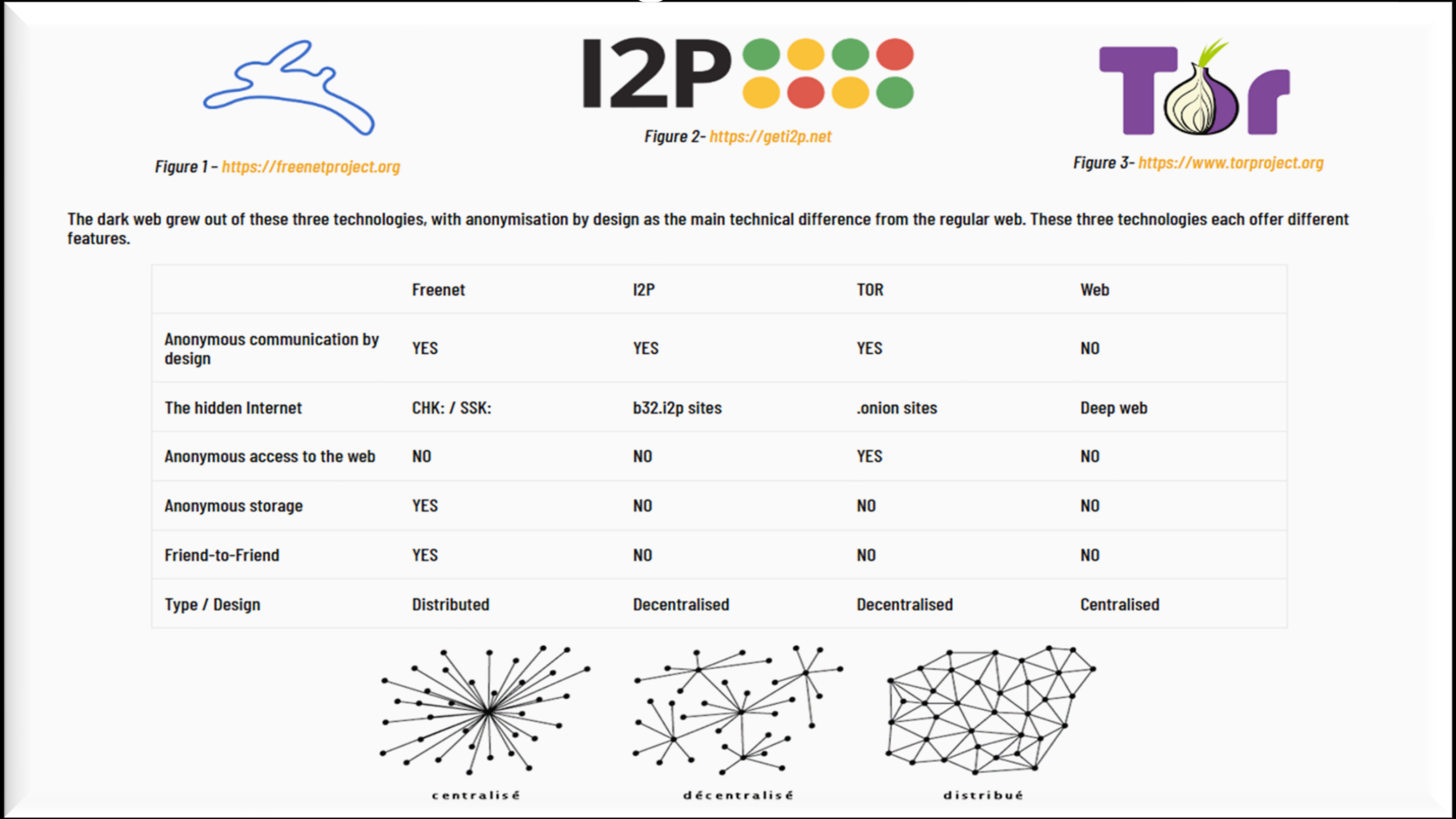


Figure 1 – https://freenetproject.org

Figure 2- https://geti2p.net

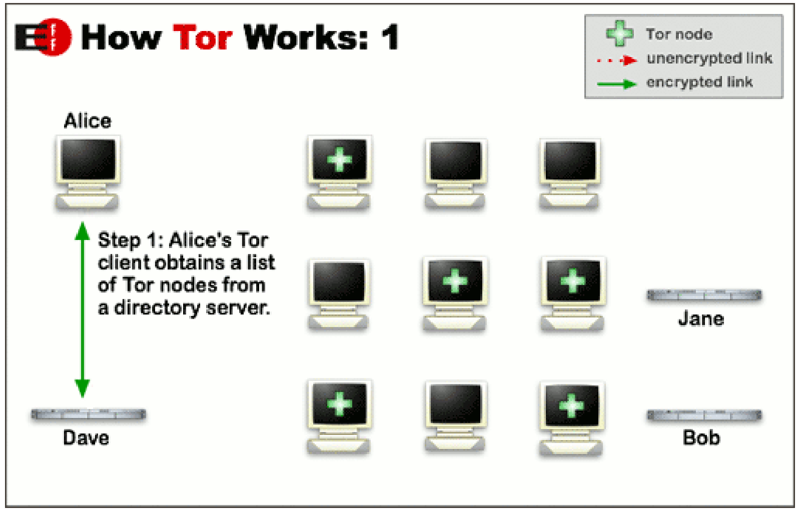
Figure 3- https://www.torproject.org

The dark web grew out of these three technologies, with anonymisation by design as the main technical difference from the regular web. These three technologies each offer different features.

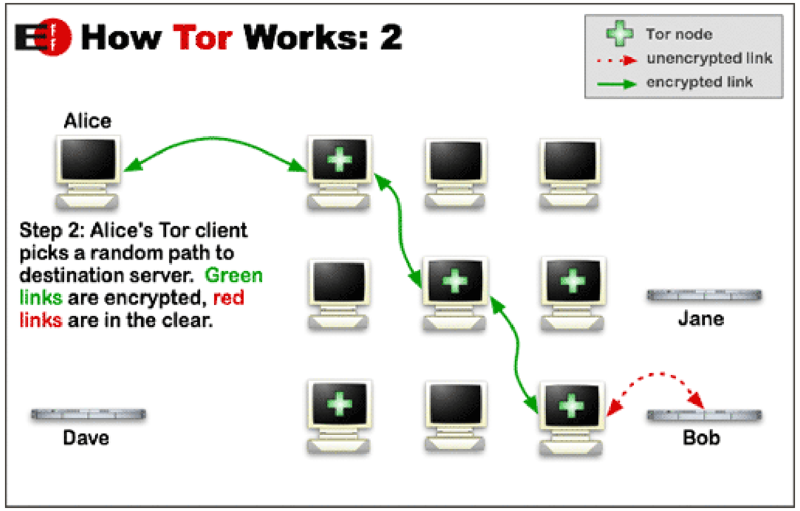
	Freenet	I2P	TOR	Web
Anonymous communication by design	YES	YES	YES	NO
The hidden Internet	CHK: / SSK:	b32.i2p sites	.onion sites	Deep web
Anonymous access to the web	NO	NO	YES	NO
Anonymous storage	YES	NO	NO	NO
Friend-to-Friend	YES	NO	NO	NO
Type / Design	Distributed	Decentralised	Decentralised	Centralised

Understanding The Dark Web

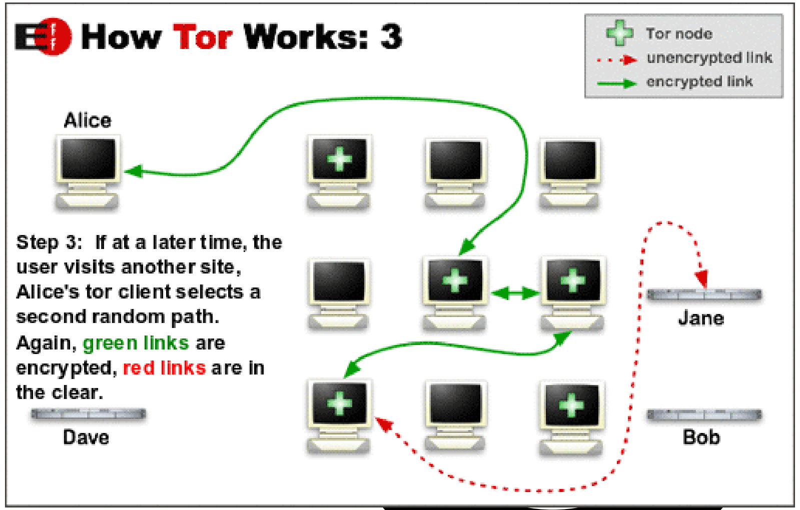
The Tor Network


How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.


How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

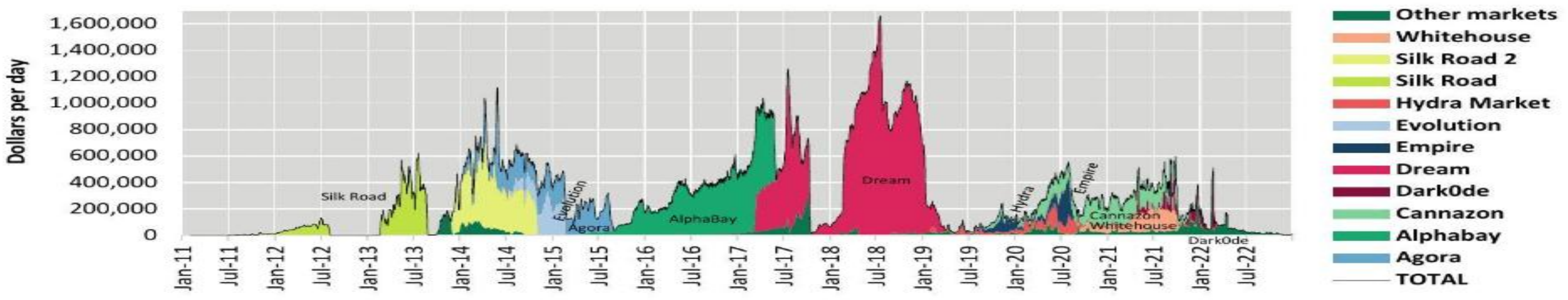

How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Risks and Illicit Activities

- **Illicit Activities on the Dark Web**
- Overview of illegal marketplaces
- Cybersecurity threats: Malware, phishing, and ransomware

FIG. 16 Daily minimum sales (mostly drug-related: >90 per cent) on 39 major global darknet markets, 2011–2022



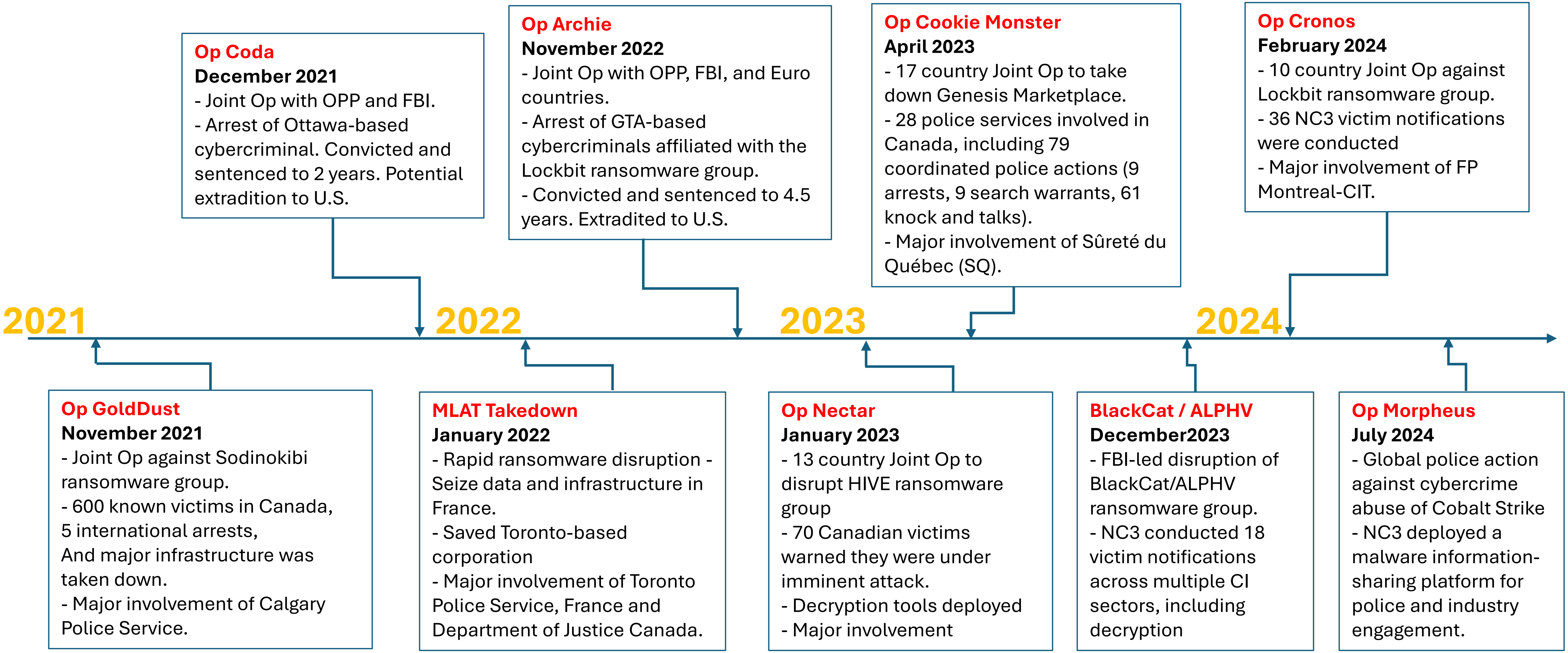
Source: UNODC analysis based on Hikari Labs data (see online Methodological Annex).

Risks and Illicit Activities

- **Information from National Cybercrime Coordination Centre (NC3)**
  - Ransomware remains the top global cybercrime threat
  - 400-500 incidents reported/ year
  - Cybersecurity threats: Malware, phishing, and ransomware

Risks and Illicit Activities

NC3 Coordinated Operations



Op GoldDust
November 2021
- Joint Op against Sodinokibi ransomware group.
- 600 known victims in Canada, 5 international arrests, And major infrastructure was taken down.
- Major involvement of Calgary Police Service.

Op Coda
December 2021
- Joint Op with OPP and FBI.
- Arrest of Ottawa-based cybercriminal. Convicted and sentenced to 2 years. Potential extradition to U.S.

MLAT Takedown
January 2022
- Rapid ransomware disruption - Seize data and infrastructure in France.
- Saved Toronto-based corporation
- Major involvement of Toronto Police Service, France and Department of Justice Canada.

Op Archie
November 2022
- Joint Op with OPP, FBI, and Euro countries.
- Arrest of GTA-based cybercriminals affiliated with the Lockbit ransomware group.
- Convicted and sentenced to 4.5 years. Extradited to U.S.

Op Nectar
January 2023
- 13 country Joint Op to disrupt HIVE ransomware group
- 70 Canadian victims warned they were under imminent attack.
- Decryption tools deployed
- Major involvement

Op Cookie Monster
April 2023
- 17 country Joint Op to take down Genesis Marketplace.
- 28 police services involved in Canada, including 79 coordinated police actions (9 arrests, 9 search warrants, 61 knock and talks).
- Major involvement of Sûreté du Québec (SQ).

BlackCat / ALPHV
December2023
- FBI-led disruption of BlackCat/ALPHV ransomware group.
- NC3 conducted 18 victim notifications across multiple CI sectors, including decryption

Op Cronos
February 2024
- 10 country Joint Op against Lockbit ransomware group.
- 36 NC3 victim notifications were conducted
- Major involvement of FP Montreal-CIT.

Op Morpheus
July 2024
- Global police action against cybercrime abuse of Cobalt Strike
- NC3 deployed a malware information-sharing platform for police and industry engagement.

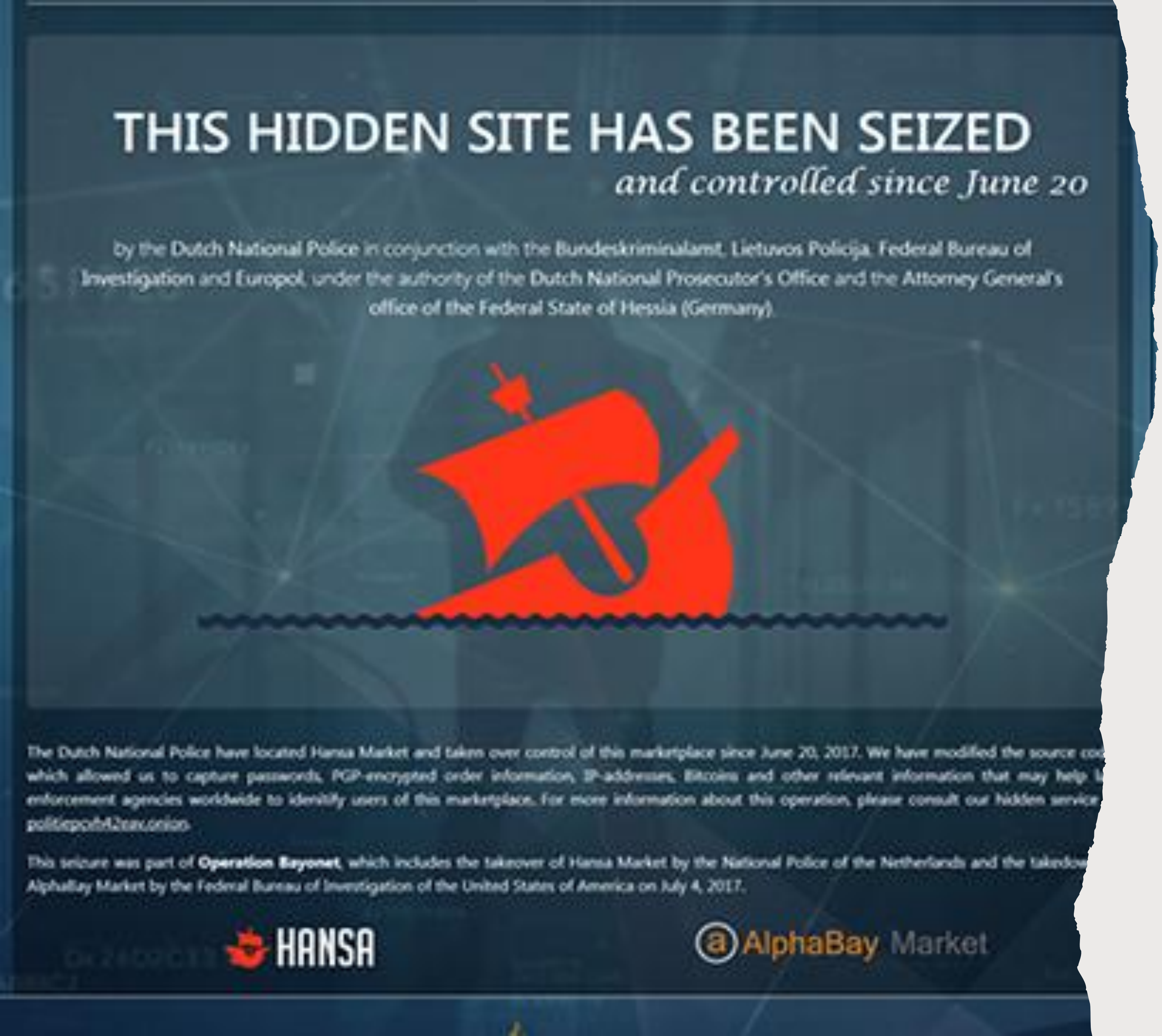
Risks and Illicit Activities

Organization

Phishing and Malware Threats

Individual

Scams and Fraud



THIS HIDDEN SITE HAS BEEN SEIZED

and controlled since June 20

by the **Dutch National Police** in conjunction with the **Bundeskriminalamt**, **Lietuvos Policija**, **Federal Bureau of Investigation** and **Europol**, under the authority of the **Dutch National Prosecutor's Office** and the **Attorney General's office of the Federal State of Hessia (Germany)**.

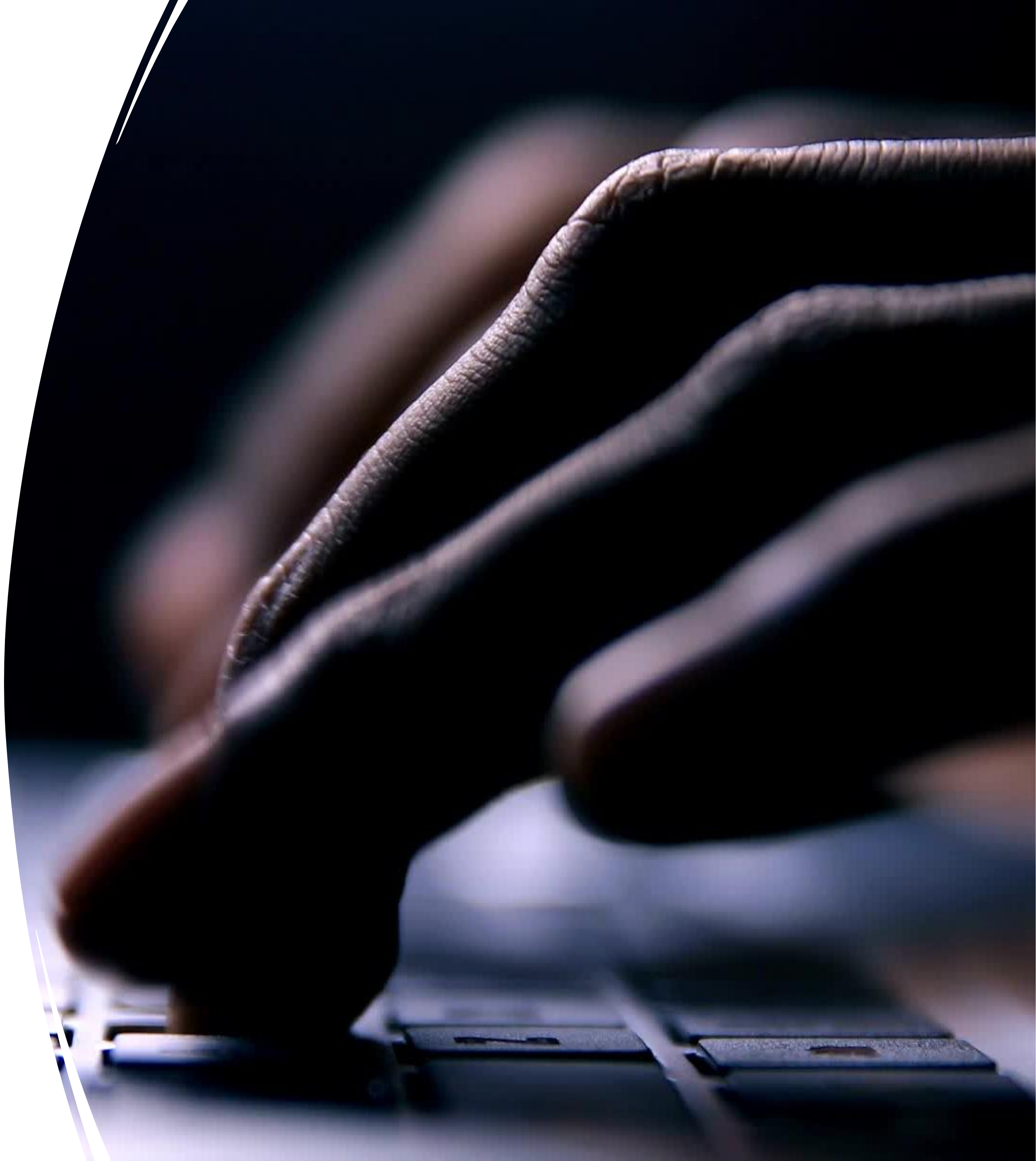
The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source cod which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help l enforcement agencies worldwide to identify users of this marketplace. For more information about this operation, please consult our hidden service politiepcvh42eav.onion.

This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takedow AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

Risks and Illicit Activities

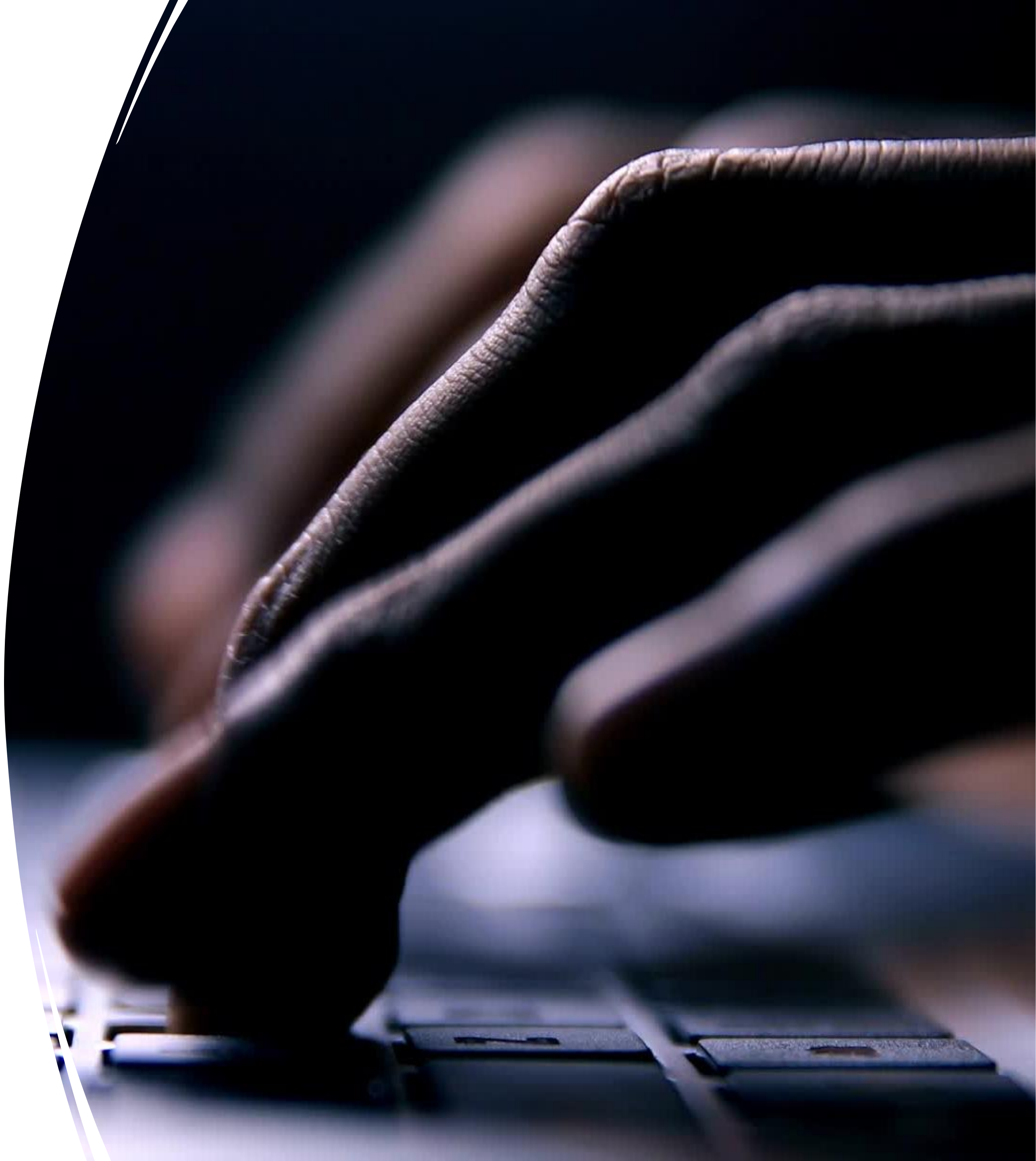
Precautions

- Be aware of legal consequences
- Utilize secure tools
- Safeguard your identity



Precautions

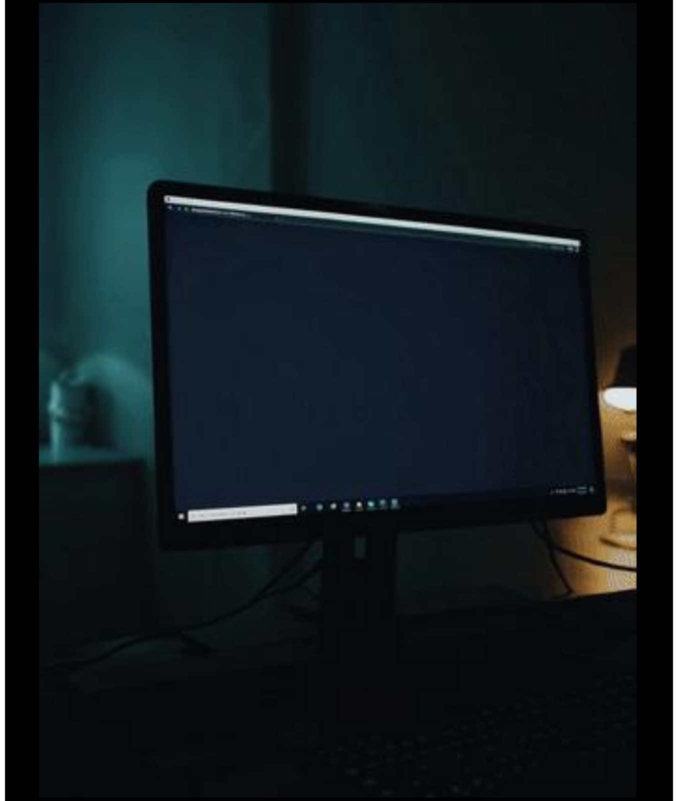
- Be Cautious with Downloads
- Financial Precautions
- Monitor Network Traffic



Precautions for this Presentation

- All the connections are using VPN (Netherlands is the exit)
- Using a Container running in a server in Singapore
- From the Container, connecting to the Dark Web using the TOR
- Why am I using a container?
  - Every time I go to the Dark Web, I start a new container
  - After I finish my threat hunting, I destroy the container

Before Diving in The Dark Web

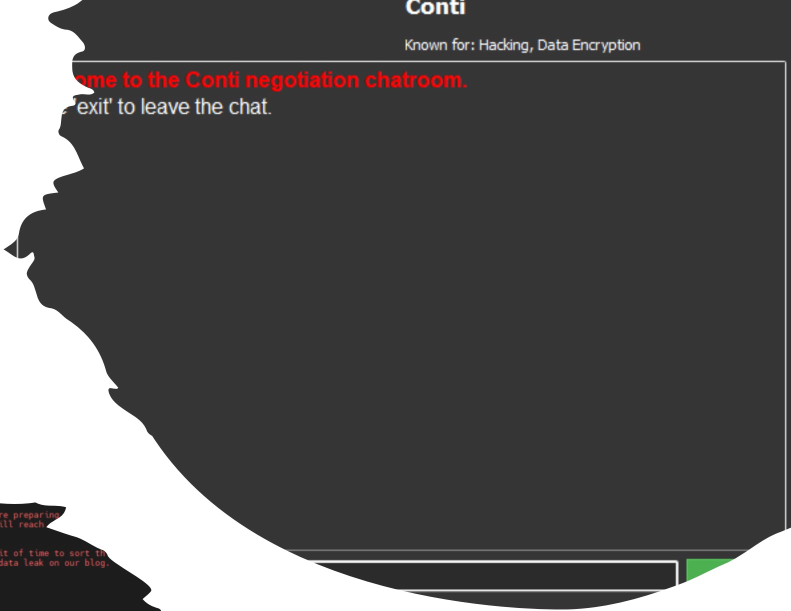


Sites you can use to find Dark Web Information

- **Blockchain Explorer**
  https://www.blockchain.com/explorer
- **Ransomware.Live**
  https://www.ransomware.live/
- **Ransonwatch**
  https://ransomwatch.telemetry.ltd/
- **Dark Web Informer**

  https://darkwebinformer.com/

Before Diving in the Dark Web



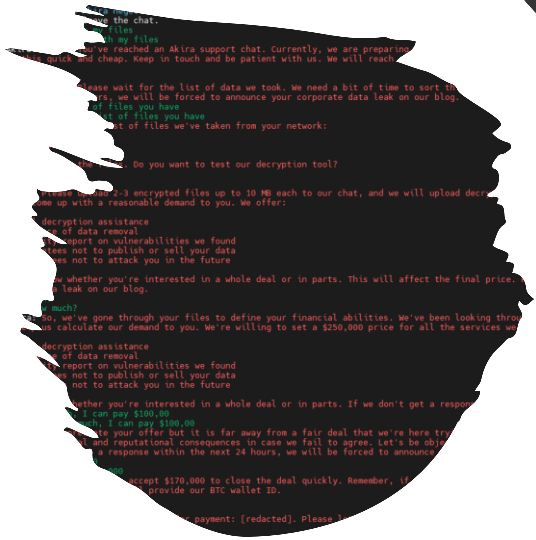
Conti

Known for: Hacking, Data Encryption

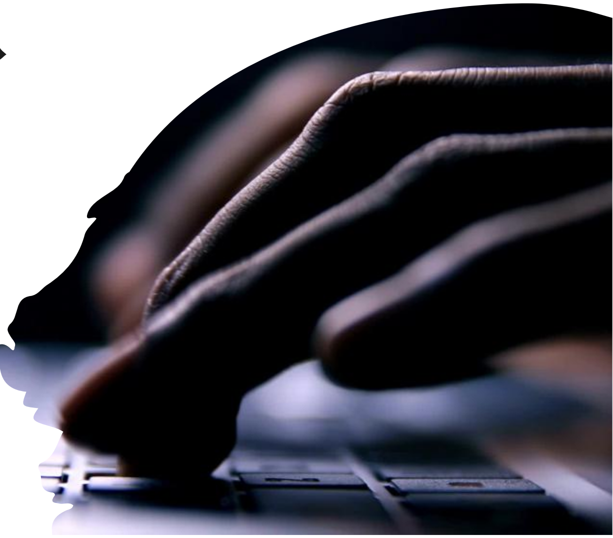
```
ome to the Conti negotiation chatroom.
'exit' to leave the chat.
```

Ransomware Chat Simulation

- Python script for simulating chat negotiations with ransomware groups based on real-world behaviour patterns.
- Simulate negotiations and learn about the behaviour
- CLI and GUI version
- https://github.com/toniall/ransomchat/



```
 kira nego
  ave the chat.
    my files
    th my files
    ou've reached an Akira support chat. Currently, we are preparing
 this quick and cheap. Keep in touch and be patient with us. We will reach

    lease wait for the list of data we took. We need a bit of time to sort th
    rs, we will be forced to announce your corporate data leak on our blog.
    of files you have
    ist of files you have
    st of files we've taken from your network:


    the    s. Do you want to test our decryption tool?


  Please upload 2-3 encrypted files up to 10 MB each to our chat, and we will upload decry
 ome up with a reasonable demand to you. We offer:

  decryption assistance
   ce of data removal
   ity report on vulnerabilities we found
   ntees not to publish or sell your data
    ees not to attack you in the future

    w whether you're interested in a whole deal or in parts. This will affect the final price.
   a leak on our blog.

  w much?
 a: So, we've gone through your files to define your financial abilities. We've been looking throu
    us calculate our demand to you. We're willing to set a $250,000 price for all the services we

  decryption assistance
   e of data removal
   ity report on vulnerabilities we found
    es not to publish or sell your data
    not to attack you in the future

    hether you're interested in a whole deal or in parts. If we don't get a respons
    , I can pay $100,00
    much, I can pay $100,00
    ate your offer but it is far away from a fair deal that we're here try
    l and reputational consequences in case we fail to agree. Let's be obje
     a response within the next 24 hours, we will be forced to announce
    0
    000
     accept $170,000 to close the deal quickly. Remember, if
     l provide our BTC wallet ID.


     r payment: [redacted]. Please le
```



The Art of War by Sun Tzu

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

Hands-On Activities - Diving in the Dark Web

- **Using the Tor Browser**
  - Steps to download
  - Configuration and best practices

Hands-On Activities
Diving in the Dark Web

- **Creating a Hidden Service**
  - Creating a Web Site in the Dark Web
  - Practical demonstration with Flask and Docker
  - Using the Docker Container

Hands-On Activities
Web Site

```
# sudo apt install tor

# apt install nginx

# systemctl start nginx

# sudo systemctl enable nginx

# sudo nano /var/www/html/index.nginx-debian.html
```

```
# nano /etc/tor/torrc

HiddenServiceDir /var/lib/tor/hidden_service/

HiddenServicePort 80 127.0.0.1:80

# sudo systemctl start tor

# sudo cat /var/lib/tor/hidden_service/hostname
```

Hands-On Activities - Diving in the Dark Web

- **Using the OnionShare**
  - Steps to download and install Onionshare cli
  - Accessing the Chat
  - Using the Docker Container

Hands-On Activities OnionShare

```
# mkdir onionshare

# cd onionshare/

# apt install tor

# systemctl start tor

# systemctl enable tor

# su - user
```

```
$ python3 -m venv appenv

$ source appenv/bin/activate-

$ sudo snap install onionshare

$ pip install --upgrade pip

$ pip3 install onionshare-cli

$ onionshare-cli --chat
```

Hands-On Activities
Diving in the Dark Web

- **Creating a Tor Relay**
  - Creating a Tor Relay
  - Verify the Connections
  - Using the Server

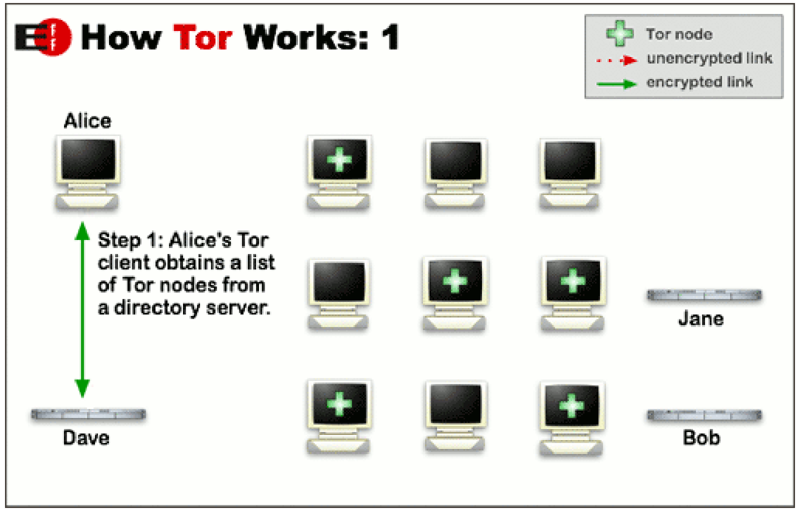
Hands-On Activities - Tor Relay

```
# apt-get update

# apt-get upgrade

# apt-get install tor
```

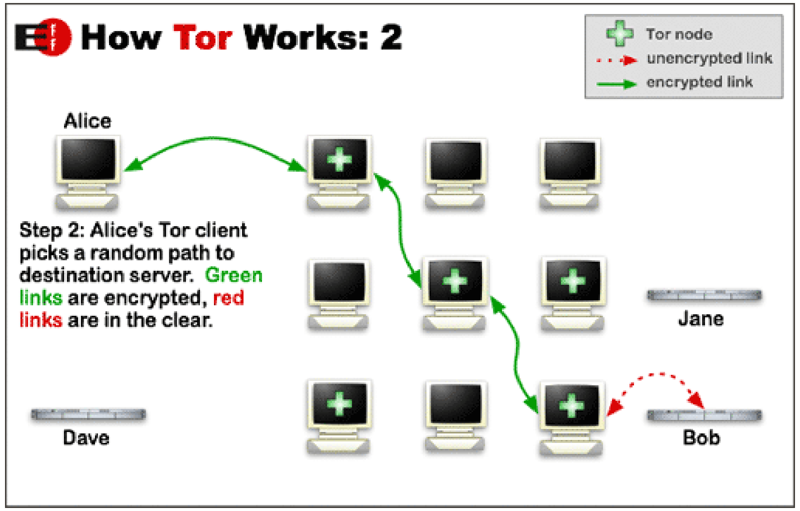
```
# nano /etc/tor/torrc


Nickname MyTorExitRelay
ORPort 9001
SocksPort 0
ExitRelay 1
ExitPolicy accept *:80, accept *:443, accept *:53, reject *:*


# sudo systemctl restart tor
```

Understanding the Dark Web

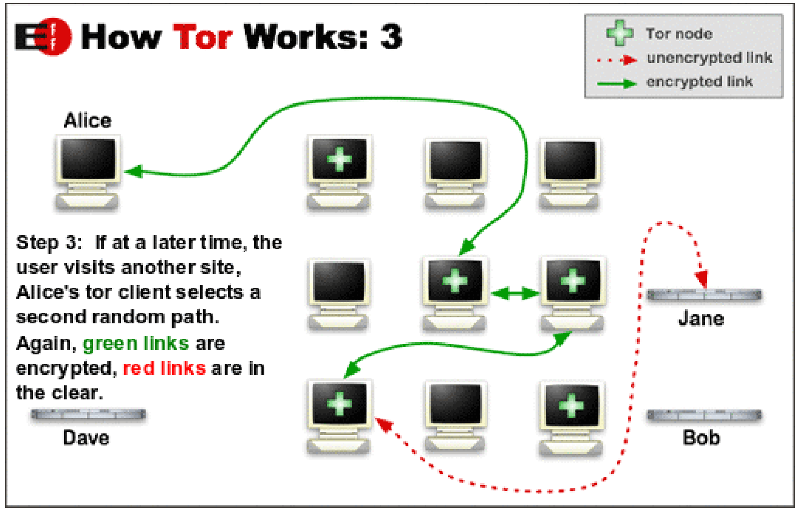
The Tor Network



Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.



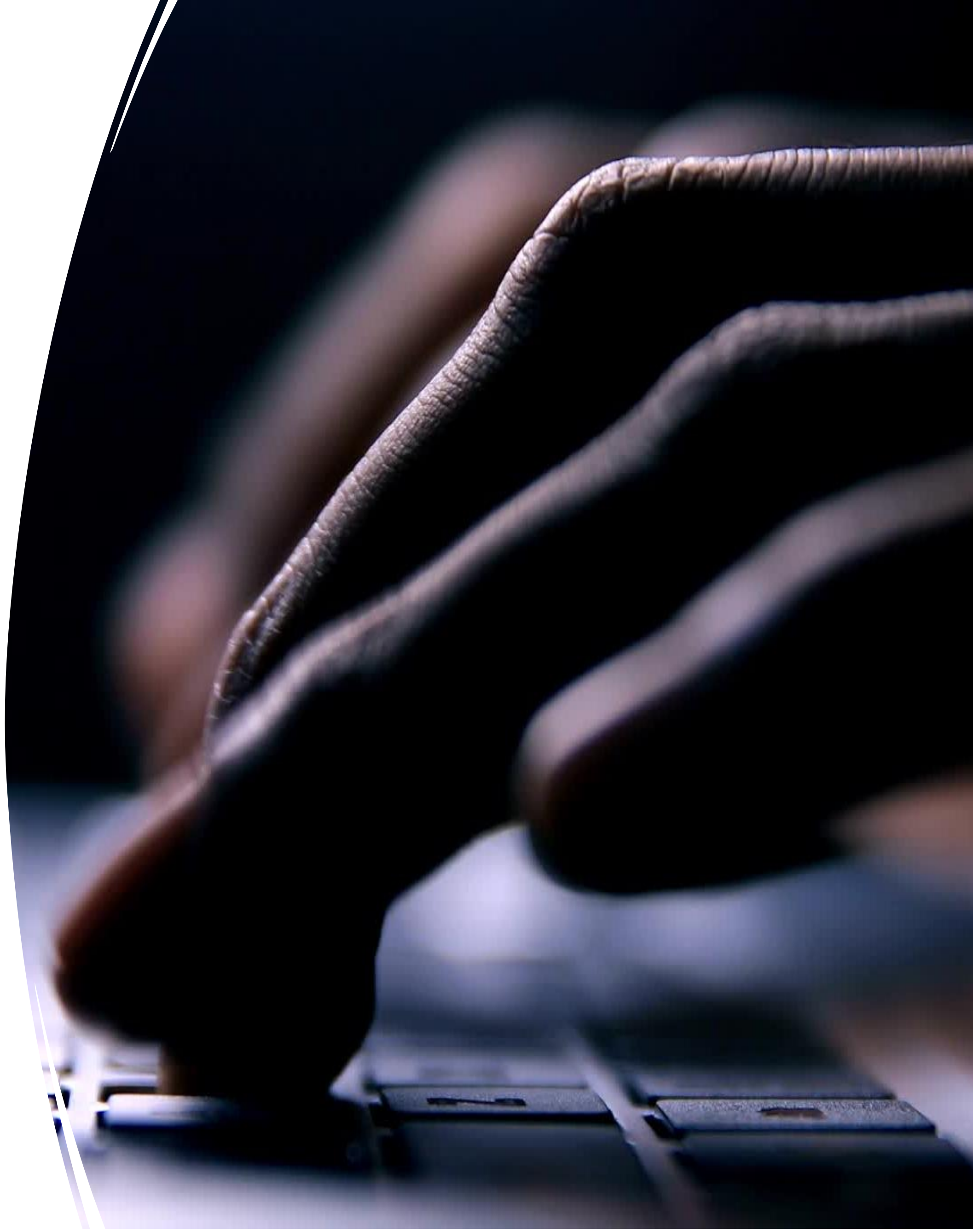
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Hands-On Activities Diving in the Dark Web

- **Creating a Docker Container**
  - Github
  - Clone the repository
  - Building the image
  - Run the container

Hands-On Activities
Diving in the Dark Web

- Creating a Docker Container
- https://github.com/toniall/DarkWebCourse/



Key Takeaways

- Dual nature of the Dark Web (positive and negative)
- Importance of ethical use

Conclusion

Final Reflections

Challenges and opportunities of the Dark Web

Importance of ongoing education and ethical engagement

Hic Sunt Dracones

Latin - "Here be Dragons."

Dangerous or new territories

Dragons, sea monsters and other mythological creatures

The potential dangers were not enough to stop sailors from sailing around the world.

Conclusion

- **Q&A Session**
- Open floor for participant questions

# ~# Contact

Shared Services for Higher Education & Research

- BCNET
- Cybersecurity Architect
- Threat Hunter / Purple Teamer
- Email: antonio.brandao@bc.net

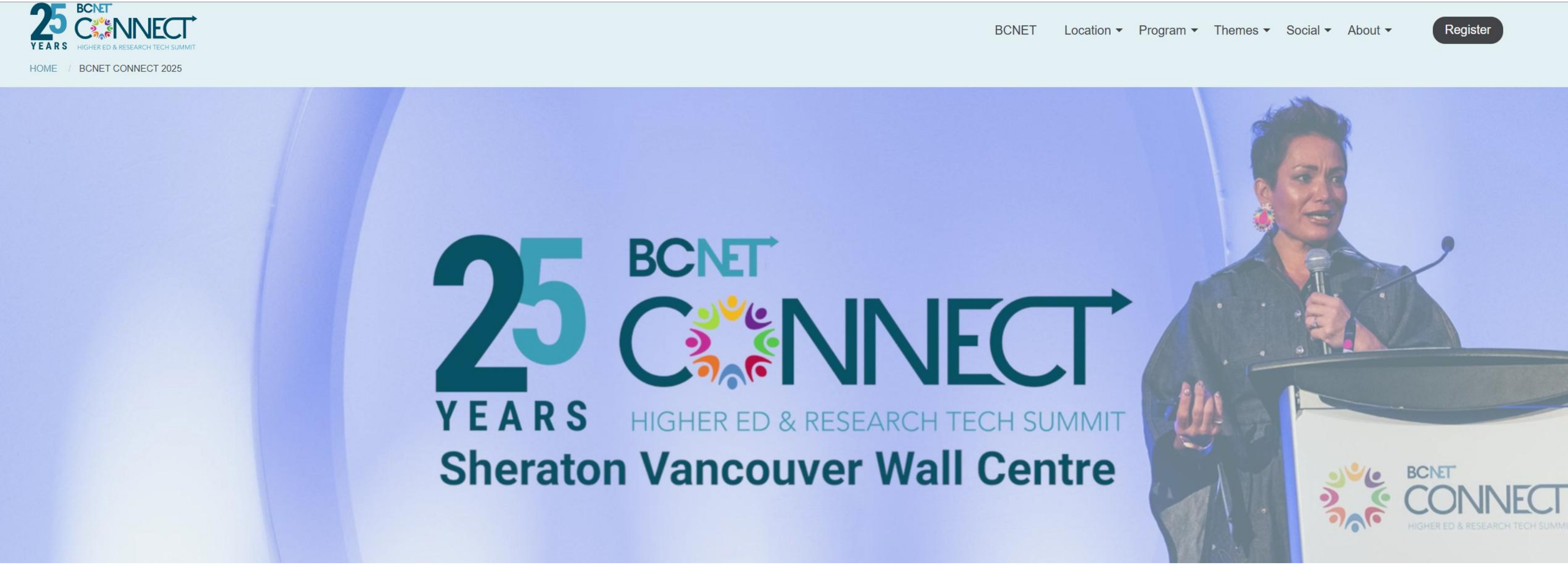
- https://www.linkedin.com/in/brandao-antonio/

Antonio Brandao

Cybersecurity Architect - Threat Hunting - CISSP - GSOM - GEIR - GCDA - GWAPT - SANS LDR551 - FOR508 - FOR608 - SEC587 - SEC555 - Veteran Brazilian Army Infantry Lieutenant Colonel

BCNET Connect 2025 - March 31st to April 3rd

https://www.bc.net/connect/


25 YEARS BCNET CONNECT HIGHER ED & RESEARCH TECH SUMMIT
BCNET
Location
Program
Themes
Social
About
Register
HOME / BCNET CONNECT 2025
BCNET CONNECT HIGHER ED & RESEARCH TECH SUMMIT

25 YEARS BCNET CONNECT

HIGHER ED & RESEARCH TECH SUMMIT

Sheraton Vancouver Wall Centre