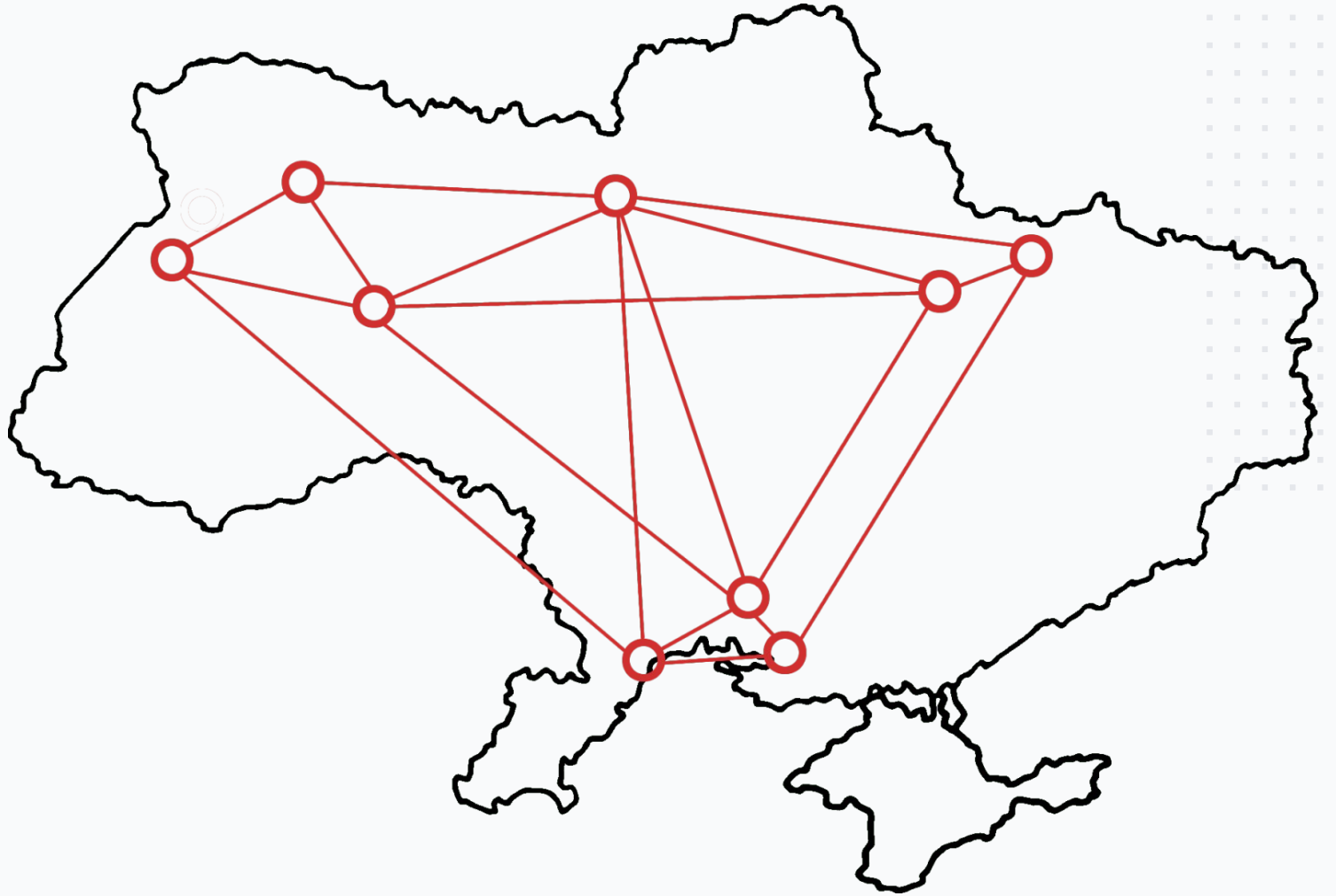
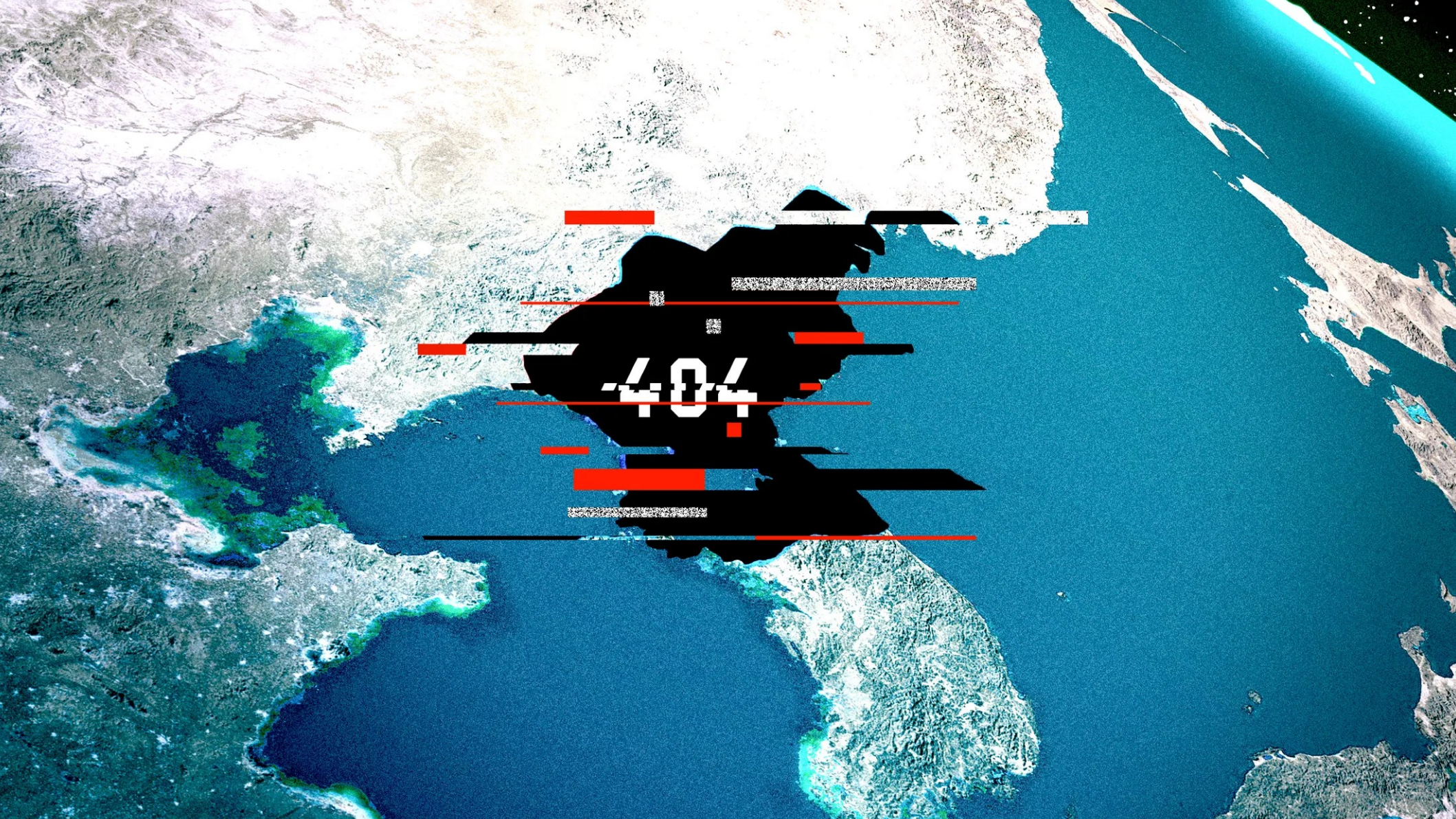


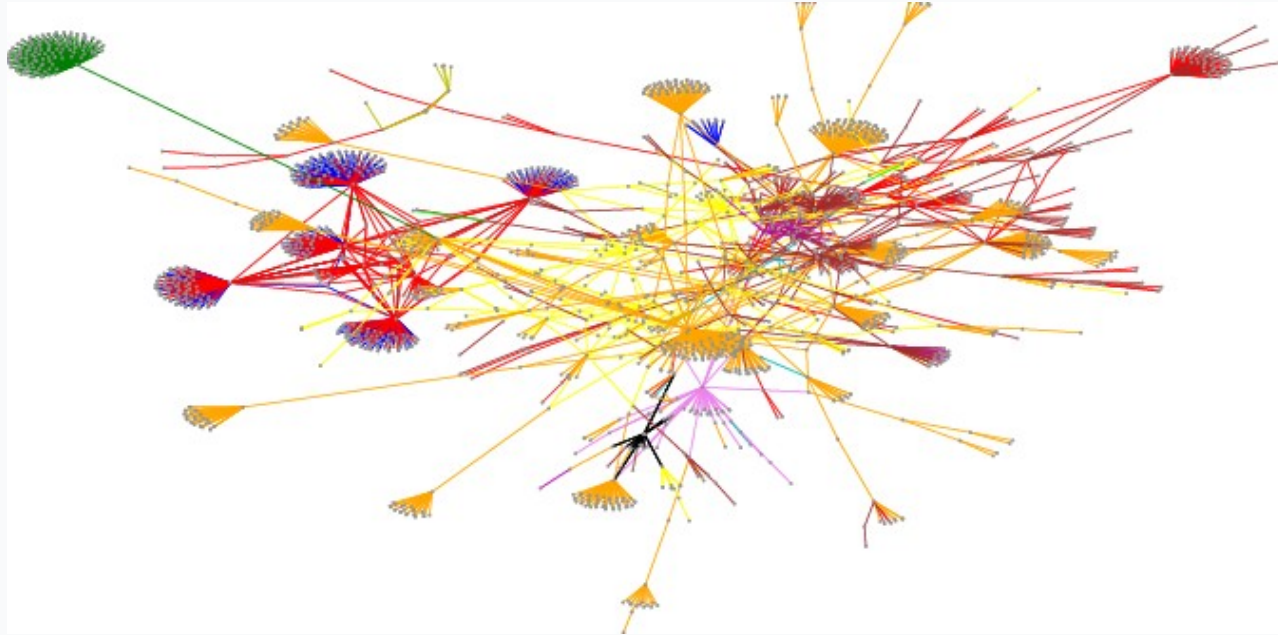
# Hosting Software Behind Enemy Lines





404





- The authorities in our target countries can see all of our traffic
- We cannot trust our “hardware“
- How do we do hosting when we don't trust anybody?

# How do the criminals do it?



**THIS WEBSITE HAS BEEN SEIZED**


This domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Central District of California under the authority of 18 U.S.C. §1030(i)(1)(A) as part of coordinated law enforcement action taken against illegal DDoS-for-hire services.


This action has been taken in coordination with the United States Attorney's Office of the District of Alaska, the Department of Justice Computer Crime and Intellectual Property Section, and

 **NCA**  
National Crime Agency

 **DEPARTMENT OF JUSTICE**  
**FEDERAL BUREAU OF INVESTIGATION**

 **POLITIE**

 **DEPARTMENT OF JUSTICE**

 **DEFENSES CRIMINAL INVESTIGATIVE SERVICE**  
PROTECTING AMERICA'S DEFENSES

# Dark Web Markets

- Focus on preventing detection
- Either take no precautions at the system level or they are easily bypassed by authorities
- Bug bounties

# thepiratebay.org

- All in the cloud
- Takes advantage of diff international law
- Fairly basic web app
- Portable



The Pirate Cloud



The Pirate Bay



- Full disk encryption
- Host in sketchy, legally undiscerning places
- Make connections with datacenters
- Dead-mans switches and physical security
- Tor
- Run database servers away from the public server
- Fly under the radar
- Many nodes
- Physical access means game over

# dComms?

- Small, disposable servers
- WLAN/hotspot comms
- Perfect slealth
- Host in safe zones
- ?