OLD DOMINION UNIVERSITY

Internet Security Research Lab

Shuai Hao
Assistant Professor
Computer Science
Old Dominion University
shao@odu.edu

WHO ARE WE

Faculty

- Dr. **Shuai Hao,** Assistant Professor
  Department of Computer Science
  Old Dominion University
  - Ph.D., Computer Science
    College of William and Mary, 2017
  - Postdoctoral Researcher
    UC San Diego, 2018 - 2019

Ph.D. Students

- Xiaoqin Liang, *2019 -*
- Skanda Dhanushkanda, *2021 -*
- Mustafa Ibrahim, *2022 -*
- Marvin Fowlkes, *2022 -*

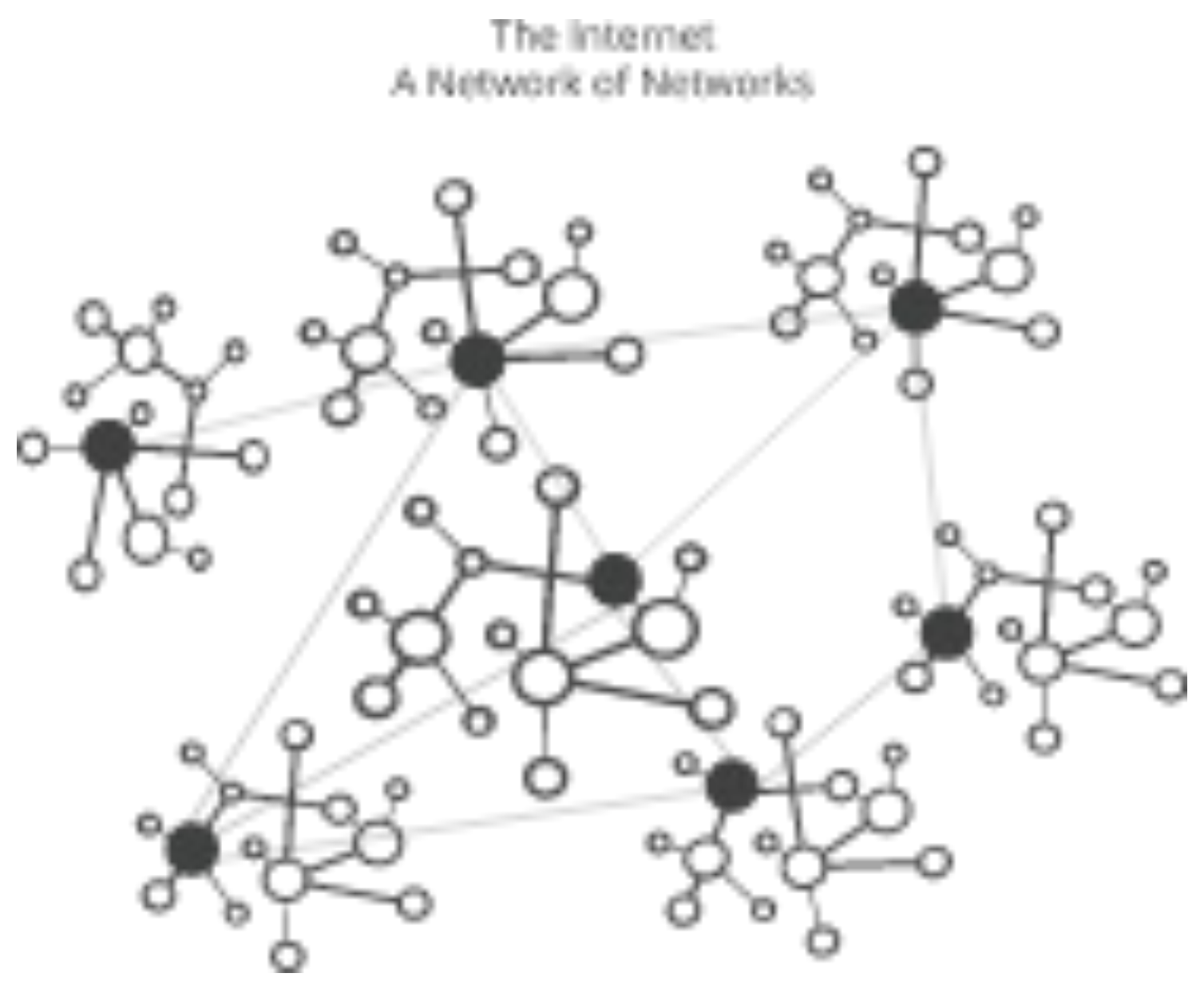
WHAT WE DO

We study Internet's Infrastructure, Components, and Security Issues

- **Internet Measurement**
  - Topology
  - Routing
  - Domain Name System
  - Content Delivery Networks
- **Internet Security**
  - Cryptographical Enhancement of the Internet (DNSSEC, RPKI, *etc.*)
  - Internet Censorship and Freedom
- **Web Security**
  - Underground Online Business
  - Online Ecosystem and Abuse
  - Defense against Online Tracking and Phishing

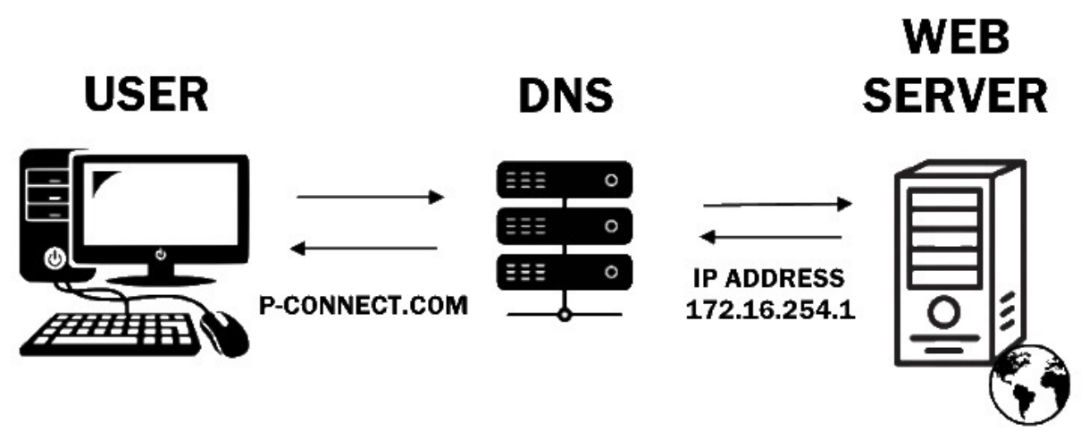
Research Area A
Internet Infrastructure and its Security Issues

- **Internet Routing**
  : the process of transmitting and routing packets over the Internet between two or more nodes



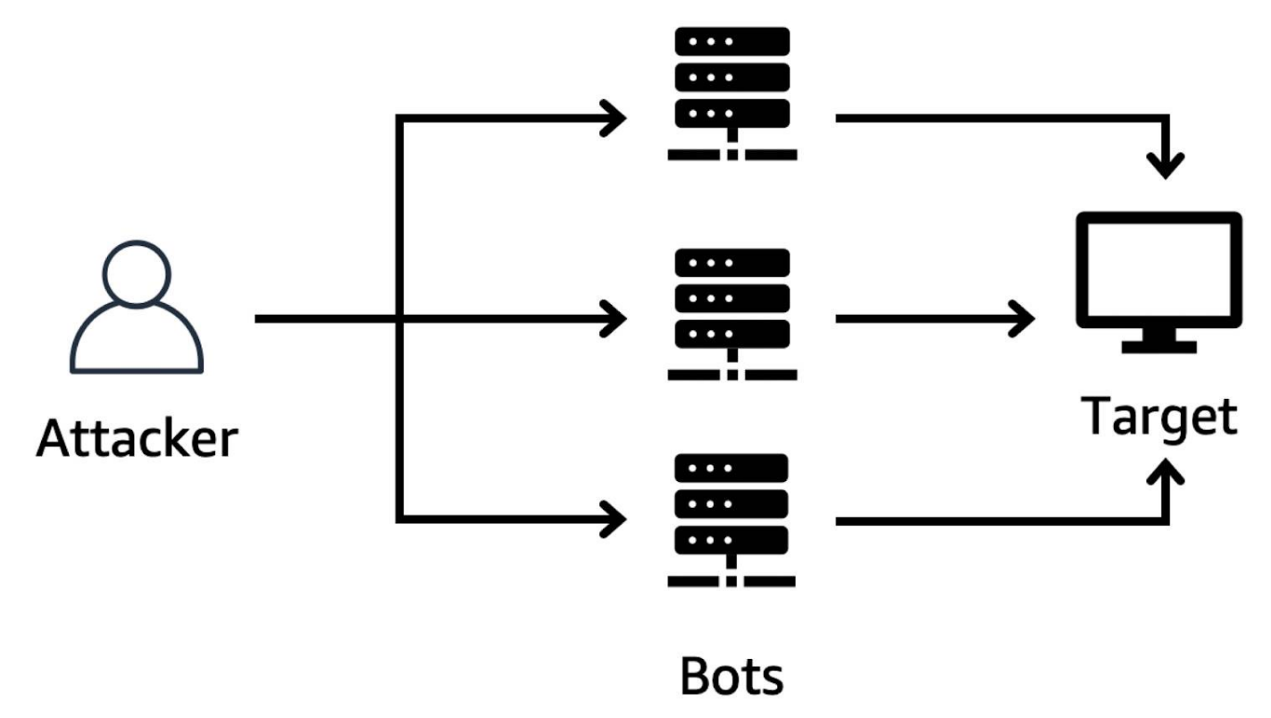
- Oct. 4, 2021, Facebook and its subsidiaries, including *Facebook*, *Messenger*, *Instagram*, *WhatsApp*, etc., became globally unavailable for a period of 6-7 hours
- The outage was caused by the loss of IP **Routing** to the Facebook's **Domain Name System**

- **Internet Components and Subsystems**
  : **Domain Name System**: translating a domain name (*e.g.*, *www.odu.edu*) to a network address (*e.g.*, 128.82.112.29)



- Oct. 21, 2016, Dyn's **DNS** system was attacked, causing many major Internet services and platforms unavailable, including *Airbnb, Amazon, CNN, Netflix, Twitter, etc.*
- The attack was a distributed denial-of-service (**DDoS**) attack launched from thousands of hosts

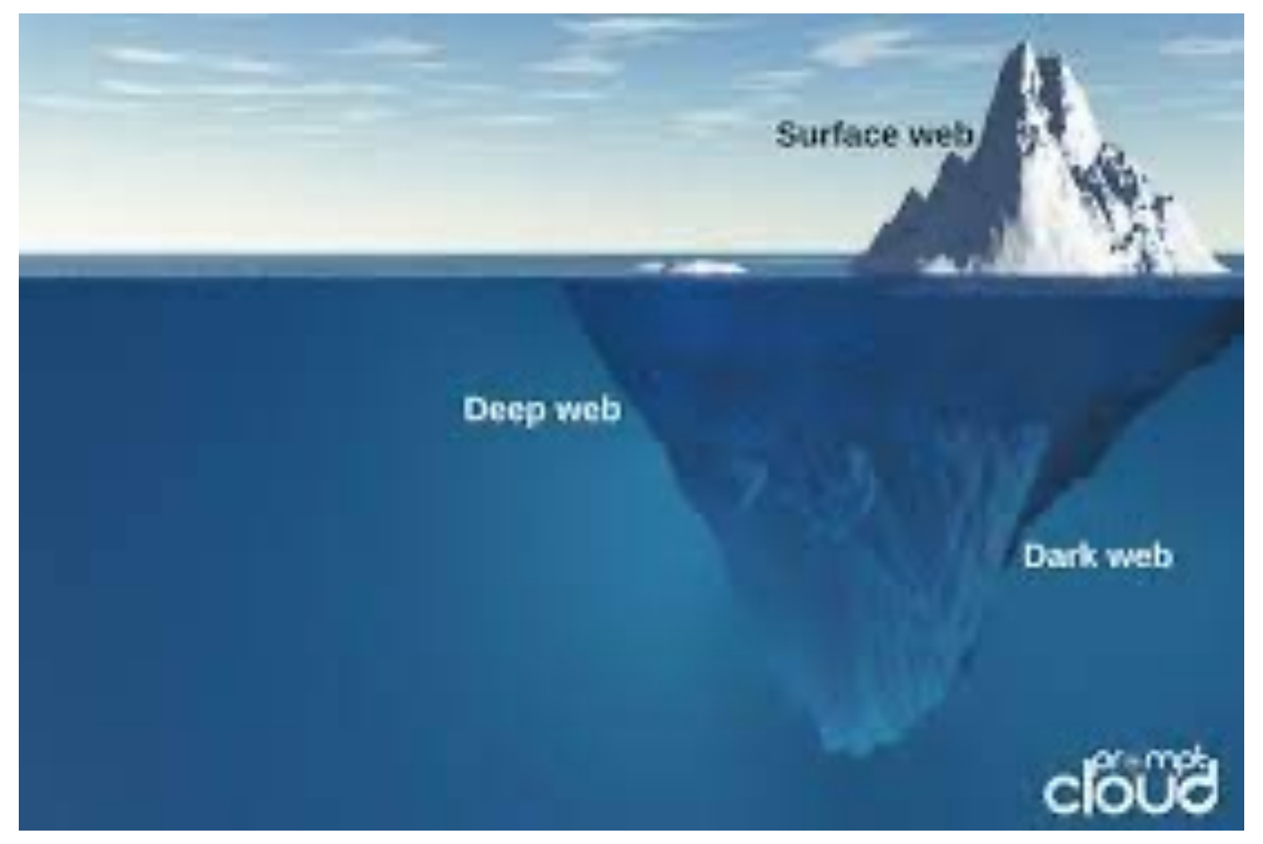
- **Internet Attack and Defense**
  : **DDoS Attack**: leverage thousands of hosts infected with malware to simultaneously send traffic to flood target system



- In 2018, the DDoS attack against Github reached 1.3T bps
- In 2021, the volume of DDoS attack against Microsoft reached 2.4T bps (22 million request per second!)

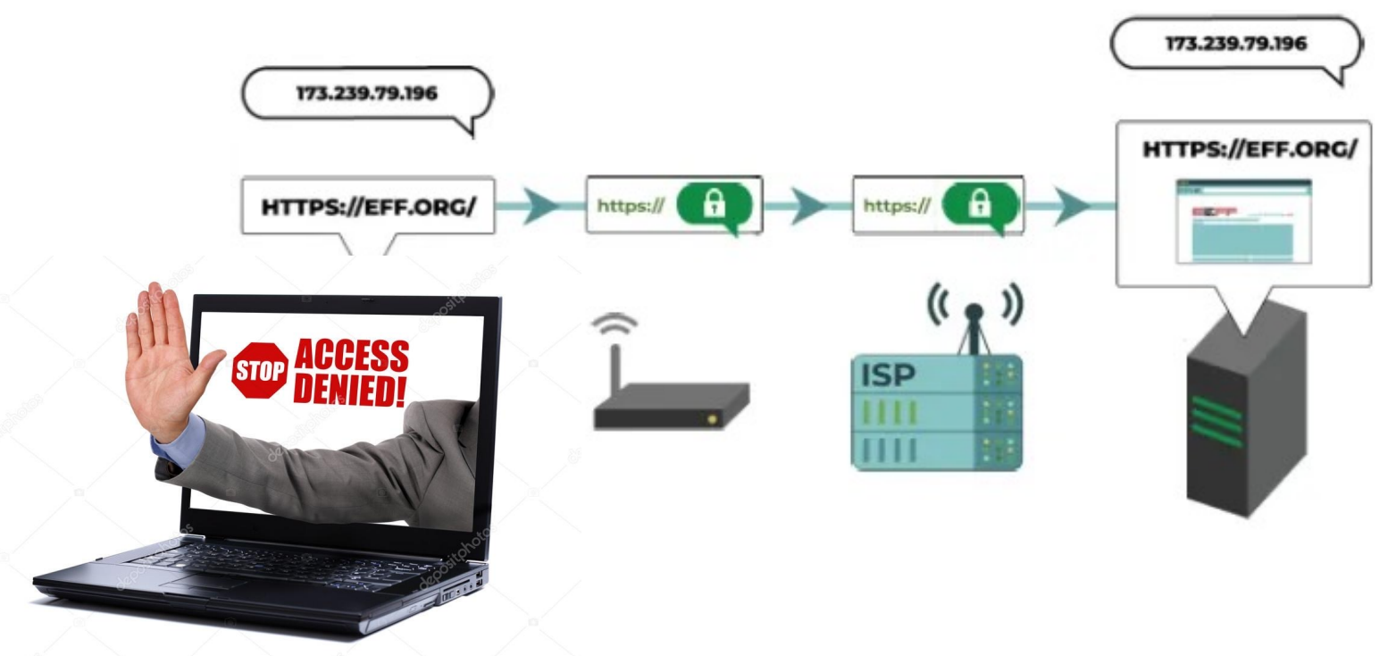
Research Area B
Web Security and Cybercrime

- **Underground Online Business**
  : Underground web activities that support economic transactions that are deemed illegal



- We measure and investigate the activities that fulfill the malicious purpose in online business systems
- We explore the ecosystem and the value chain that accomplish the underground economy

- **Internet Censorship**
  : Internet censorship controls what can be viewed by a certain group of Internet users, typically placed by authority entities such as governments or organizations



- We developed framework to investigate the state of Internet censorship in global scale
- We explored techniques that could be used for censorship circumvention

Potential Available Projects for Undergraduate Student Research

- **Study Internet with real traffic**: leverage the real, captured Internet requests (e.g., DNS queries) to identify and understand the underlying service dependency and security risks
- **Setup Honeypots to observe Internet malicious behavior**: Using public Internet recourses to setup Honeypots and attract attackers to visit, to observe and identify their purposes and behavior
- **Observe and explore Internet Censorship activities with developed framework**