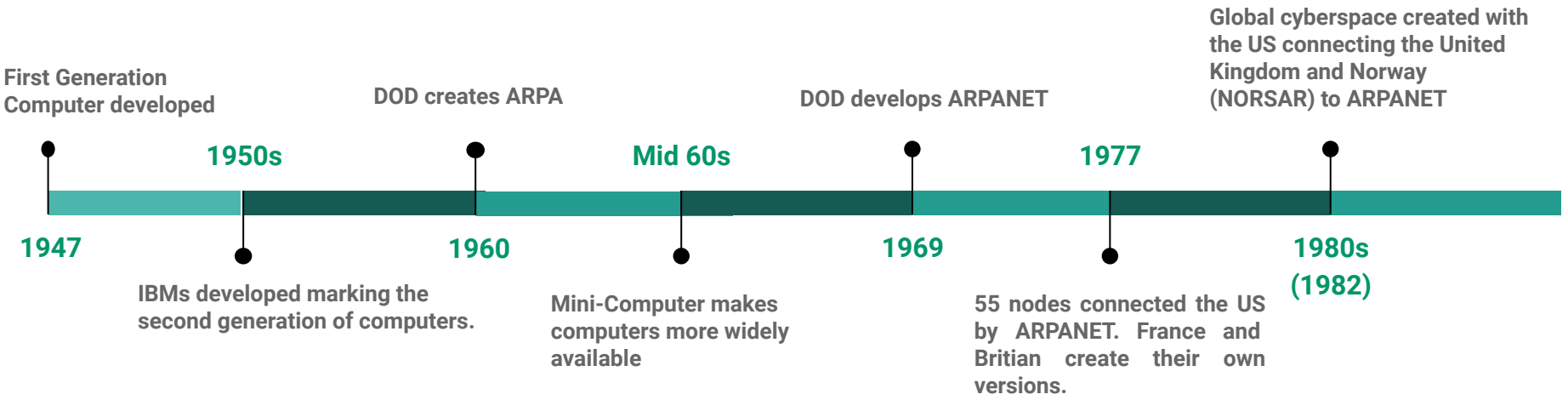
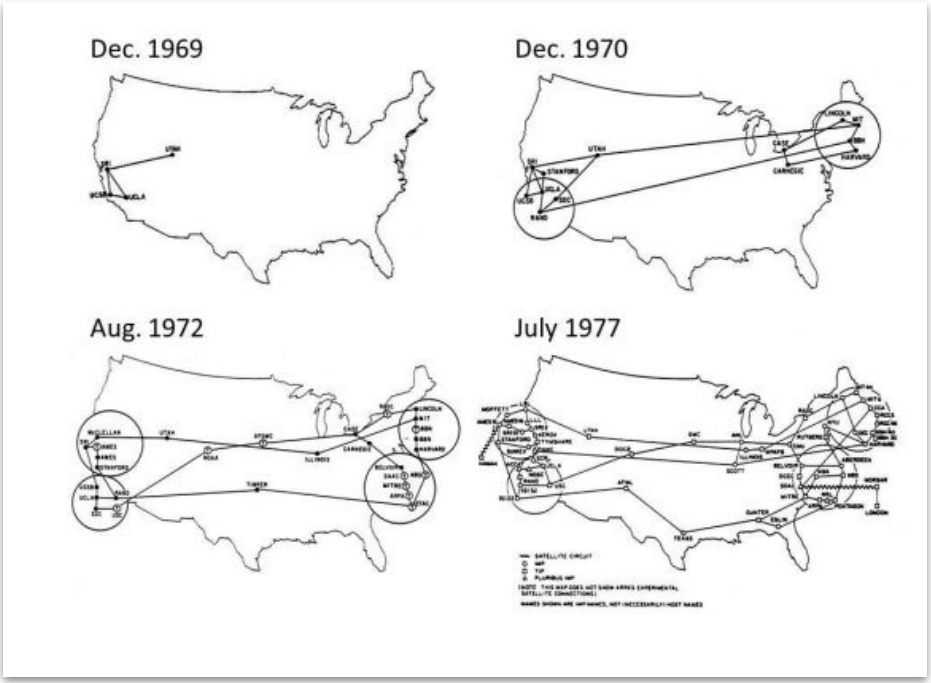
USA Cyber History and National Cybersecurity Strategy

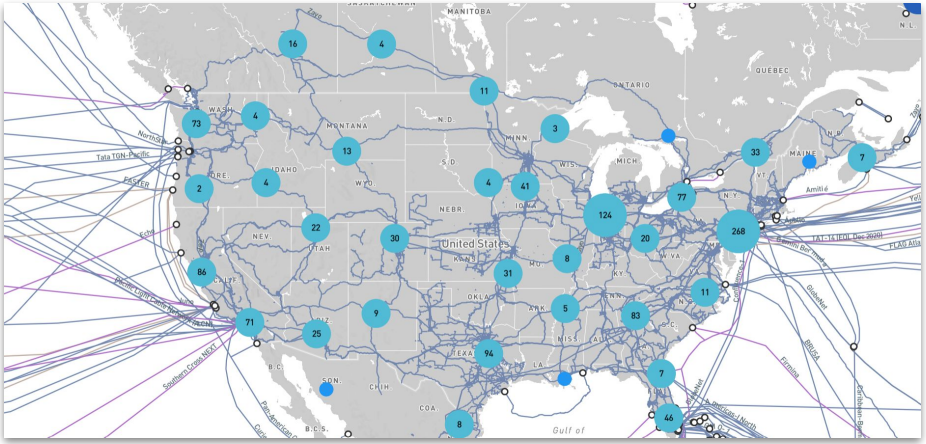
Team 6

1.1 The United States and Cyberspace: A Brief History



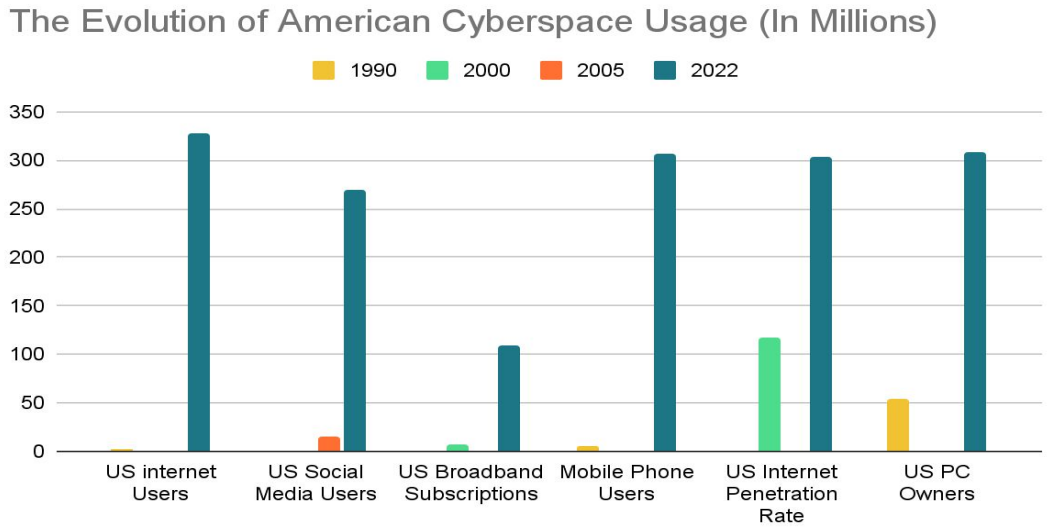
1.2 US Network Infrastructure



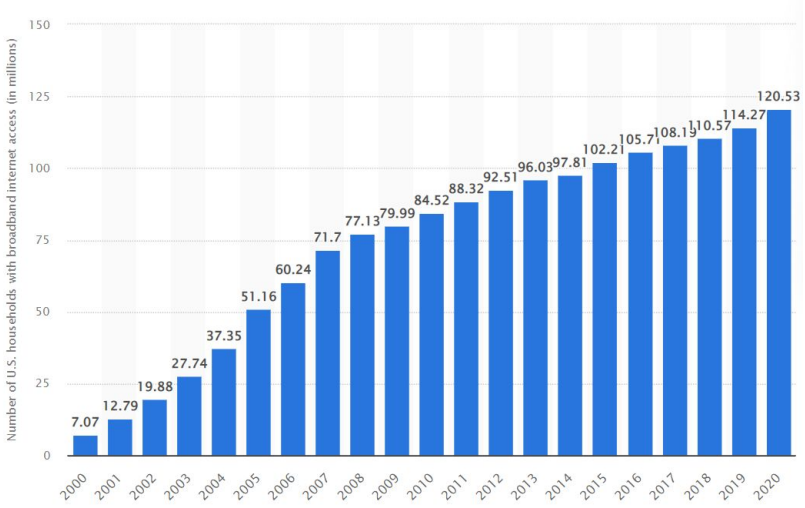


1.3-1.4 Key Features of the USA's Cyberspace

- Mostly Privately Owned.
- Competitive Market.
- Compuserve, Mindspring, HE.net, PSINET and UUNet.com were the top five providers in 1990
- AT&T, Comcast, Charter,Verizon and Centurylink are the top 5 providers in 2022

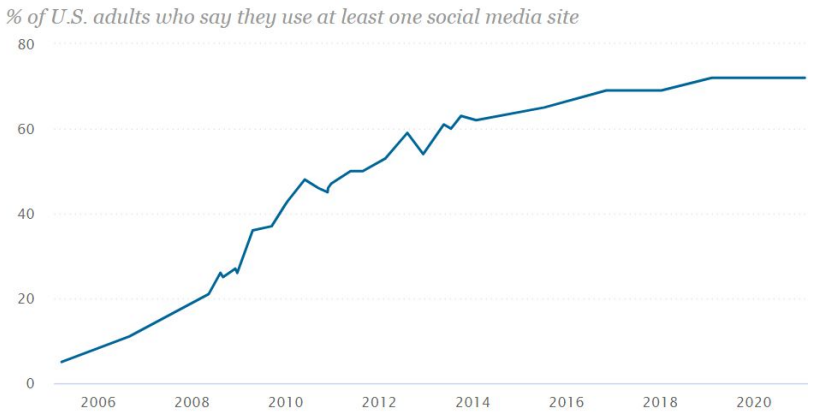


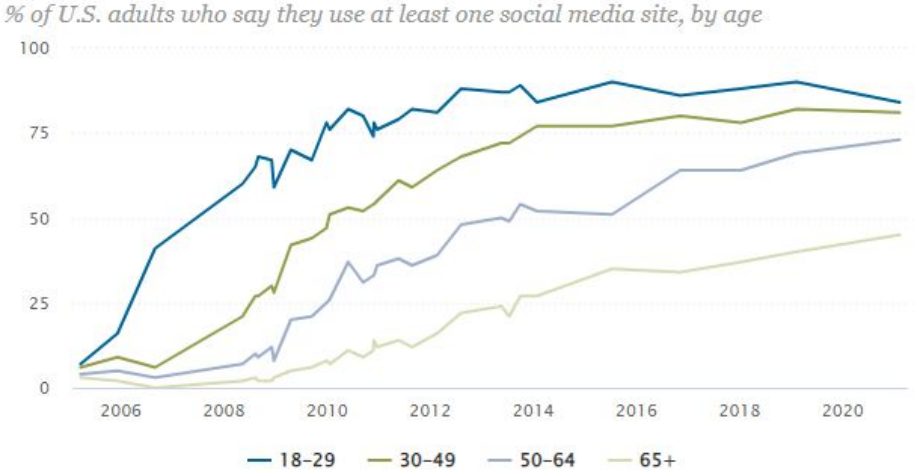
Growth of Internet usage in the last 20 years



- Data from Statista
- The growth of internet user has been constant during the years, it reaching a threshold now
- The number of people using the internet uses at least one social media

Social media usage in the last 15 years





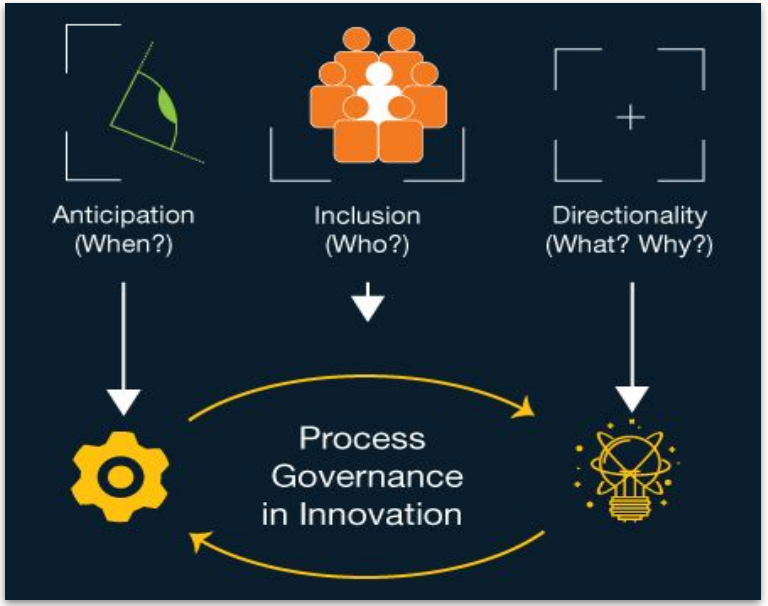
- Even older adults are using now social media
- The rate of growth is almost the same one for all ages with a spike in the younger generation

Why America invested in cyberspace

- To establish communications between leaders after nuclear armageddon
- Commercialized to help the private sector
- Surveillance was drastically increased after 9/11

2.1 Technical Governance

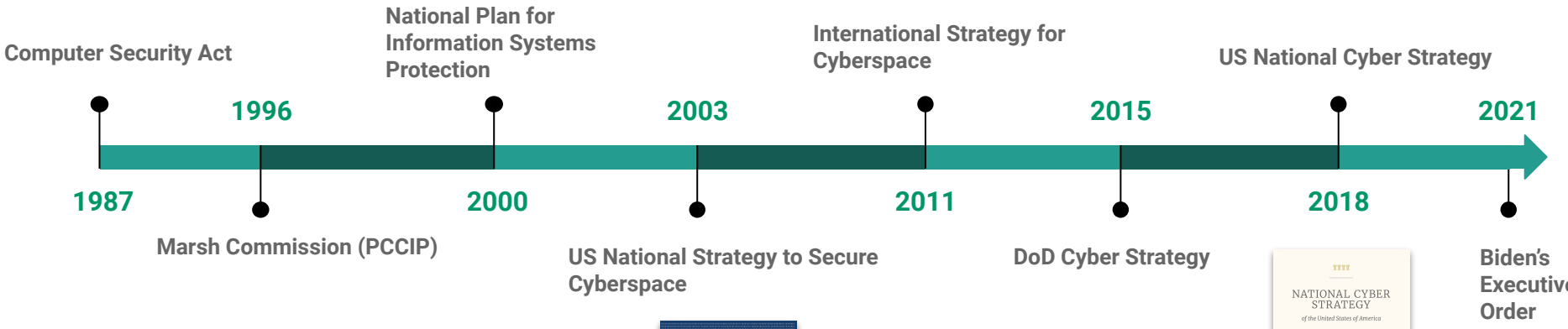
- ARPANET
- IANA
- US Cyber Command



2.2 Political Governance

- UNGGE
- NATO
- COE
- UNODC
- INTERPOL

3.1 The United States' National Cyber Strategy



3.1 Major Events the US faced that lead to Adoption

- The proliferation of the internet and IoT devices
- National Strategy of 2003: 9/11
- National Strategy of 2018: Major events during Obama Administration
  - “Digital Optimism”
  - Deterrence

- External Threats and Attacks (nuclear threats, terrorist attacks, global conflicts, espionage)

- President Obama to President Trump
- Desired state of cyberspace

3.2 US Cyber Strategy

- Government entities within US Cyber Strategy
  - DoD
  - DHS
  - FBI
  - CISA
  - Cyber Command
  - NIST

- Current Issues with this?

3.2 The Major Goals and Priorities of US Cyber Strategy

US National Cyber Strategy- **The 4 Pillars**

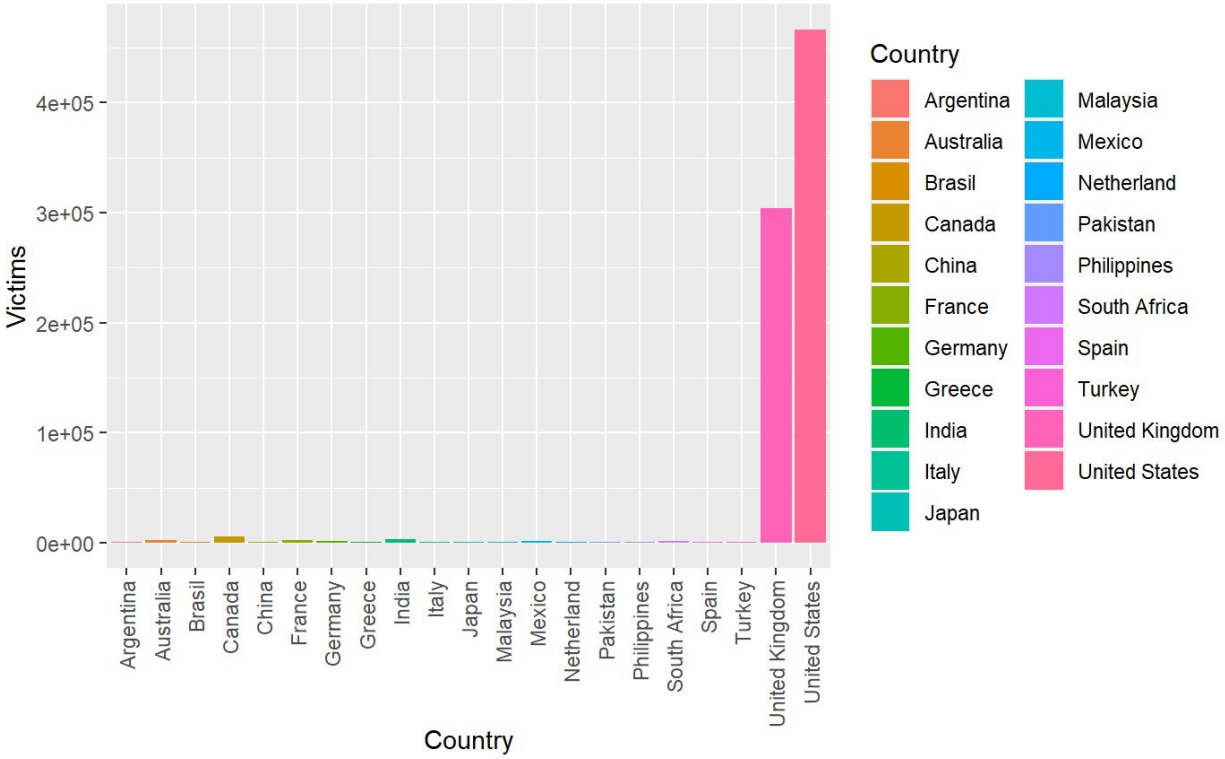
- Protecting the People, Homeland, Way of Life
- Promoting American Prosperity
- Preserving Peace Through Strength
- Advance American Influence

3.2 President Biden's Executive Order

- **Modernize federal government cybersecurity**
- Secure federal government networks
  - Stricter guidelines for companies selling to government
  - Cloud infrastructure implementation

- Requires service providers to disclose all cyber incidents that threaten government networks

3.2 International comparison of cyber victims in 2021



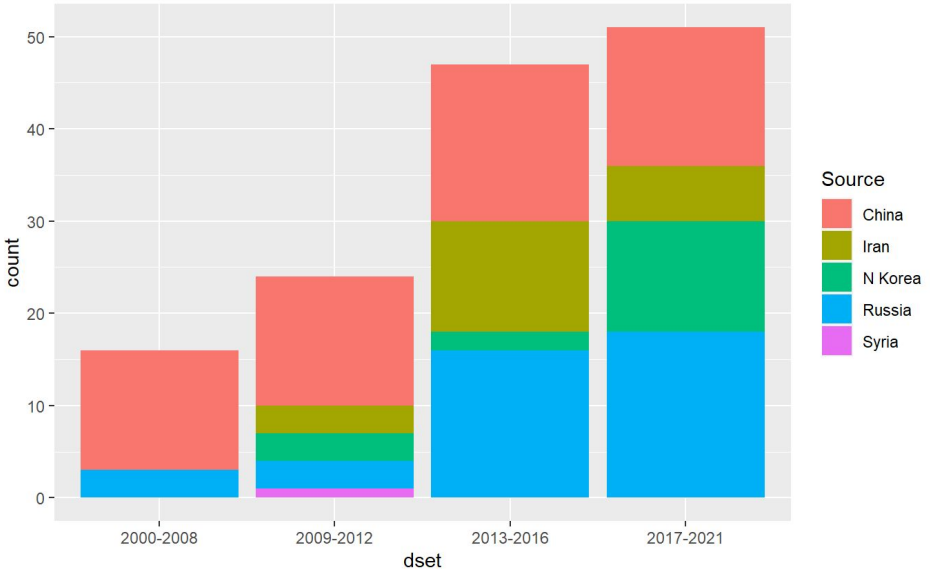
Why does US need a cyber strategy?

- country with the most victims of attacks
- minimize losses due to those attacks

3.3 The Major Threats Against The United States

- **Dataset:** Dyadic Cyber Incident Release 2.0 of June 2022

- The external major Threats that US has are China, Russia, Iran, and North Korea
- The increase number of attacks in the last 2 administration facilitated the creation of a new cyber strategy

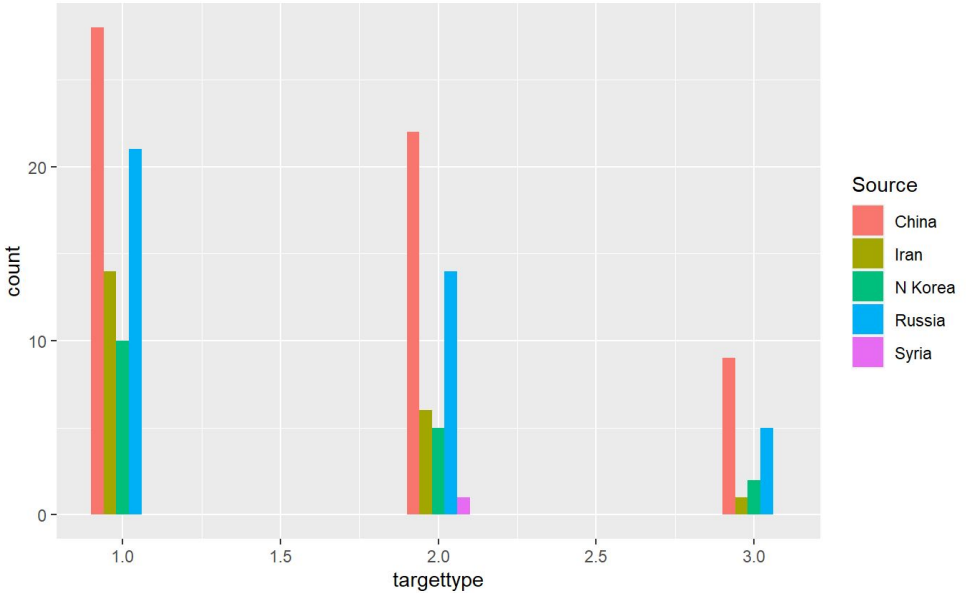


3.4 The Targets of External Attackers

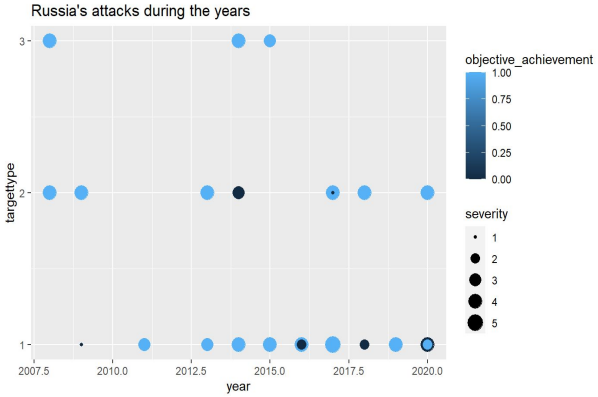
Target type:

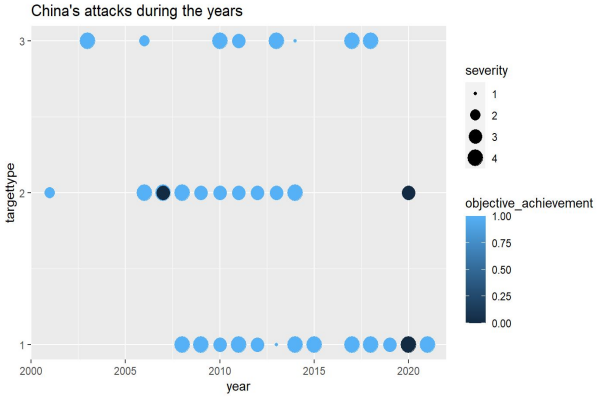
1. Private companies
2. Government non-military
3. Government military

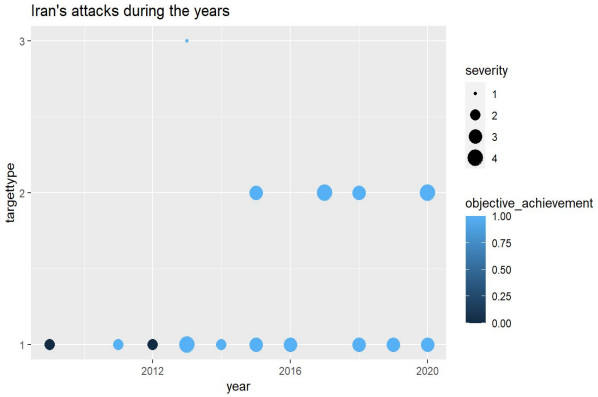
- Most of the attacks were done towards private companies. All the major countries attacking the US have the same trends
- Government military targets are the least attacks because they are usually believed to possess stronger security measures

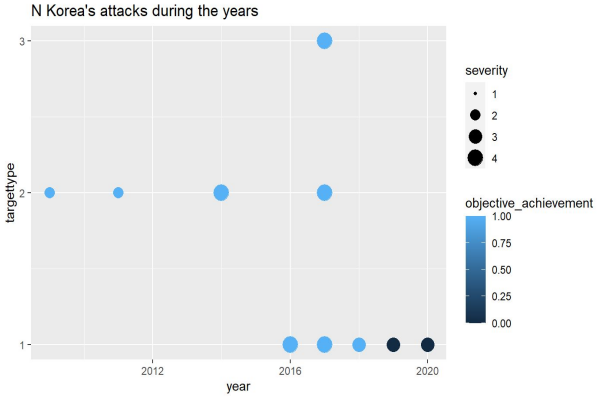


3.4 Attacks by target type and severity for each country









Target type:

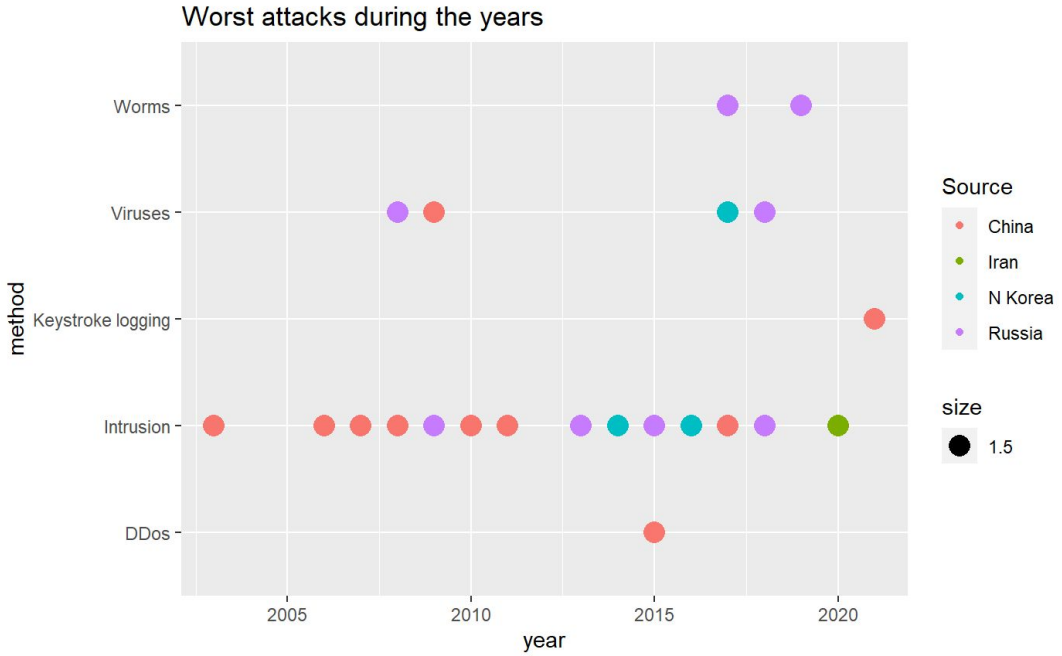
1- Private companies

2- Gov non-military

3- Gov military

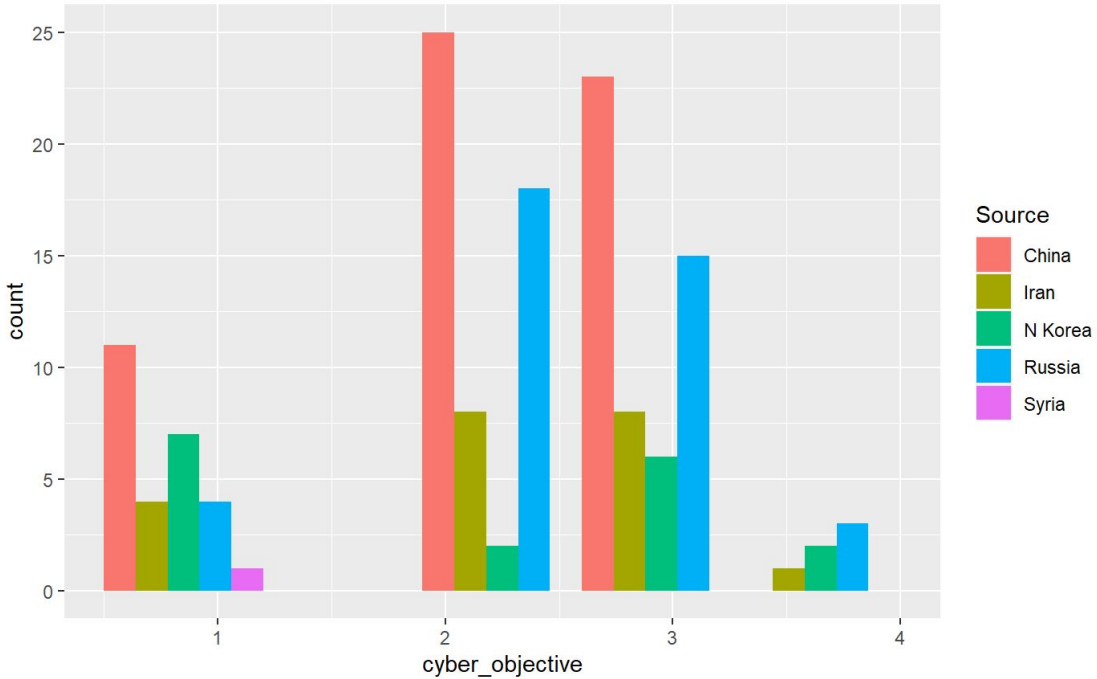
- The majority of attacks were successful
- Most attacks have a severity of 3 and 4

3.4 The worst attacks during the years



- Intrusion is the main attack method throughout the last 20 year
- Russia uses a variety of methods
- China’s main method is intrusion

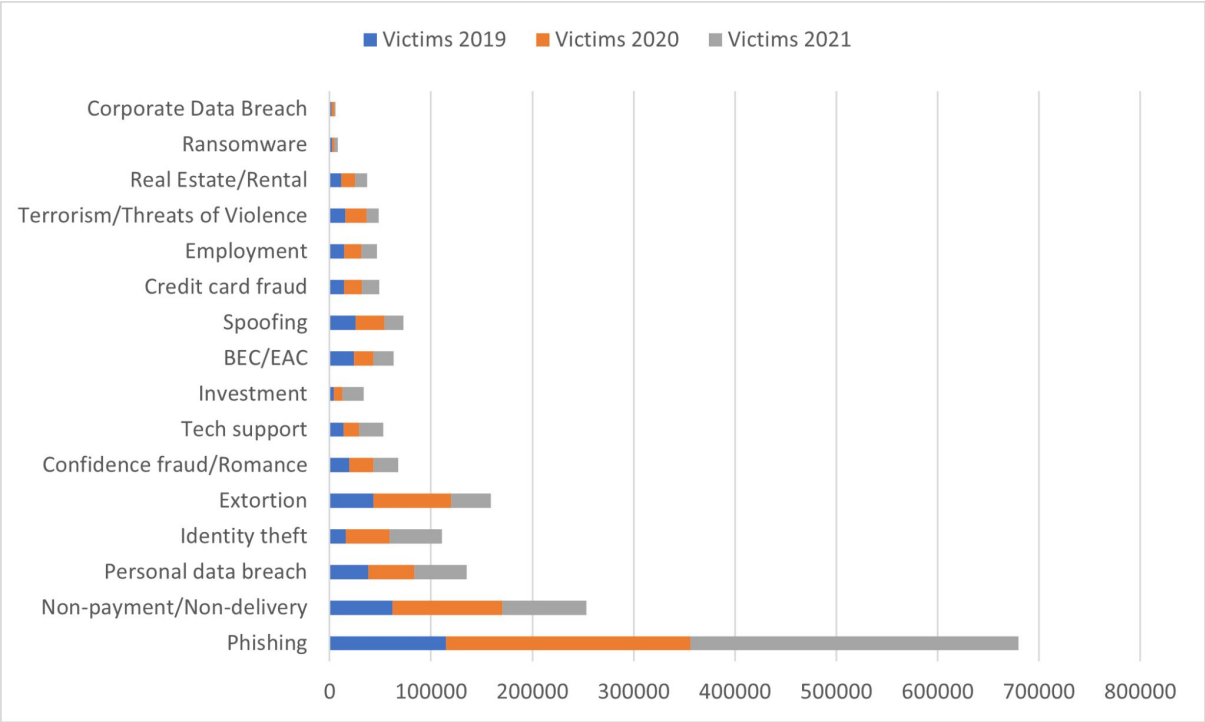
3.4 What are the objectives of attacking countries?



1. Disruption
2. Short-term Espionage
3. Long-term Espionage
4. Degradation

- Espionage is the first objective of every attacker

3.4 Victims per type of attack during the years

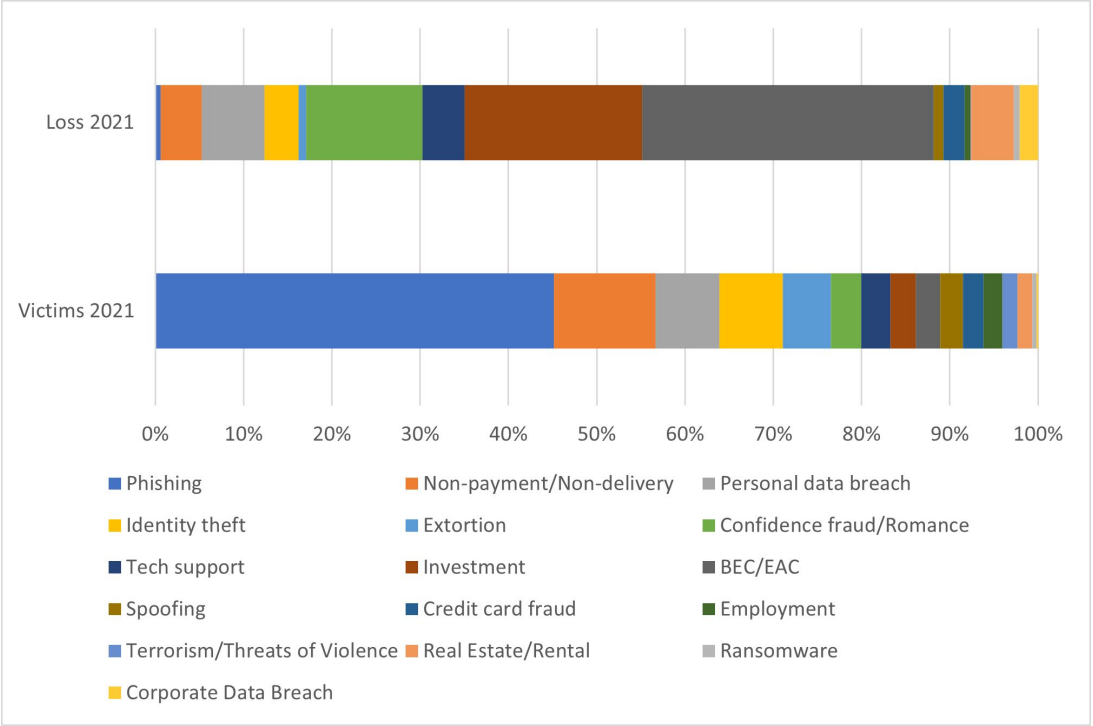


- **Dataset:** FBI incident crime report 2021

- Trend of growth in the number of victims in the last three years
- Phishing is the number one attack performed

3.4 Comparison between victims and losses

- Number of victims doesn't equal huge losses
- Phishing has a lot of victims, but very little losses
- BEC and investments attack have few victims, but great losses



3.4 Existing and Alternative Evidence

- Data from FBI Incident Crime Report

- Alternative data: analysis of darknet market (the foundation)
  - Prices
  - Trends
  - Sales in markets vs. actual number of attacks

- Ideal Data: Companies must disclose cyber incidents when they are attacked.
  - Why is this difficult?

- Policies on obtaining data
  - President Biden’s Executive Order
  - CISA Cyber Incident Reporting for Critical Infrastructure Act

3.4 Elephant In the Room: What is not addressed

Threats not addressed by US Cyber Strategy

- Future issues such as IoT security, network congestion
- Attacks in FBI report that are not emphasized
    - Attacks that have too much attention
    - Attacks that don’t get attention: Real-estate scams, Investment scams

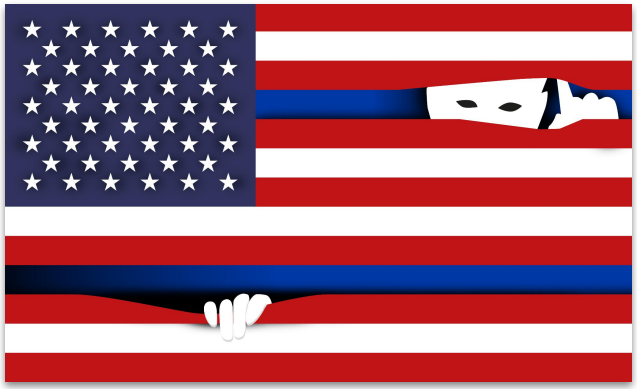
3.5 Official Goals and Actual Policies

Does the official goal match with the actual policies?

- External threats
- Critical infrastructure
- Future proofing the development of America’s cyber security?
- US cyber strategy is broad

3.5 Conclusion

- The US cyber strategy continues to evolve
- The US is attacked frequently as seen in FBI report
- Private-Public cooperation within US
- Some major attacks are neglected
- US cyber strategy is based on broad principles



Team Member Responsibilities

- **Justin:** Project lead, Part 3 literature reviewer and data hunter, presenter
- **Marzia**: Part 1 and 3 data hunter, data manager, data analyst, presenter
- **Akshitha**: Part 1 and 2 Literature reviewer, narrator, presenter
- **Affan**: Part 1 Literature reviewer, data hunter
- **Tejodeep**: Part 2 Literature reviewer, data hunter

THANK YOU FOR THE ATTENTION!

We are open to any questions

Unsuccessful Attempts