The Undeclared Cyber World War:

Analyzing the growing risk from Cyber Attacks

Capstone Project
James Tramel & Jason Rincon

Agenda

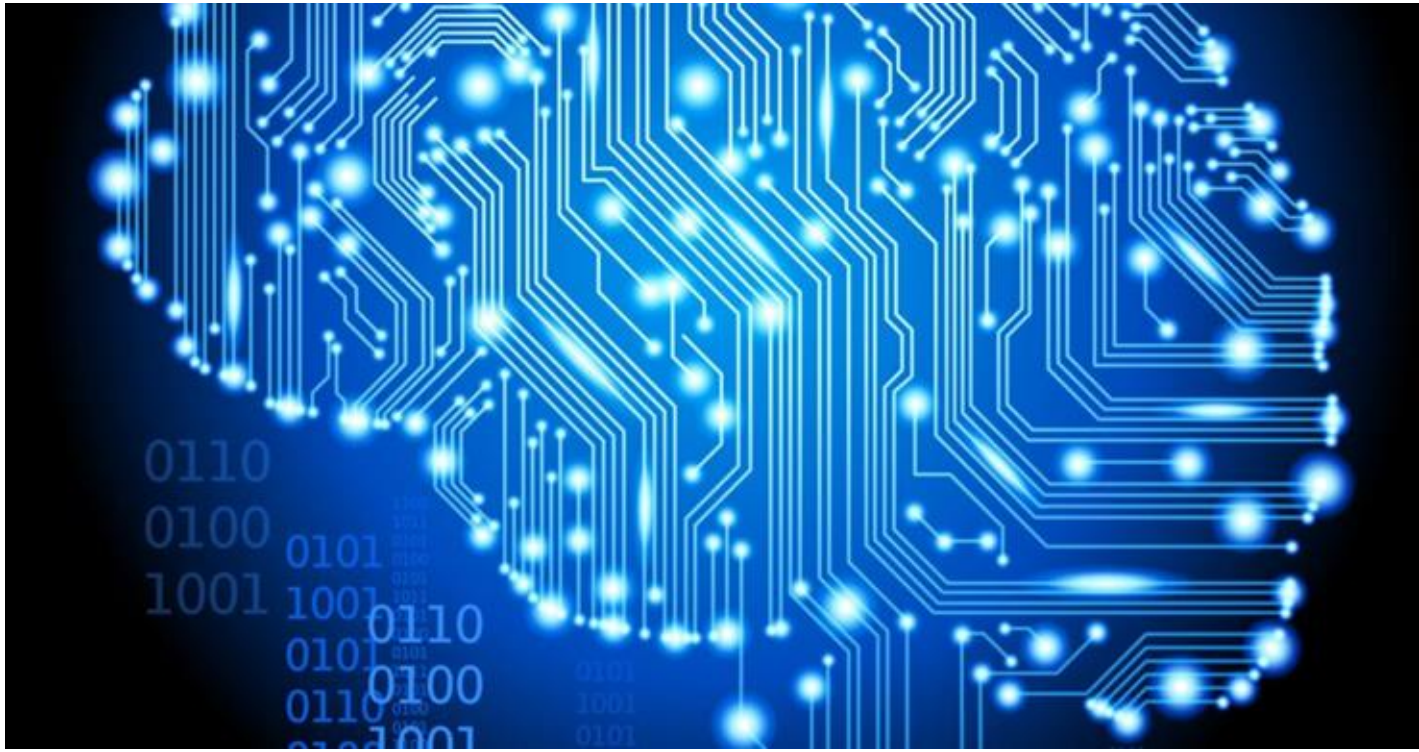
- ❑ Introduction
- ❑ Timeline
- ❑ Methodology
- ❑ Results
- ❑ Conclusions
- ❑ Additional considerations

NYU | STERN

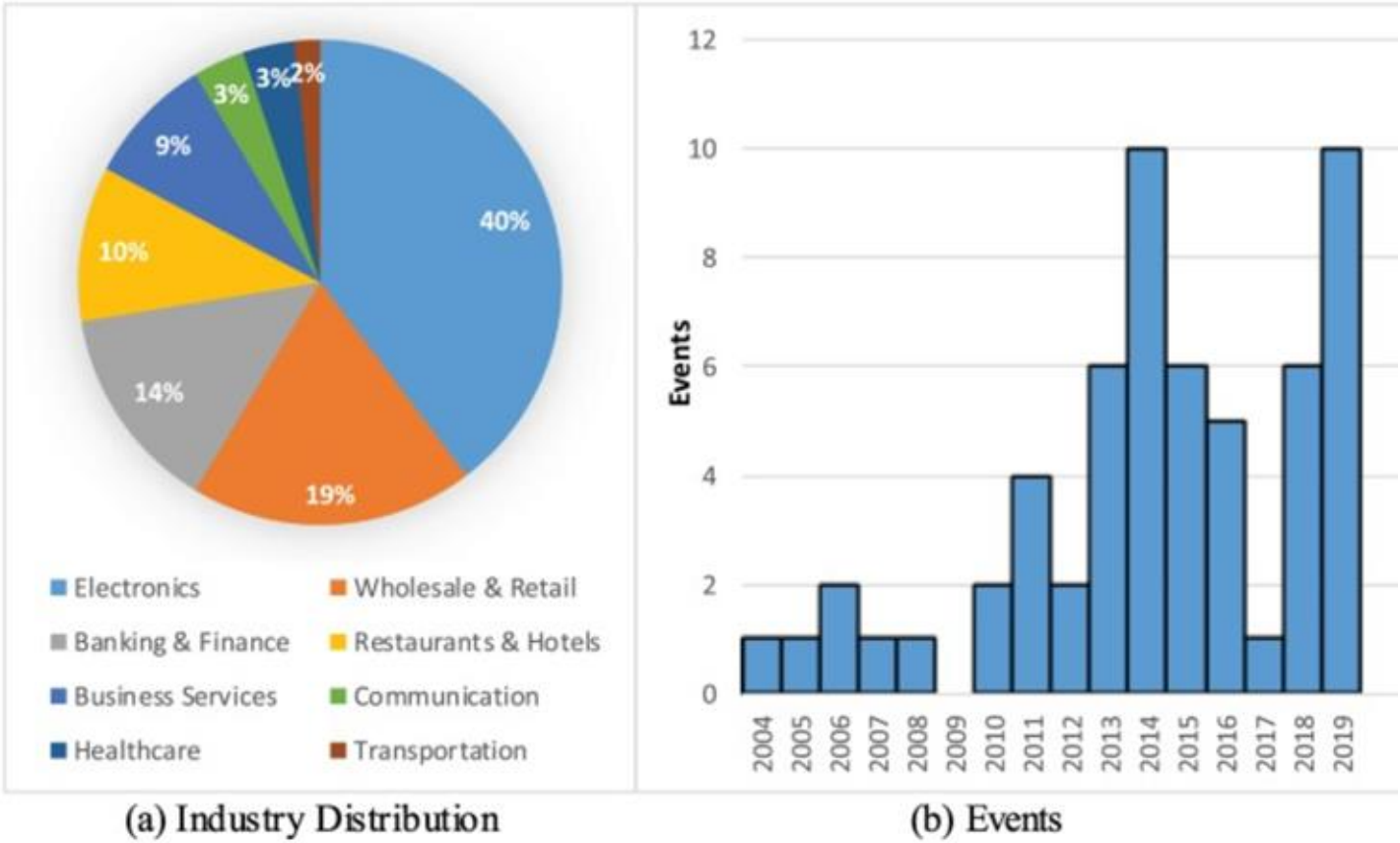
NYU STERN

I - Introduction

Software and computing technologies **have changed and will continue** to change the world - but not without new risks



- Highest average cost in 17 years, rising YOY
- United States of over $8.63 million on average
- An attack on one company affect firms in that vertical
  - Returns drop, premiums up
  - Affects reputation
  - Market reactions

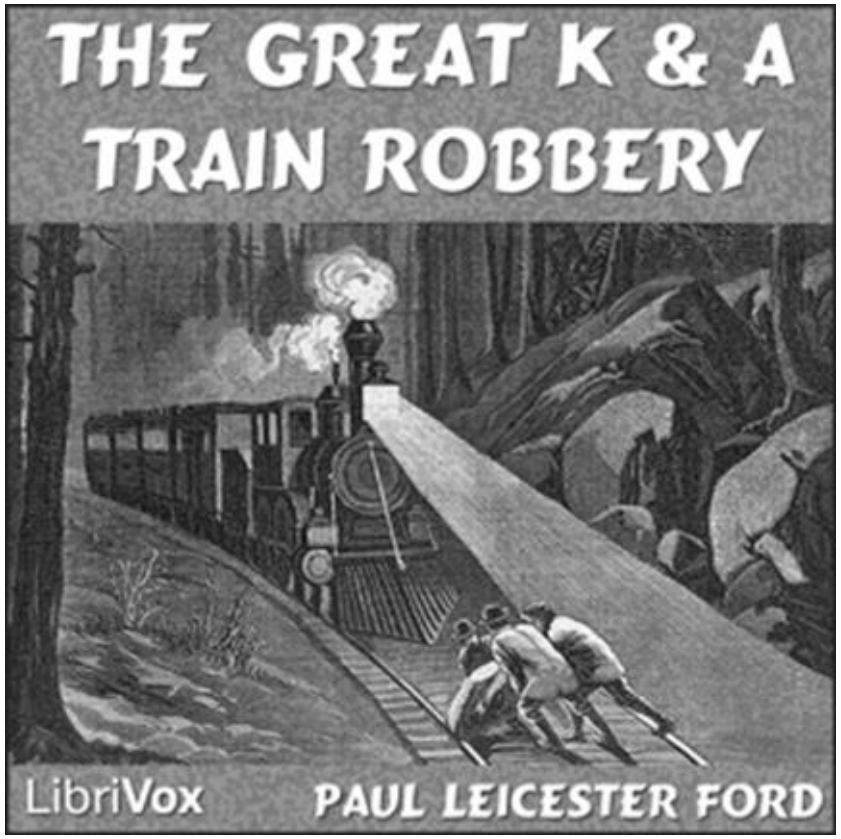


(a) Industry Distribution (b) Events

Data as a commodity

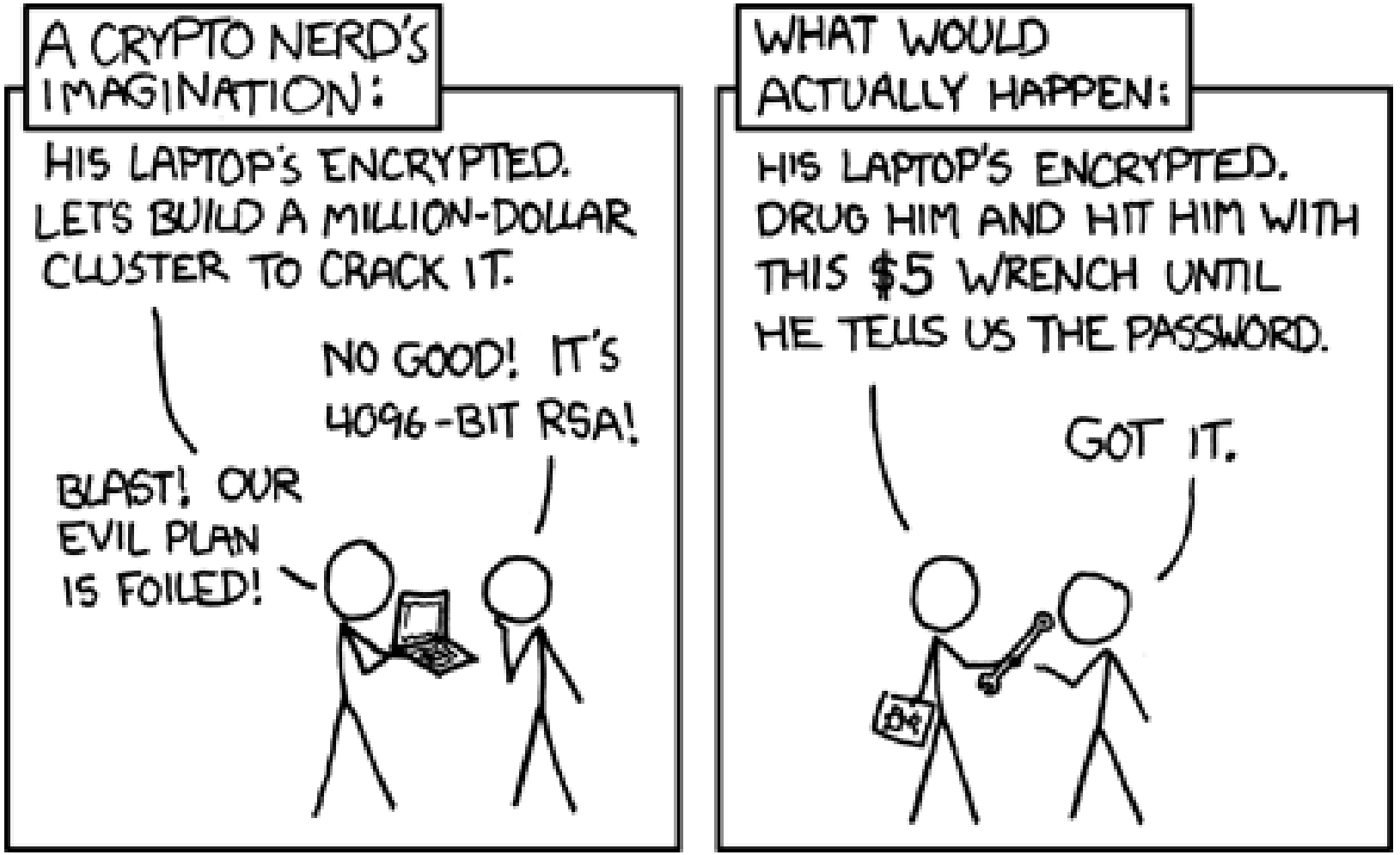
The only way to create an **impenetrable system** is to never let a person use it

Monetary theft



Data Black Market

Criminals



https://xkcd.com/538/

Ransomware

Non - Banks

HIGHER EDUCATION

Lincoln College to Close Permanently After Ransomware Attack

The Illinois college, which opened in 1865, said recent financial troubles and projected enrollment shortfalls were exacerbated by a ransomware attack last semester that rendered systems inoperable.

May 10, 2022 • News Staff

First Death from a Cyber attack

Game is changing

Cyber attacks are showing up in larger and more critical areas, by larger and more persistent actors

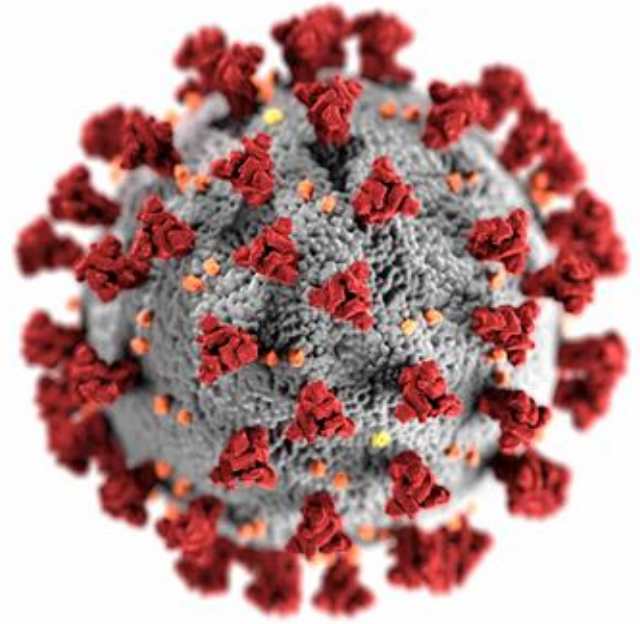
- Israel/Saudi and/or Russia/Ukraine
- North Korea / Sony
- Colonial pipeline
- Log4J / Log4Net / Solarwinds

State based actors

Persistent actors with unlimited funds

RBV or TCE?
State Paid, State Sponsored, or blind eyes?
Are they any world wide regulations?

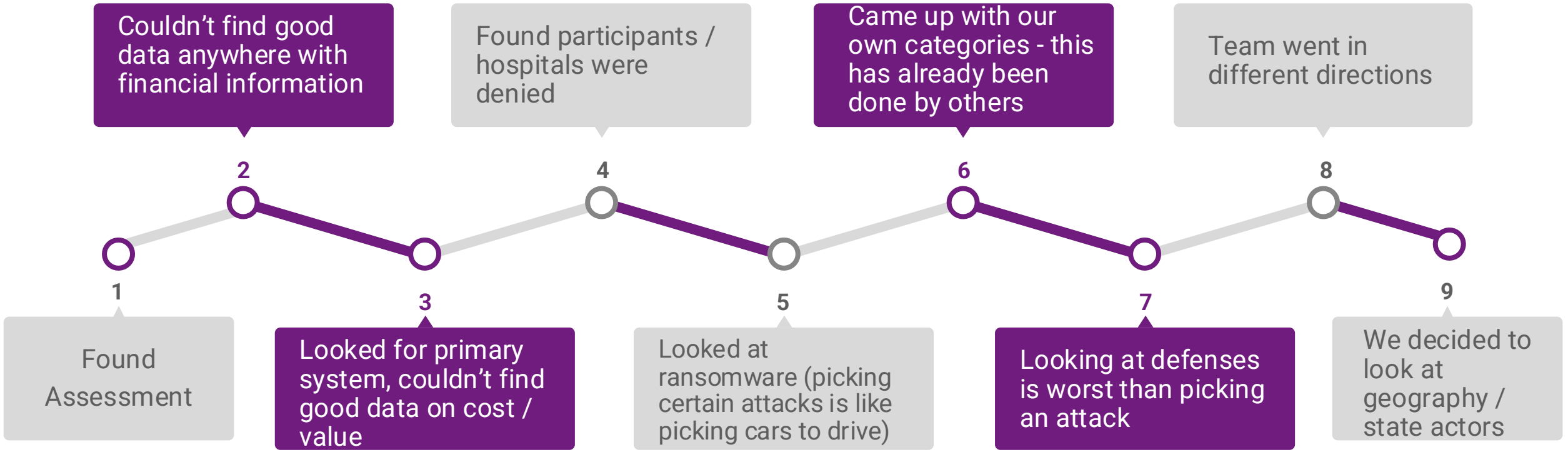
War in Ukraine, Covid, Cyber-Espionage



Cyber Cold War, Arms Race

II - Timeline

Timeline of the project



III - Methodology

1

Obtaining data

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

*US based **nonprofit** policy research organization, whose purpose is to define the future of national security.*

- **835** cyber-attacks
- Occurred during the last **19 years**
- **Focus**

  government agencies, defense, high-tech companies, or over $1M

Cleaning and searching

PROPOSED SEC CYBERSECURITY RULES

The proposed U.S. Securities and Exchange Commission cybersecurity rules would require companies to report material incidents on a Form 8-K and provide periodic disclosure on issues including:

- Policies and procedures to identify and manage cybersecurity risks.
- Management's role in implementing cybersecurity policies and procedures.
- The board of directors' cybersecurity expertise and oversight.
- Updates on previously reported material cybersecurity incidents.

- Data analysis
- Researching each case in public sources
- Identify
  - Data
  - Type of Attack
  - Motivation
  - Mechanism

3

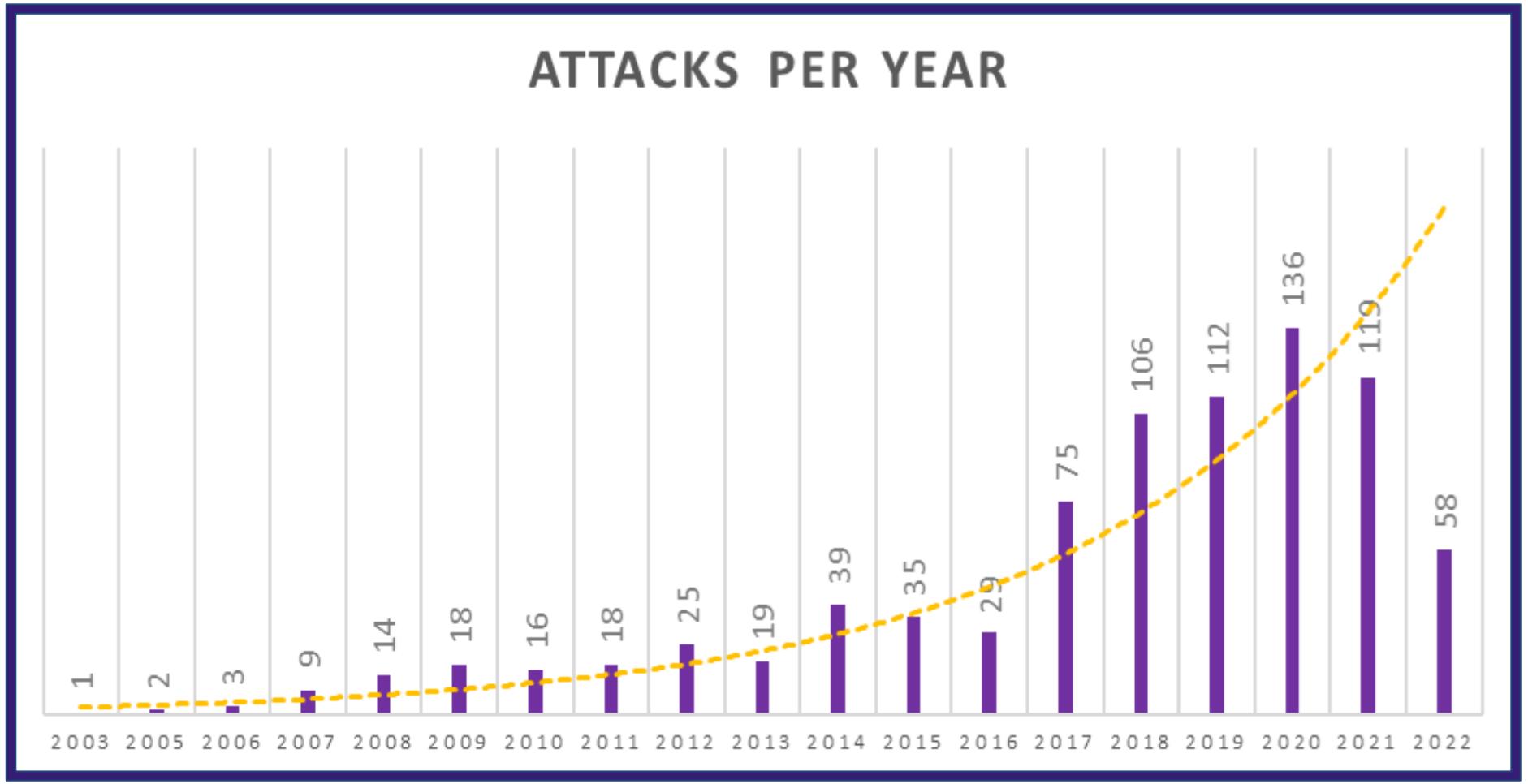
Categorizing

Demographics	Year, Perpetrator, Sector, Victim, Sponsored, Criminal
Type of Attack	Disruption, Leak, Unclear, Espionage, Sabotage, Theft
Motivation	Economic, Political, Information, Terrorism
Mechanism	Campaign, Malware, DDoS, Phishing, Ransomware, Remote Access

Analyzing

- Distribution
- Correlations
- Trends
- Forecasts

IV - Results



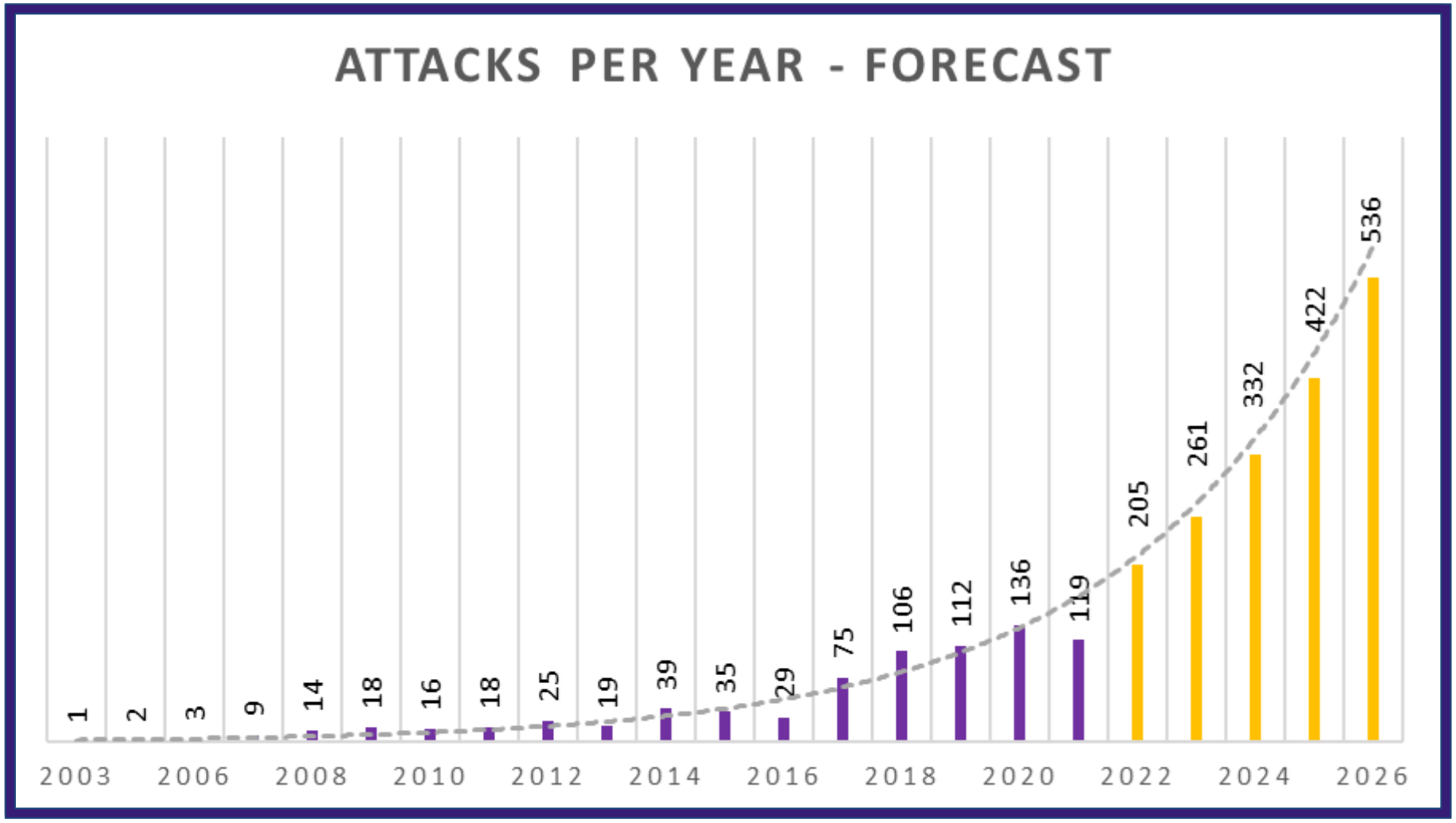
835
Events

32%
Ave. Growth

87
Victim Countries

36
Perpetrator Countries

* 2022 data of Q1 (First Quarter)

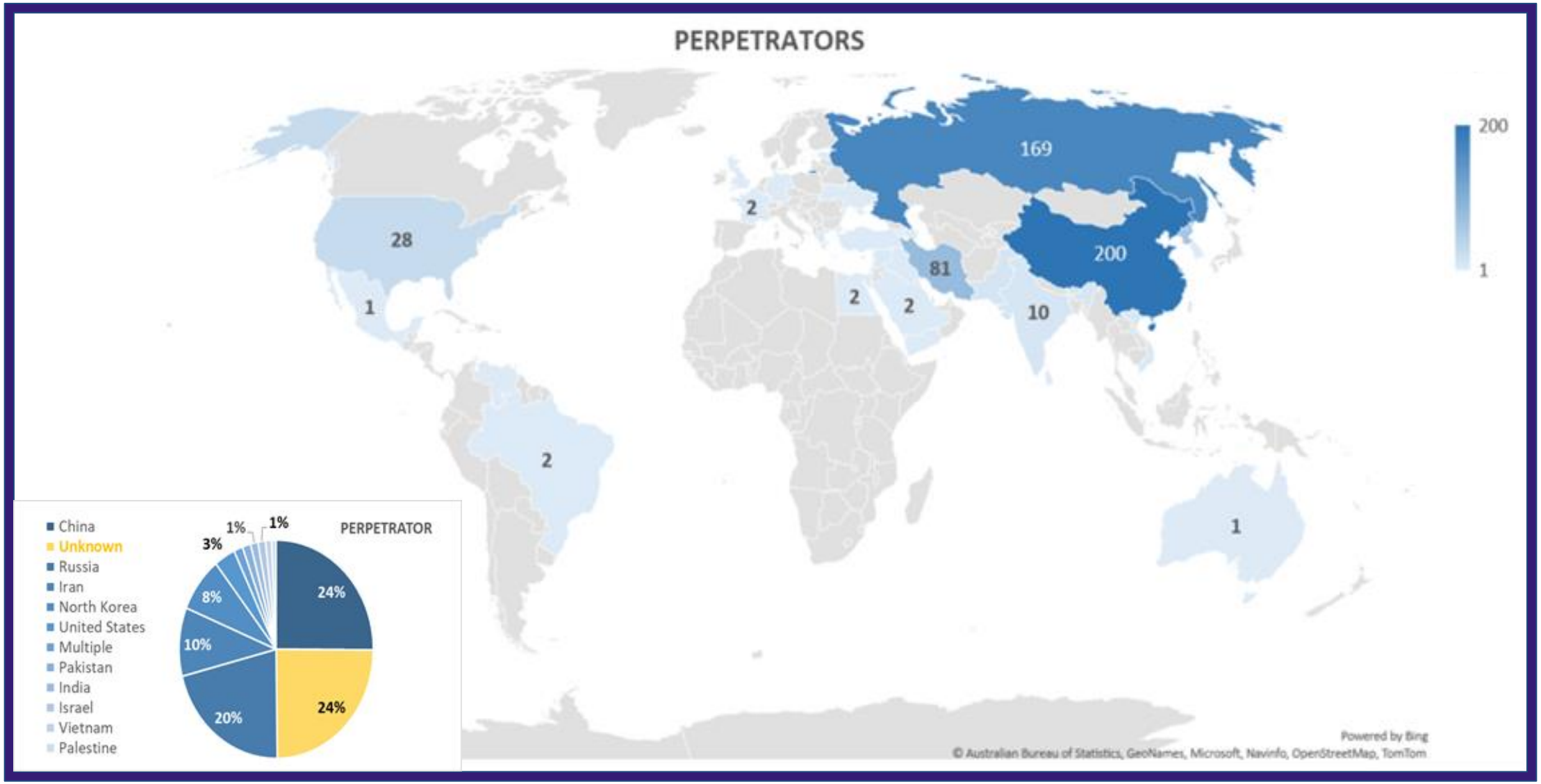


2,592

Events by 2026

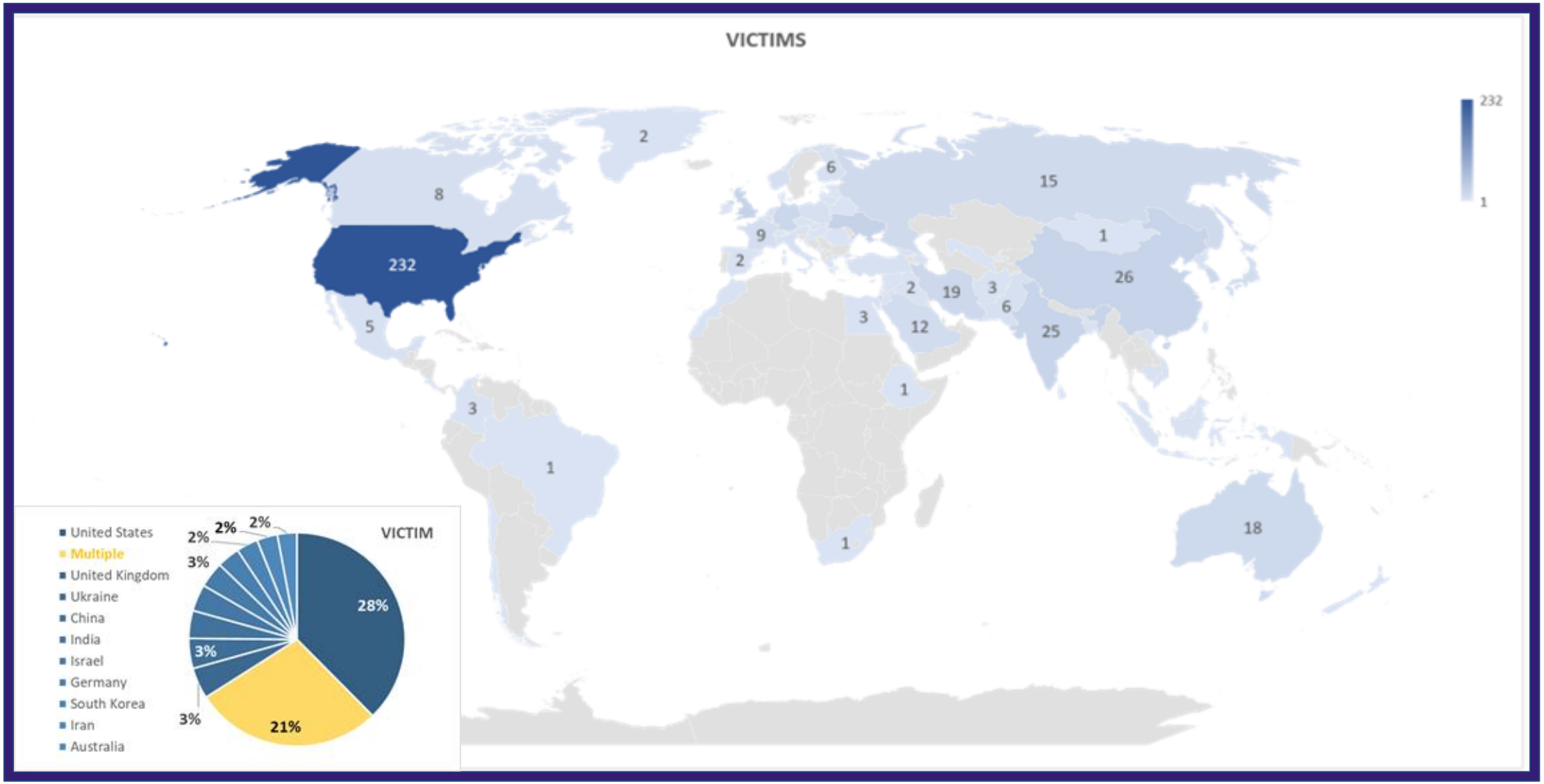
Double

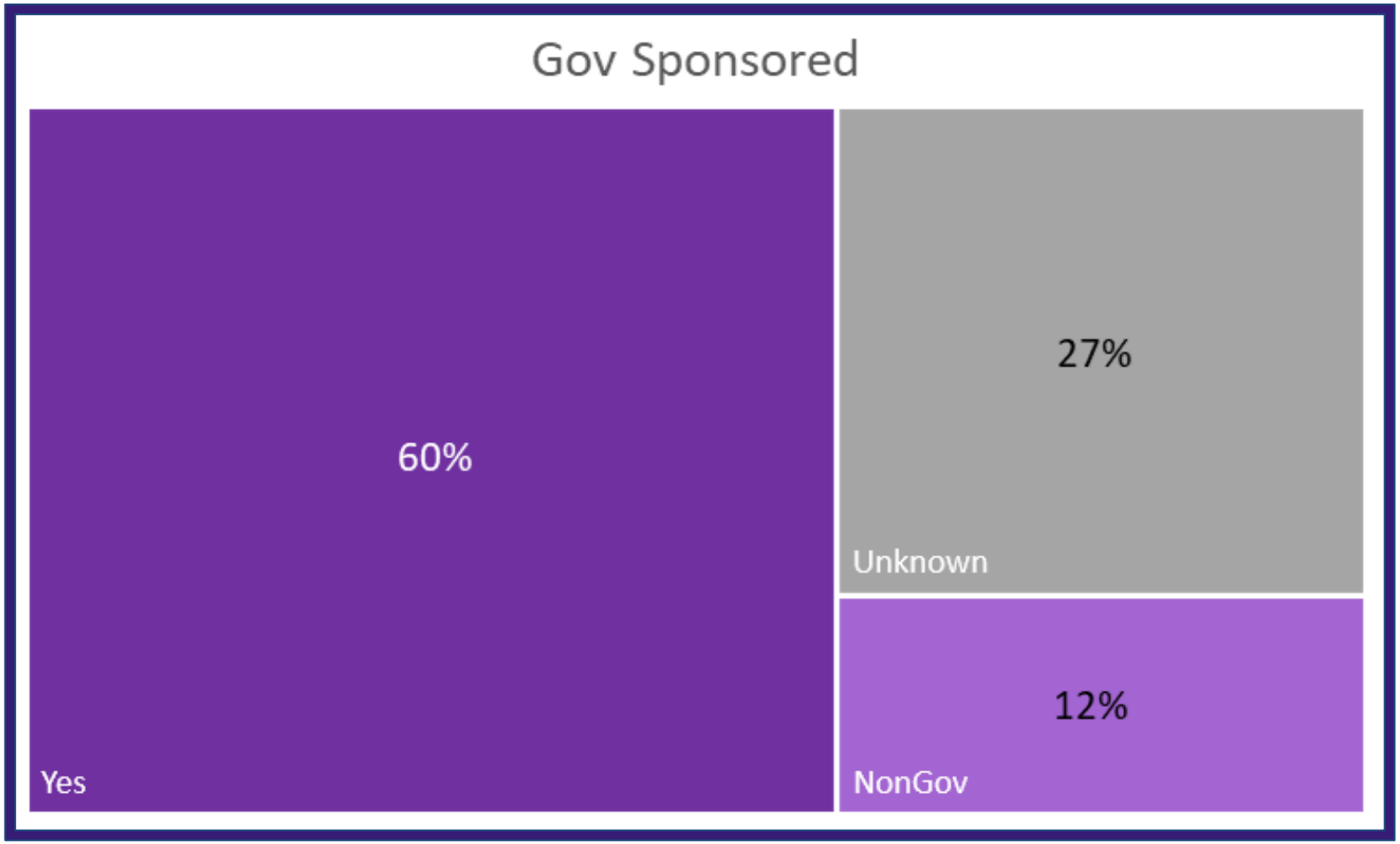
2022 events by 2026


PERPETRATORS
169
200
28
2
81
200
1
2
2
10
2
1
1
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom
China
Unknown
Russia
Iran
North Korea
United States
Multiple
Pakistan
India
Israel
Vietnam
Palestine
PERPETRATOR
24%
24%
20%
10%
8%
3%
1%
1%

NYU STERN

Results

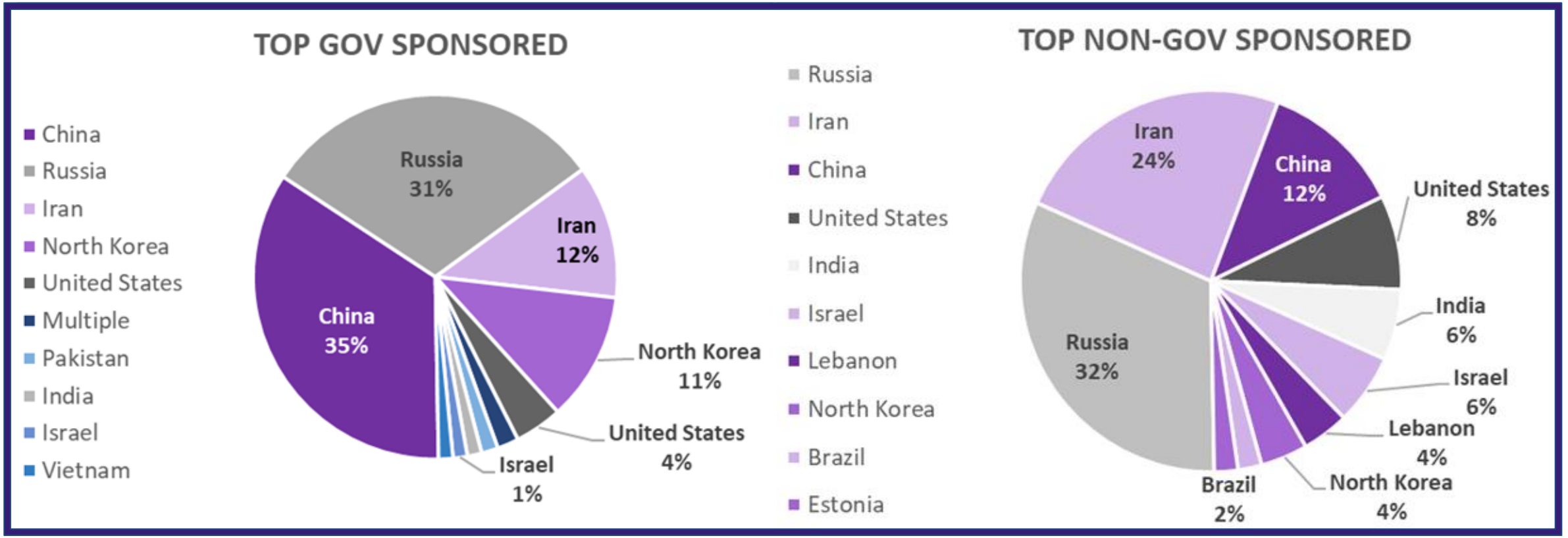


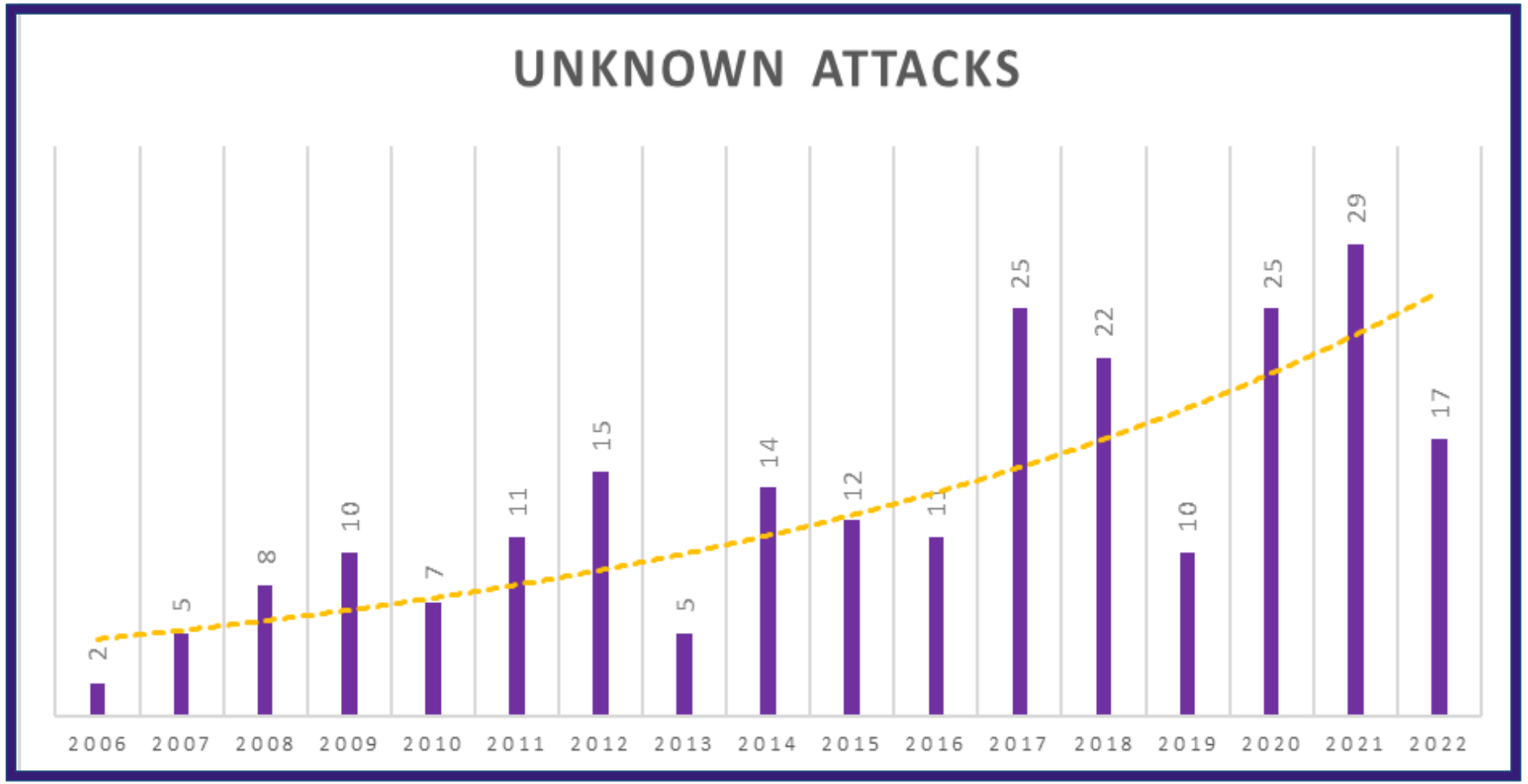


60%
Gov Sponsored

12%
Non-Gov

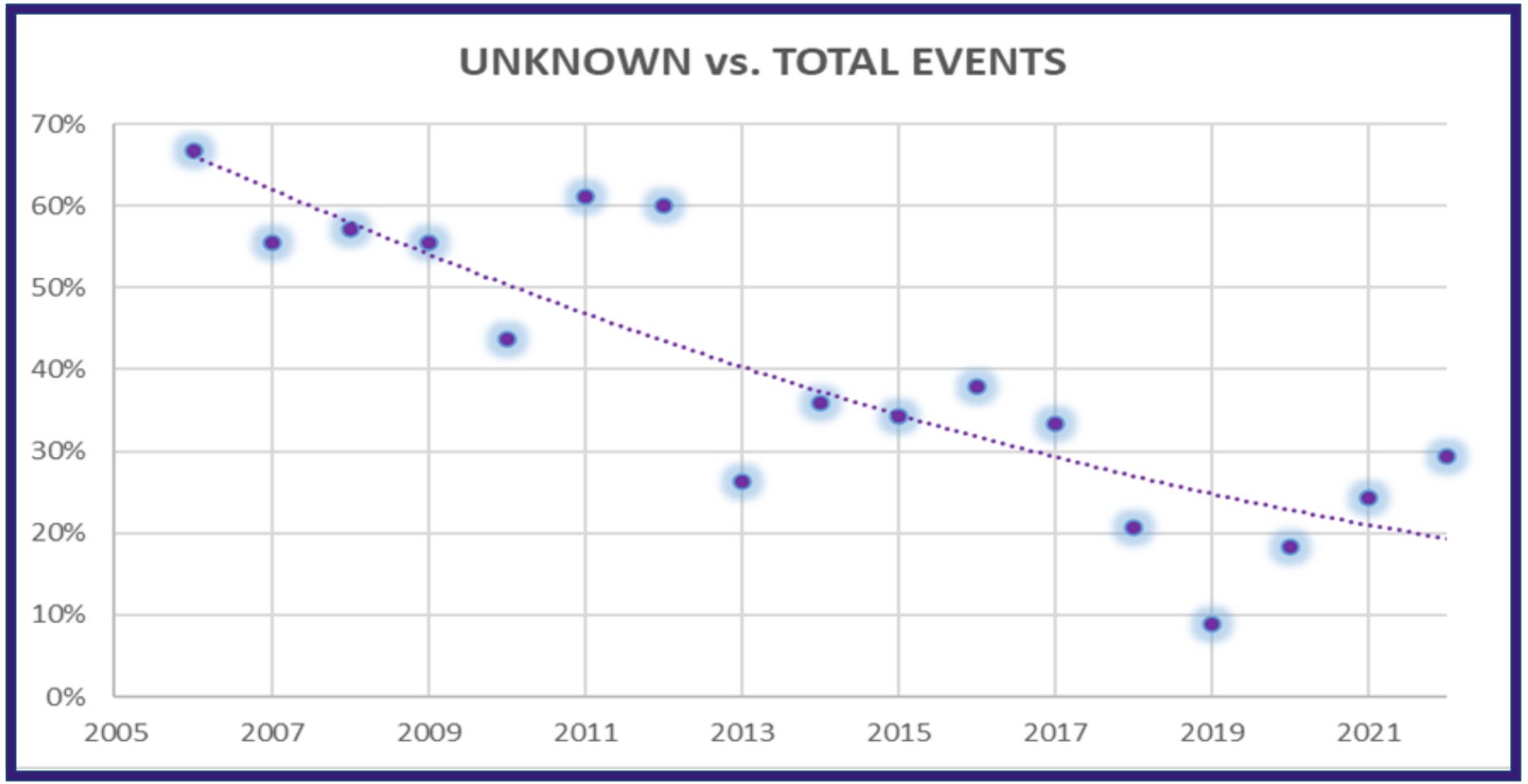
27%
Unknown


TOP GOV SPONSORED
China
Russia
Iran
North Korea
United States
Multiple
Pakistan
India
Israel
Vietnam
Russia 31%
Iran 12%
China 35%
North Korea 11%
United States 4%
Israel 1%
TOP NON-GOV SPONSORED
Russia
Iran
China
United States
India
Israel
Lebanon
North Korea
Brazil
Estonia
Iran 24%
China 12%
United States 8%
India 6%
Russia 32%
Israel 6%
Lebanon 4%
North Korea 4%
Brazil 2%



228
Events

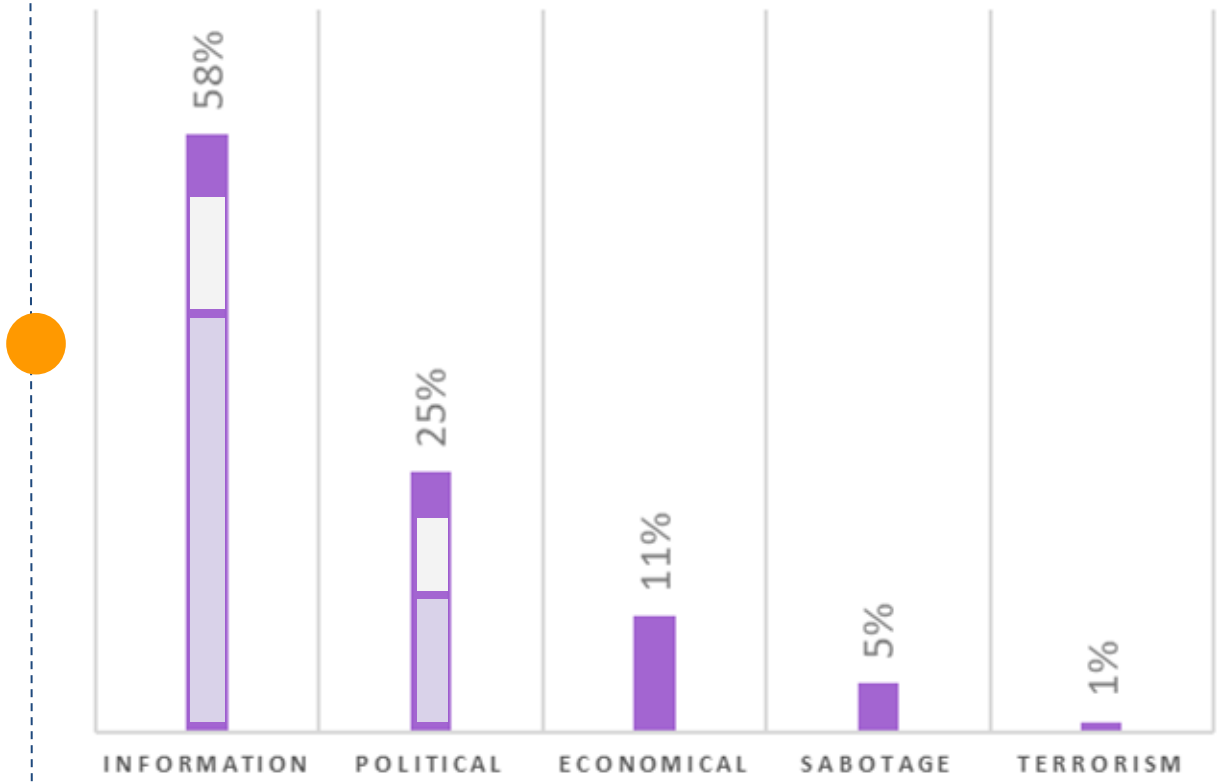
20%
Ave. Growth

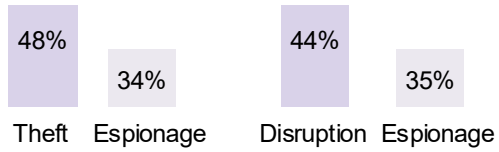


67%
2006

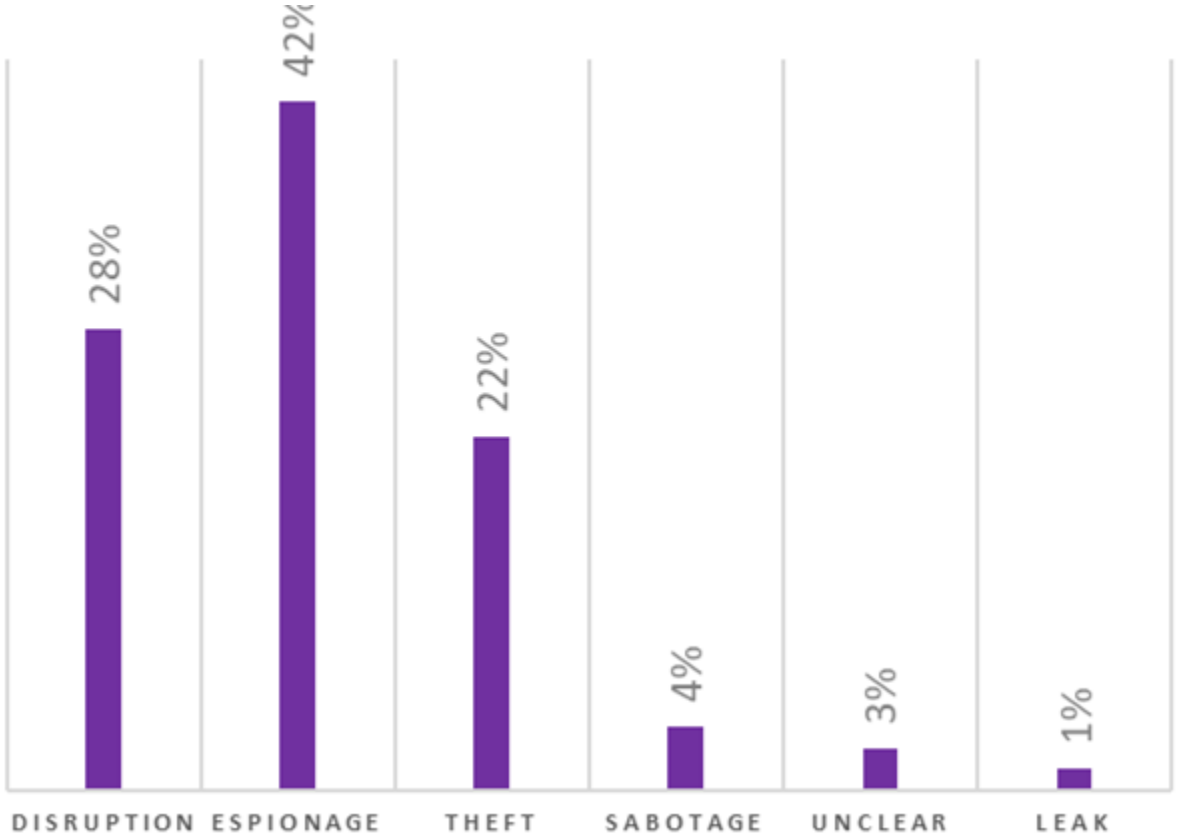
24%
2022

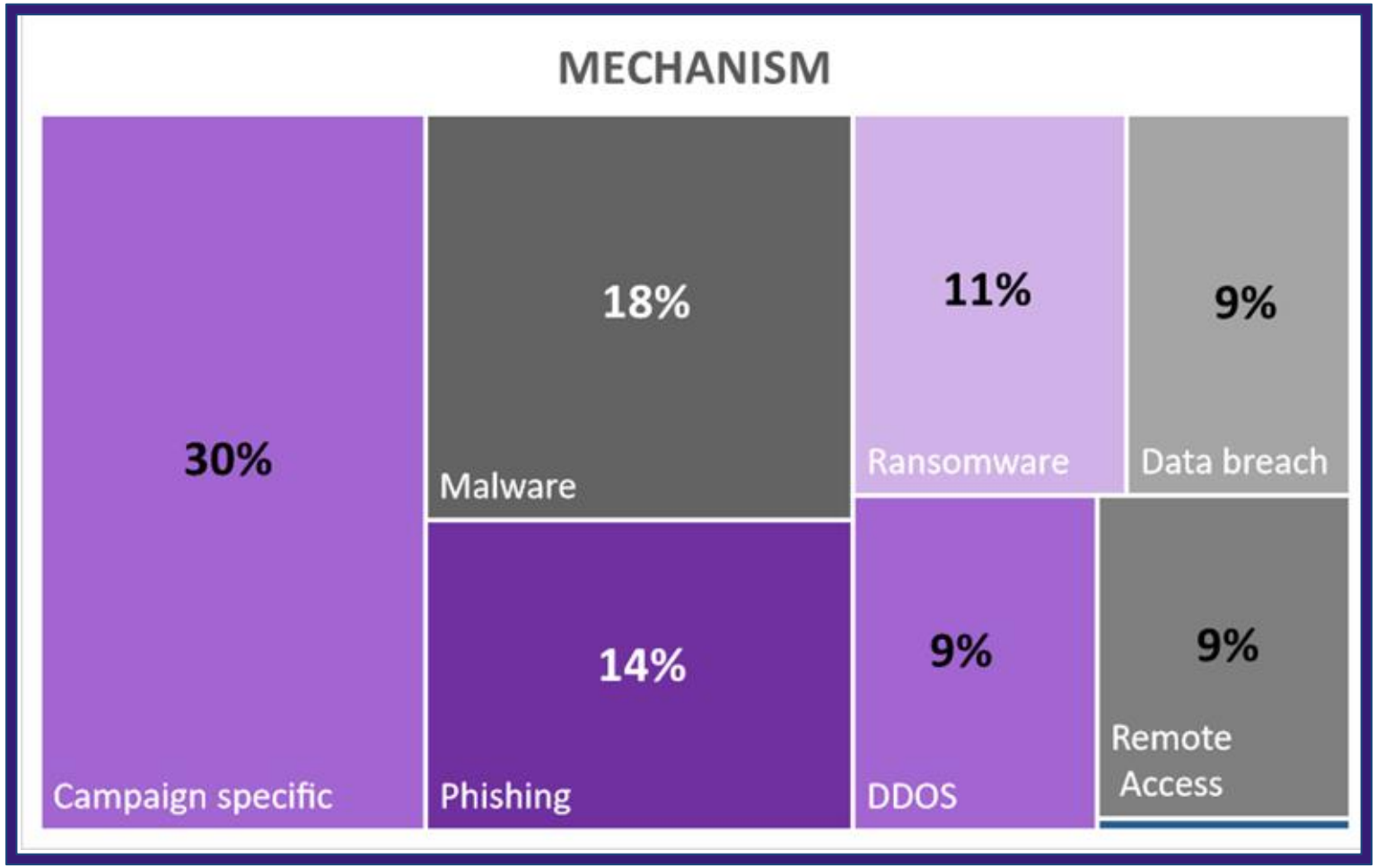
MOTIVATION





TYPE OF ATTACK





60%
Phishing Average Growth

58%
Malware Ave. growth

126%
Ransomware Ave. Growth

Summary of Results

- Cyber-attacks are increasing, with not signs of slowing down. CSIS is in line with other data sets.
- Attacks at least will be **double** by 2026
- **State sponsored** cyber attacks are increasing and represent more than **60% of total case**s
- **China** is the largest perpetrator, followed closely by **Russia**. **Iran** is slightly ahead of **North Korea** for a third position, and then other nations follow more distantly behind.
- Most of the attacks aim to get **Information** from governments and organizations by espionage and theft **(64%)**
- Attacks are now easily tracked and **just 24% are from unknown** perpetrators compared to 67% in 2006
- **Campaigns** are the common path that perpetrators are using to obtain large amount of data during prolonged periods of time
- **Ransomware** is the type of attack with higher growth rate in the last five years **(126%)**

V - Conclusions

More Research

- Cost / benefit to countries
  - Gain - information, monetary value, strategic?
  - Cheaper than other means?
- Will we see this trend continue? Will other countries commit more cyber attacks?
- Why aren't weaker cyber countries attacked?

Conclusions

- Digital transformation may put at risk many businesses who may not prioritize, lead, or better manage the risk of their digital assets and dependencies against things like persistent threats.
- The number of attack vectors available in the digital age has increased the number of opportunities for theft and exploitation
- The digital age presents new challenges at a faster pace, and businesses and states may not be adapting quickly enough in the face of a persistent and active threat.
- Risk management practices have been adopted to secure currency and commodities in the financial sector, but this is not in place in the same way for the technology sector. As data is a commodity, perhaps this type of security should be more closely addressed.
- In the face of advanced persistent threats from state actors, additional regulations and state-based support may be needed until a peaceful accord can be reached globally.

Suggestions for what to do now

- Add a Risk Management program to software and information technology departments
  - Software first, not hardware or networks
  - Systems engineering - DevSecOps
  - Audits and Standards
  - Operational principles like banks
  - Operational Risk management
  - Trade based risk management
  - Economic risk management
  - Regulatory risk management
  - Reputation risk management
- Global regulation - virtual borders

Thank you!