DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA

An Analysis of the DPRK's Cyber Resources and Their Threat to Global Security and Economic Stability

WHO WE ARE

Matt **Boutilier**

Lucas **Hoyles**

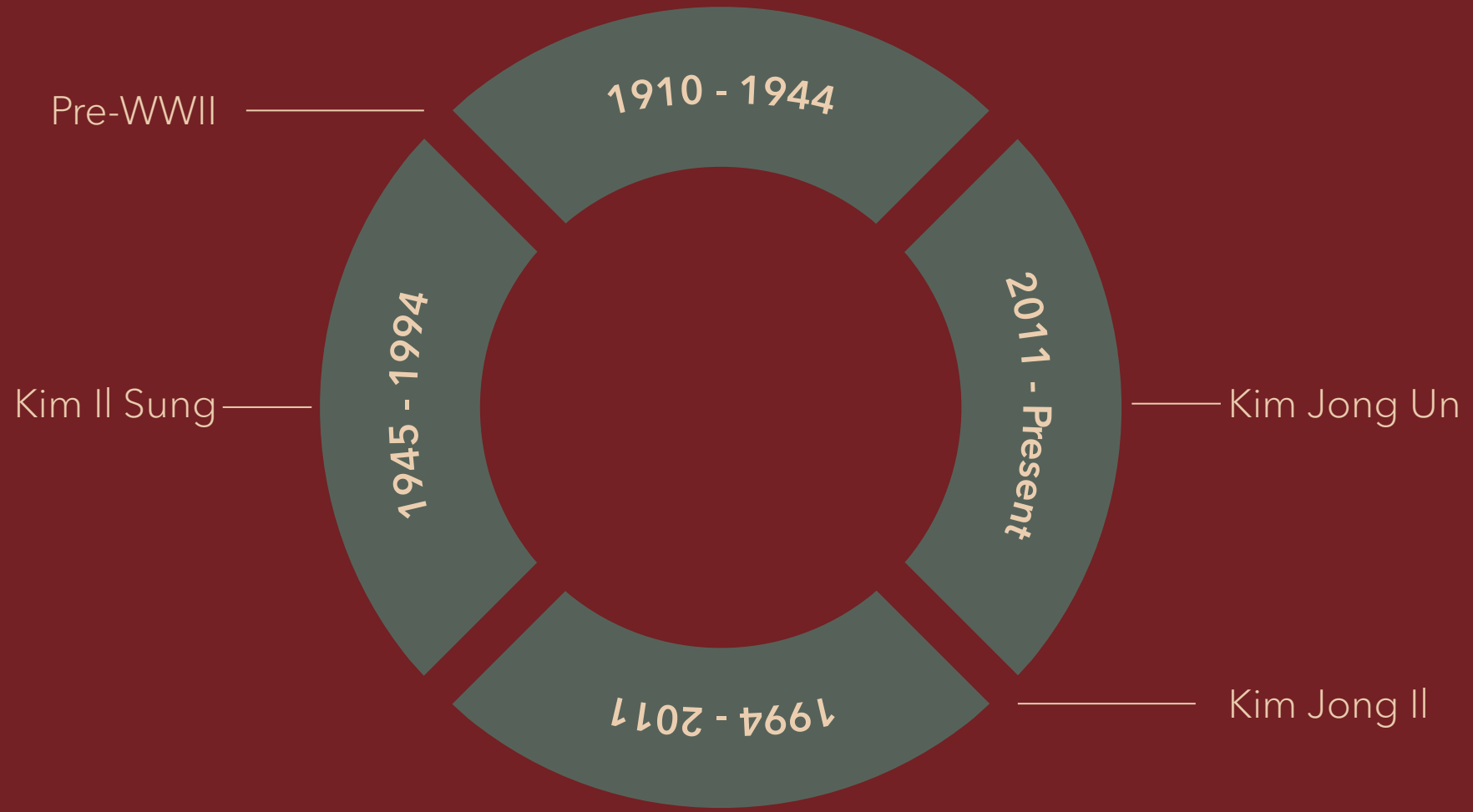
Liam **Nolter**


NORTH KOREA

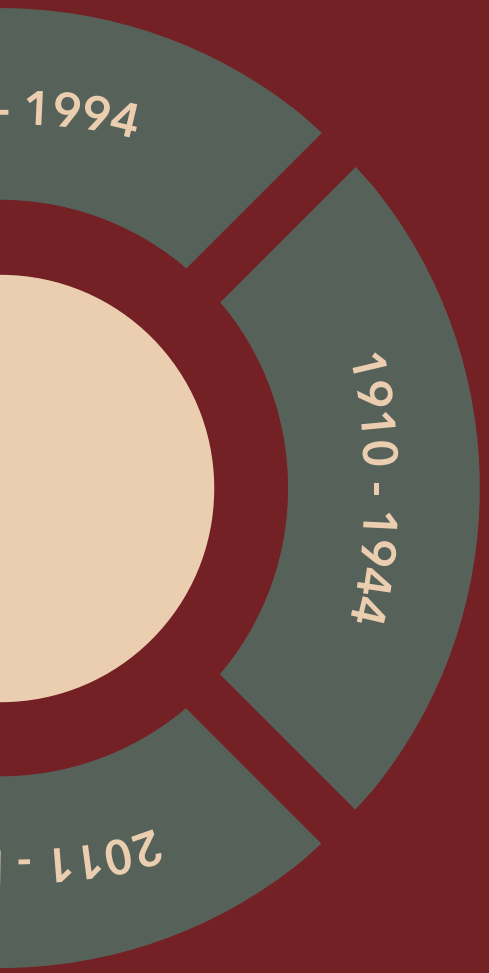
HISTORY & ORIGINS

- Former Japanese Colony
- Soviet-Influence
  Post-WWII
- Formation of the Democratic People's Republic of Korea
  1948
- Formation of Kim Dynasty
  1980

HISTORICAL TIMELINE

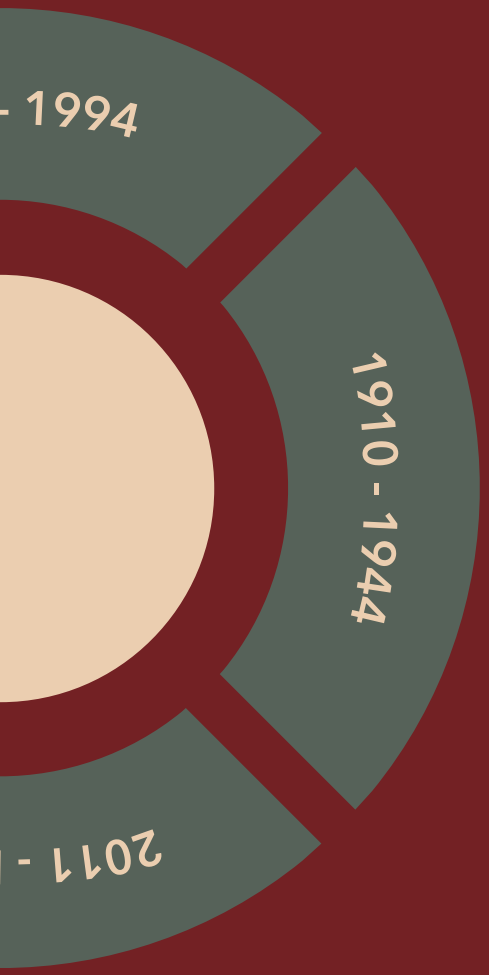


HISTORICAL TIMELINE



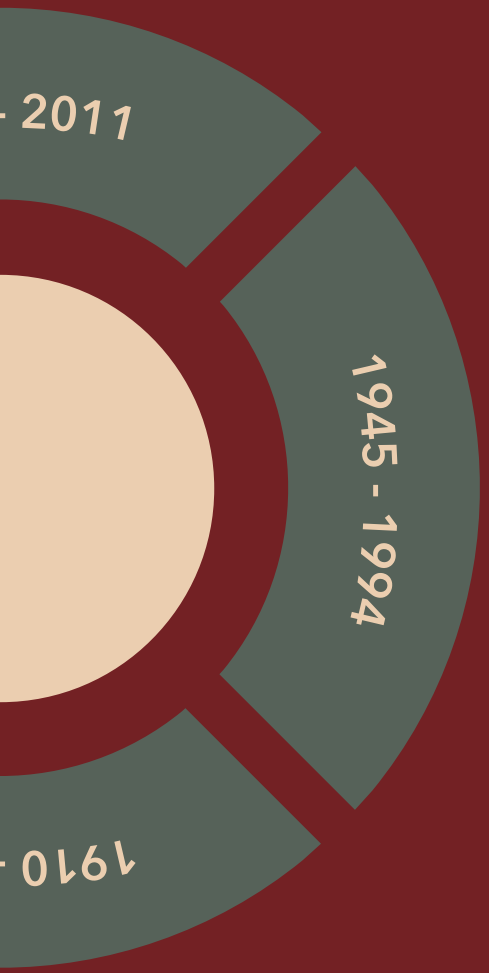
- 1910 – Japan colonized Korea due to its military strength and then it was renamed
- 1937 – Kim Il-Sung led guerrilla attacks against the Japanese, from which he gained fame with the Soviet Union
- 1942 – Korean resistance movements grew stronger, with communist groups in the north gaining momentum and support from the Soviet Union

HISTORICAL TIMELINE



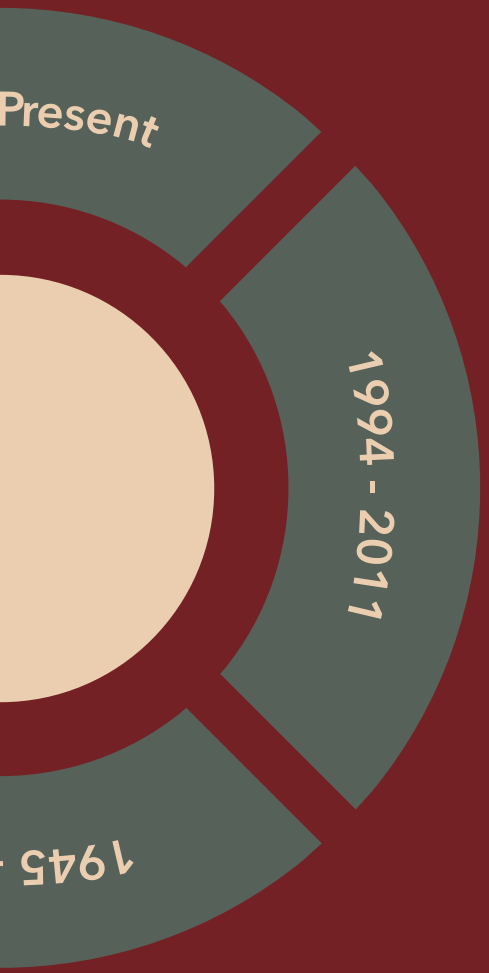
- 1945 – Kim Il-Sung emerges as the leading candidate for leadership through support of the Soviet Union
- 1949 – Worker's Party of Korea is formed, and Kim Il-Sung is elected as chairman
- 1972 – North and South Korea announce a joint statement for peaceful reunification

HISTORICAL TIMELINE



- 1994 – Kim Il-Sung dies from a heart attack, Kim Jong-Il takes over, but the presidential role was abolished
- 2001 – Kim Jong-Il appoints his son Kim Jong-Nam to a senior position in the Ministry of Public Security and promises him leadership
- 2009 – Speculations that Kim Jong-Un is being prepared to become the next leader and is named chairman of the National Defense Committee

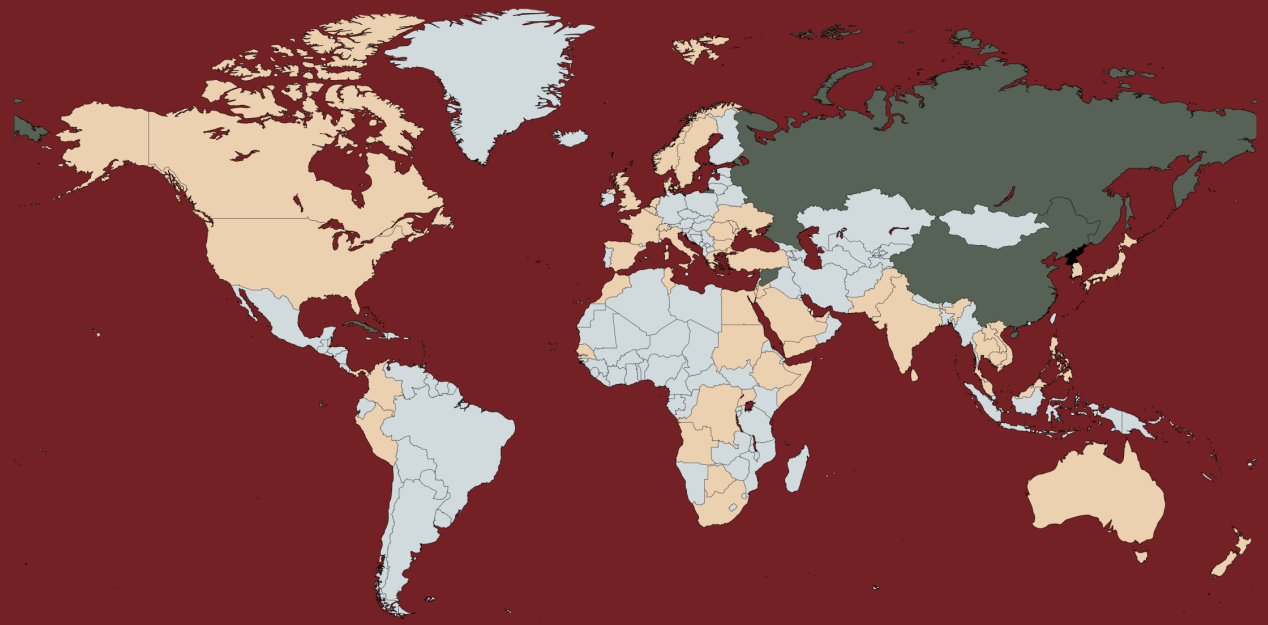
HISTORICAL TIMELINE

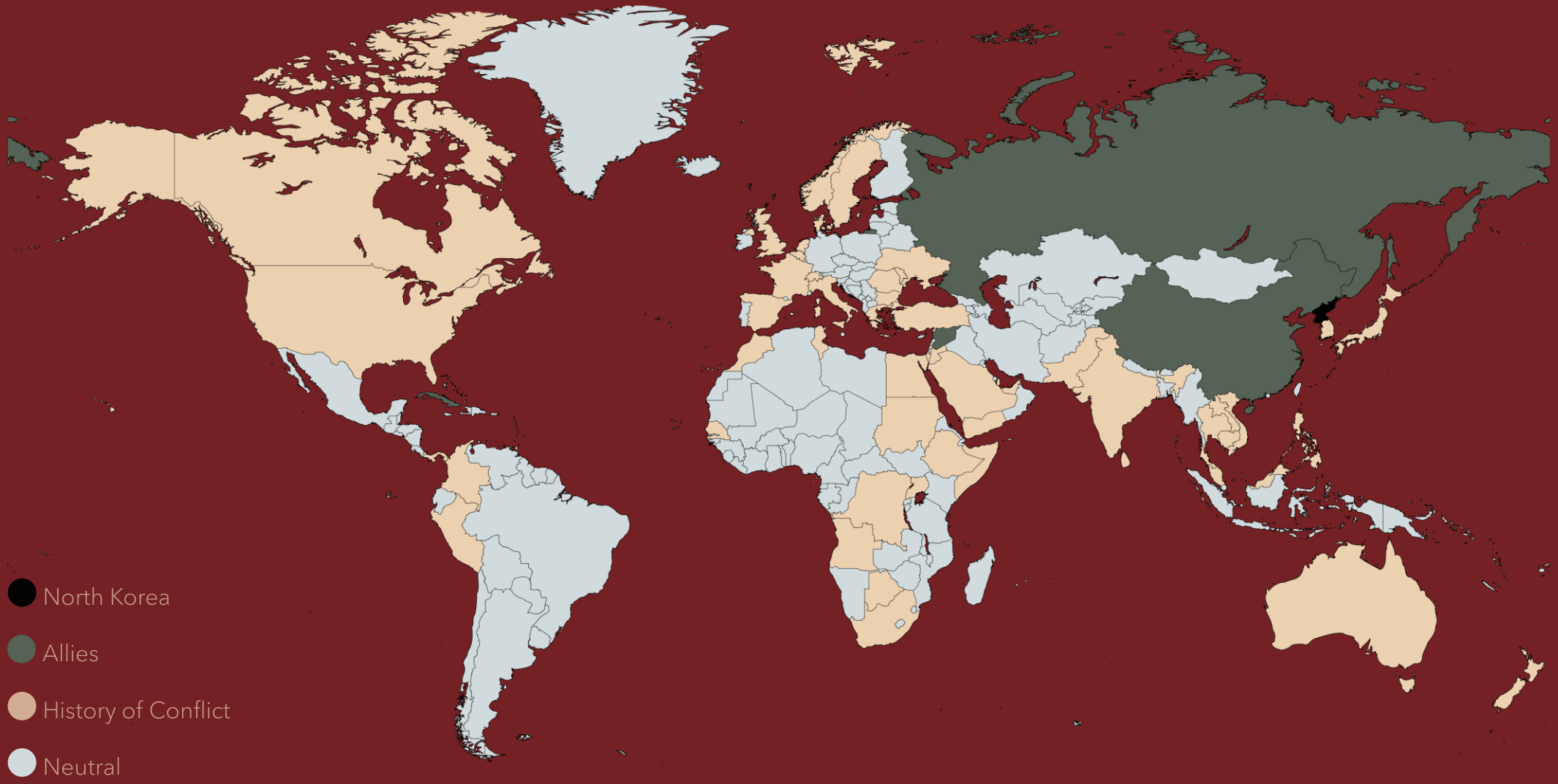


- 2011 – Kim Jong-Il dies from a heart attack and Kim Jong-Un is declared supreme leader
- 2012 – Kim Jong-Un makes his first public speech as leader of North Korea and announces that threats against North Korea will not affect the country
- 2020 – North Korea shut their borders in response to COVID-19 and enforced a “Shoot-To-Kill” order to prevent anyone from crossing the border

INTERNATIONAL RELATIONS

- North Korea
- Allies
- History of Conflict
- Neutral




North Korea
Allies
History of Conflict
Neutral

GOVERNMENT

- Democracy on paper
- Dictatorship in practice
- Governed by the *Socialist Constitution of The Democratic People's Republic of Korea*

LEGAL SYSTEM

"Citizens are guaranteed freedom of speech, the press, assembly, demonstration and association.

The State shall guarantee the conditions for the free activities of democratic political parties and social organizations."

SOCIALIST CONSTITUTION OF THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA – **ARTICLE 67**

"A person who has spread incitement or propaganda with a purpose against the nation shall be sentenced to a term of reform through labour of less than 5 years.

In particularly grave cases, he or she shall be sentenced to a term of reform through labour of more than 5 years and less than 10 years."

CRIMINAL CODE OF THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (DPRK) **§ 62 (CHAPTER III, SECTION 1)**

MILITARY RESOURCES

- Participated in the Nuclear Non-Proliferation Treaty from 1985-1993
- Currently holding ~30 nuclear warheads
- Announced Hydrogen-Bomb in 2016

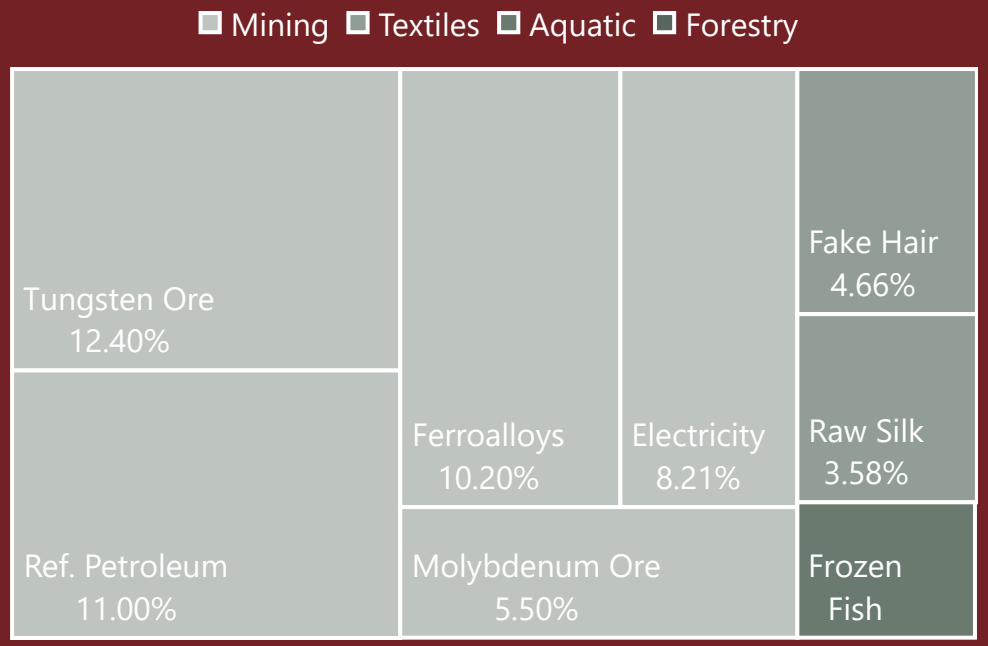
Ri Chun-hee & Kim Jong viewing an apartment in Pyongyang.
(Belfast Telegraph, 2022) (BBC News, 2016)

ECONOMY

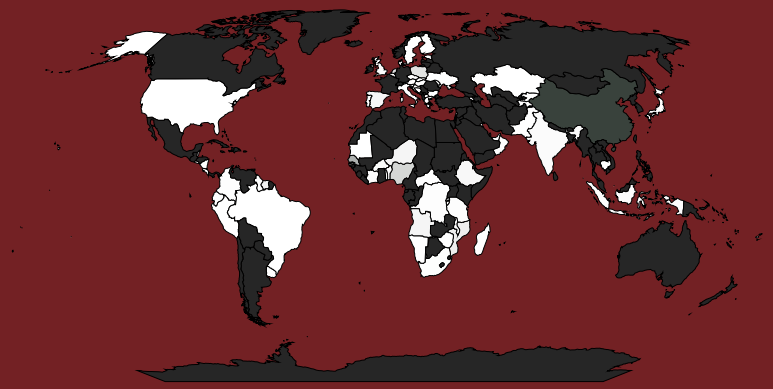
- *Command Economy* system
  - Government controls the majority of industries to maintain control of production
- Globally…
  - 182nd in Per Capita **Export Value**
  - 219th in Per Capita **Import Value**

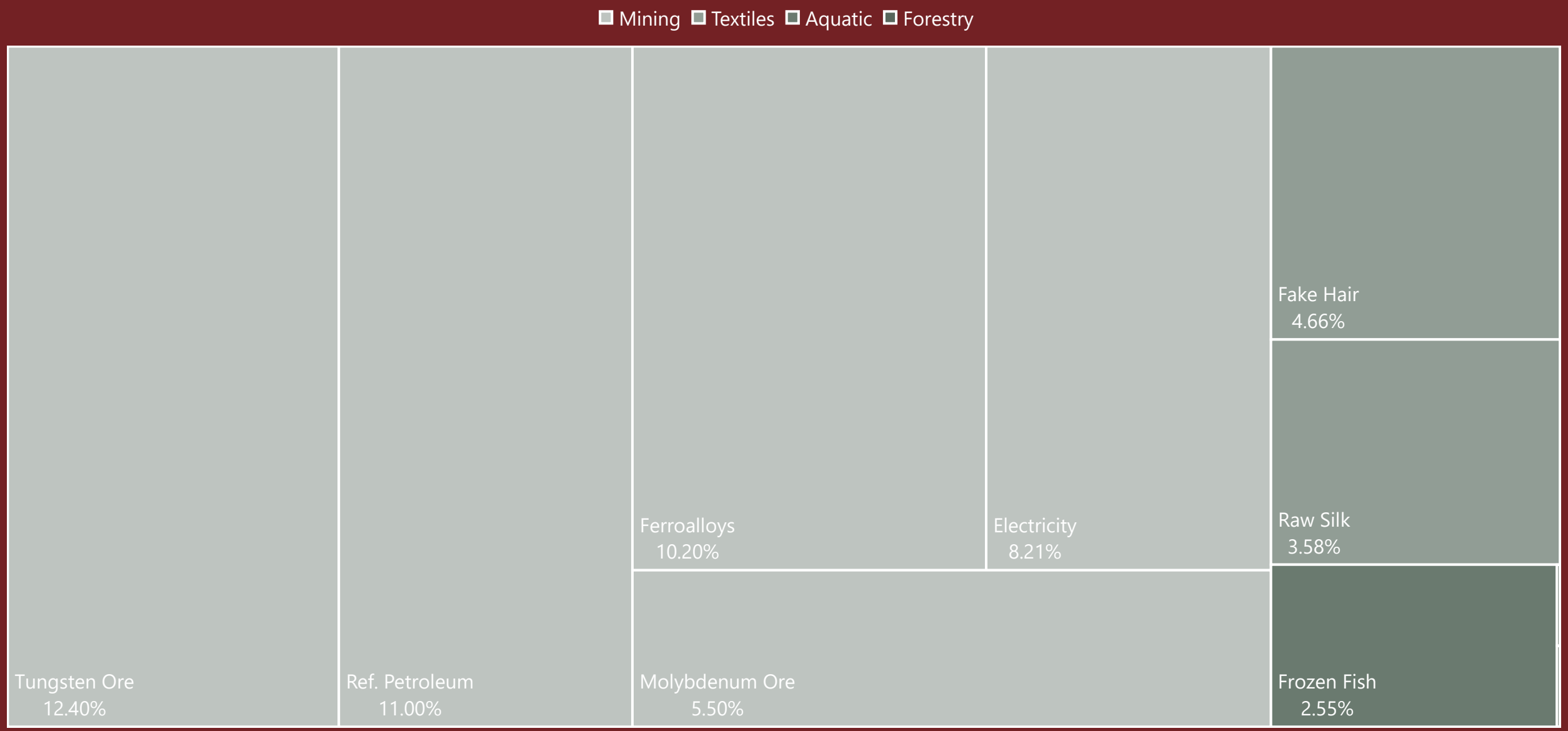
EXPORTS

EXPORTS



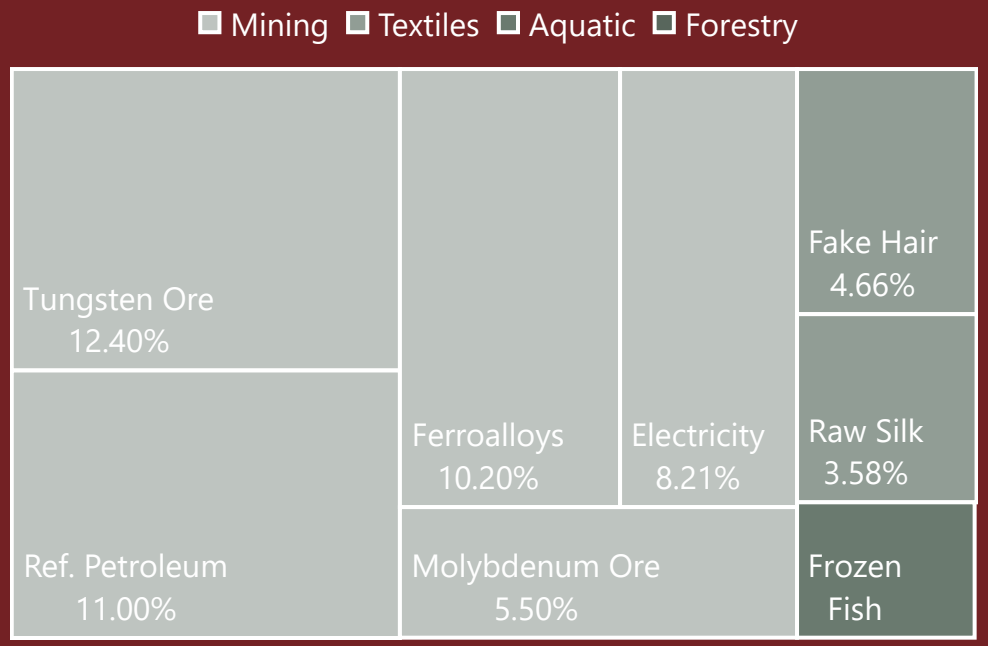
IMPORTERS



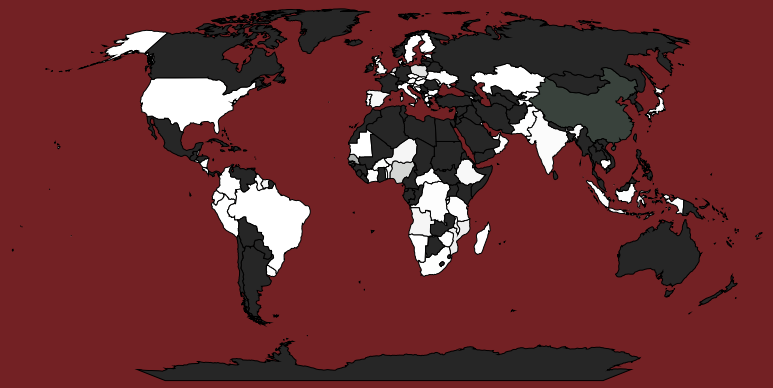

Mining
Textiles
Aquatic
Forestry
Tungsten Ore
12.40%
Ref. Petroleum
11.00%
Ferroalloys
10.20%
Electricity
8.21%
Molybdenum Ore
5.50%
Fake Hair
4.66%
Raw Silk
3.58%
Frozen Fish
2.55%

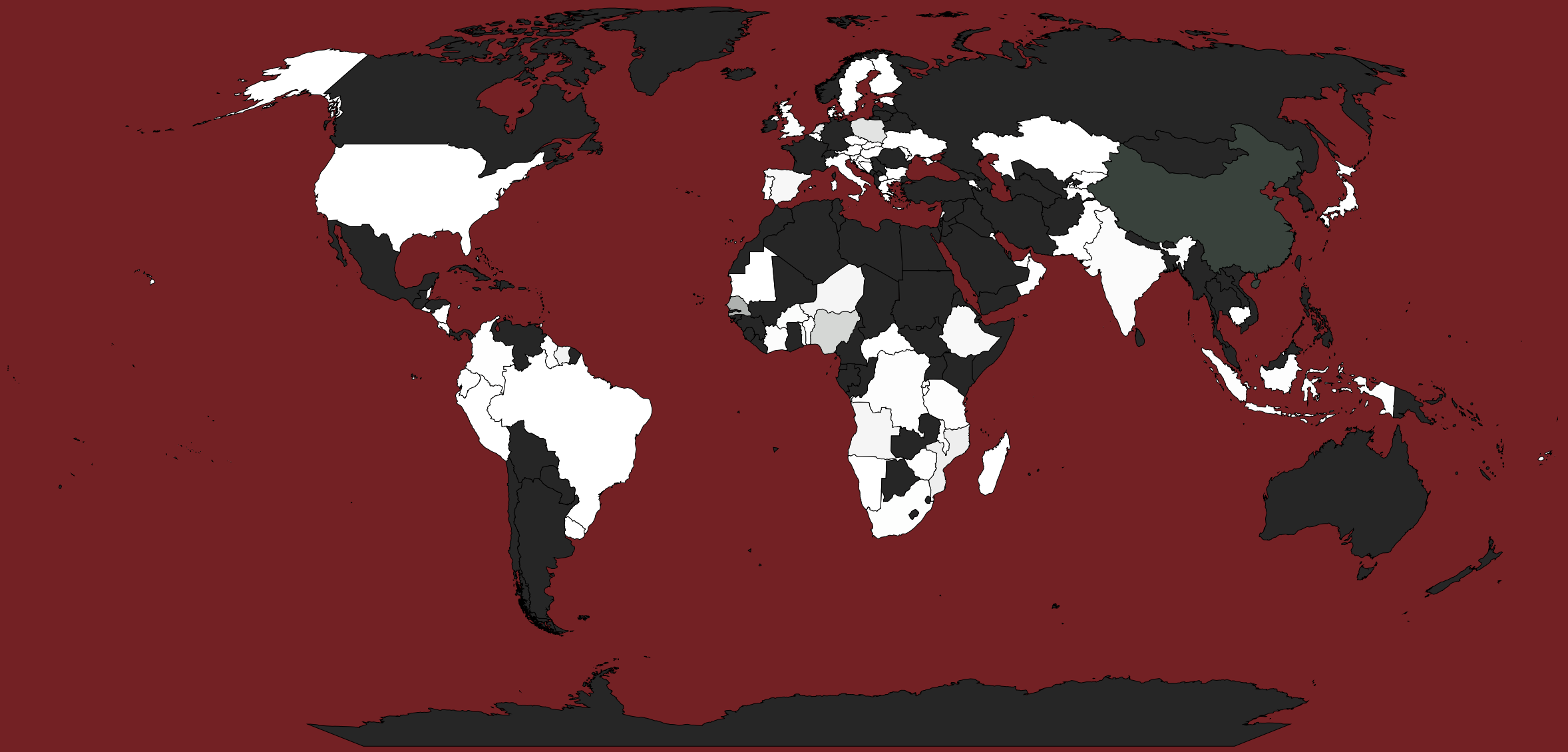
EXPORTS

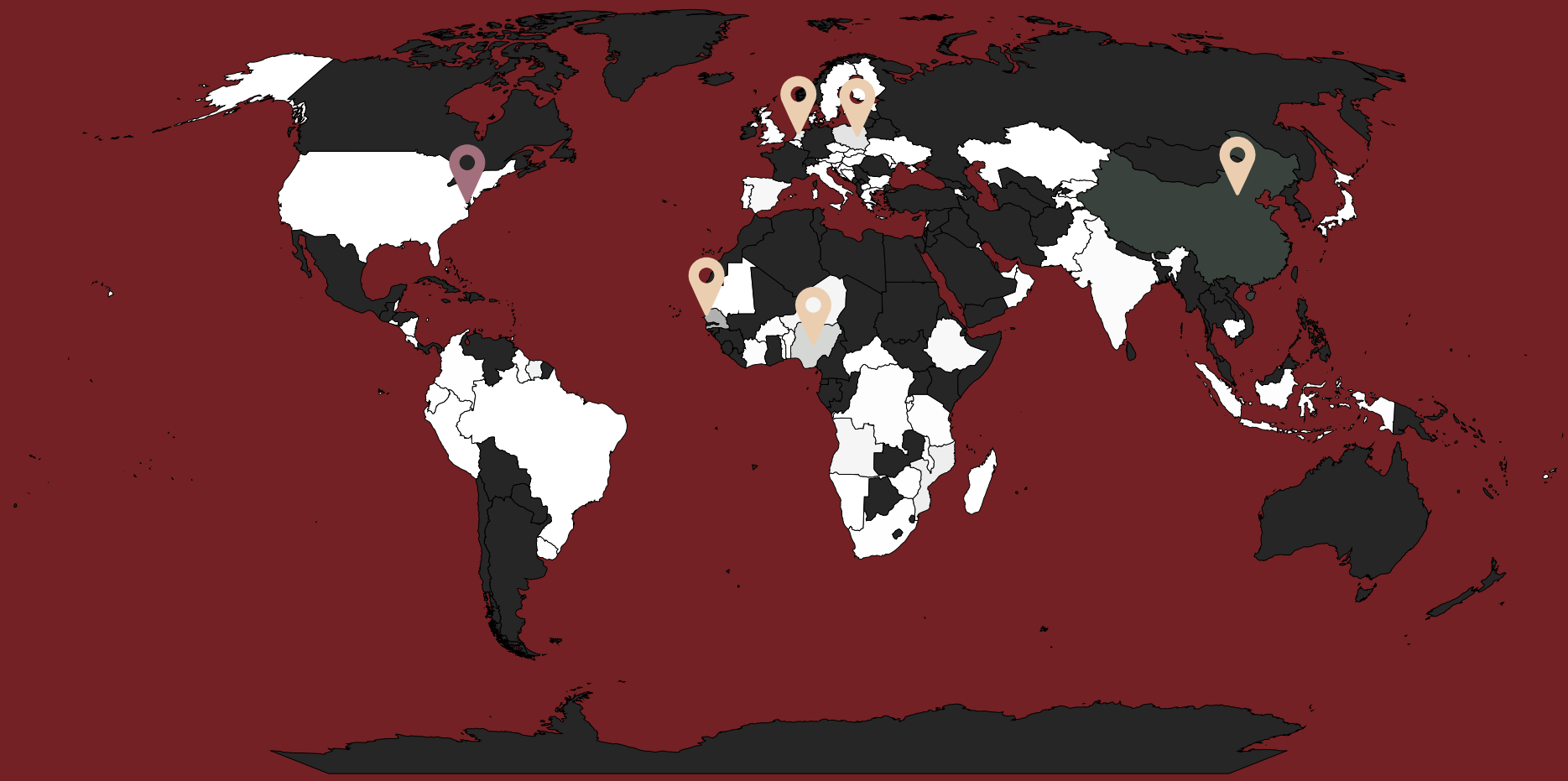
EXPORTS



IMPORTERS







% of Total
52.67%
26.33%
0.00%

Powered by Bing

Top 5 (2022)

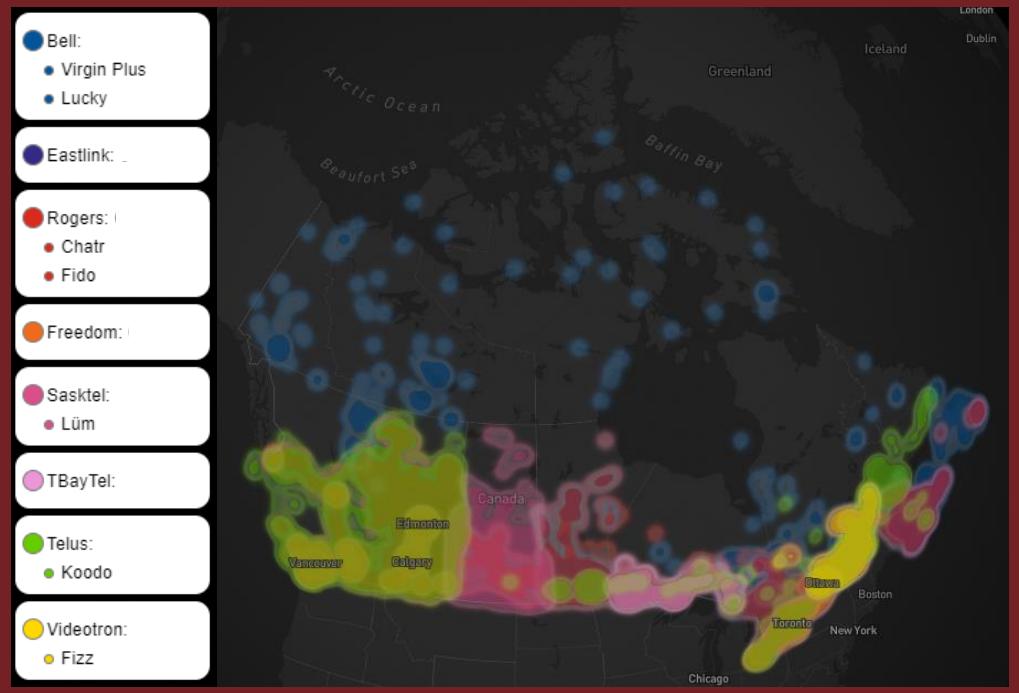
Country	% of Total
1. China	52.67%
2. Senegal	10.83%
3. Nigeria	5.64%
4. Poland	3.86%
5. Netherlands	3.14%
63. USA	0.01%
Gross: USD$248,426,656	

INFRASTRUCTURE

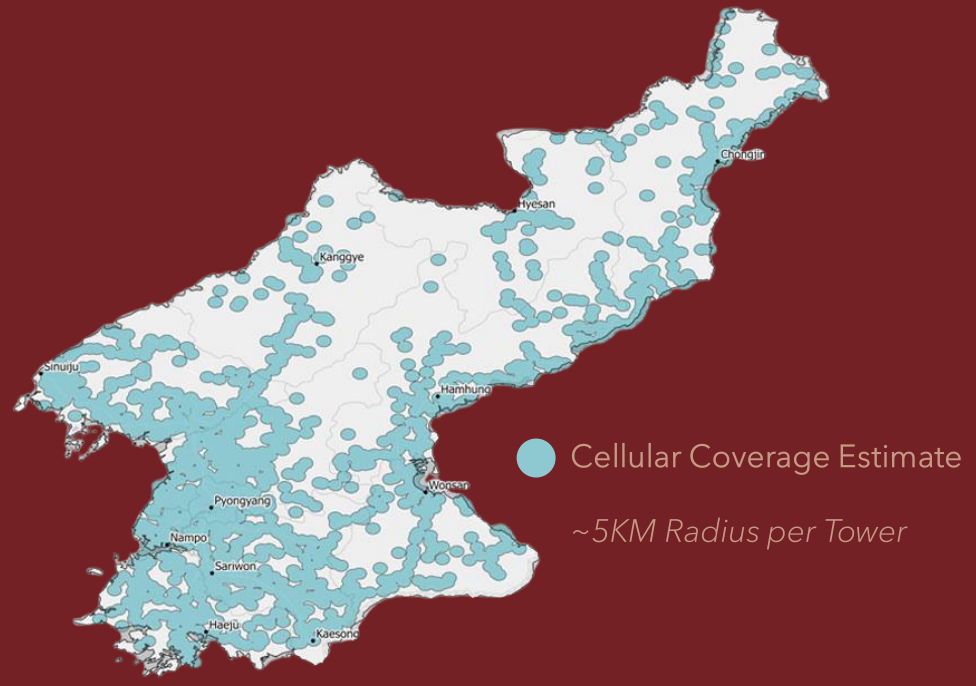
- **Fibre-Optic** or **DSL** connections for larger entities
- **Point-to-Point** Connections for most homes
- **19%** of Households own a computer
- **1%** of Households have access to *Kwangmyong*
- **~30** families with unrestricted internet

CELLULAR

CANADA



NORTH KOREA



PUBLIC AWARENESS

“I was taught about the World Wide Web, and even had to memorize it for an exam, but I only knew about the internet in theory…

I knew it was a sort of network where you can search but didn’t actually know what it was. “

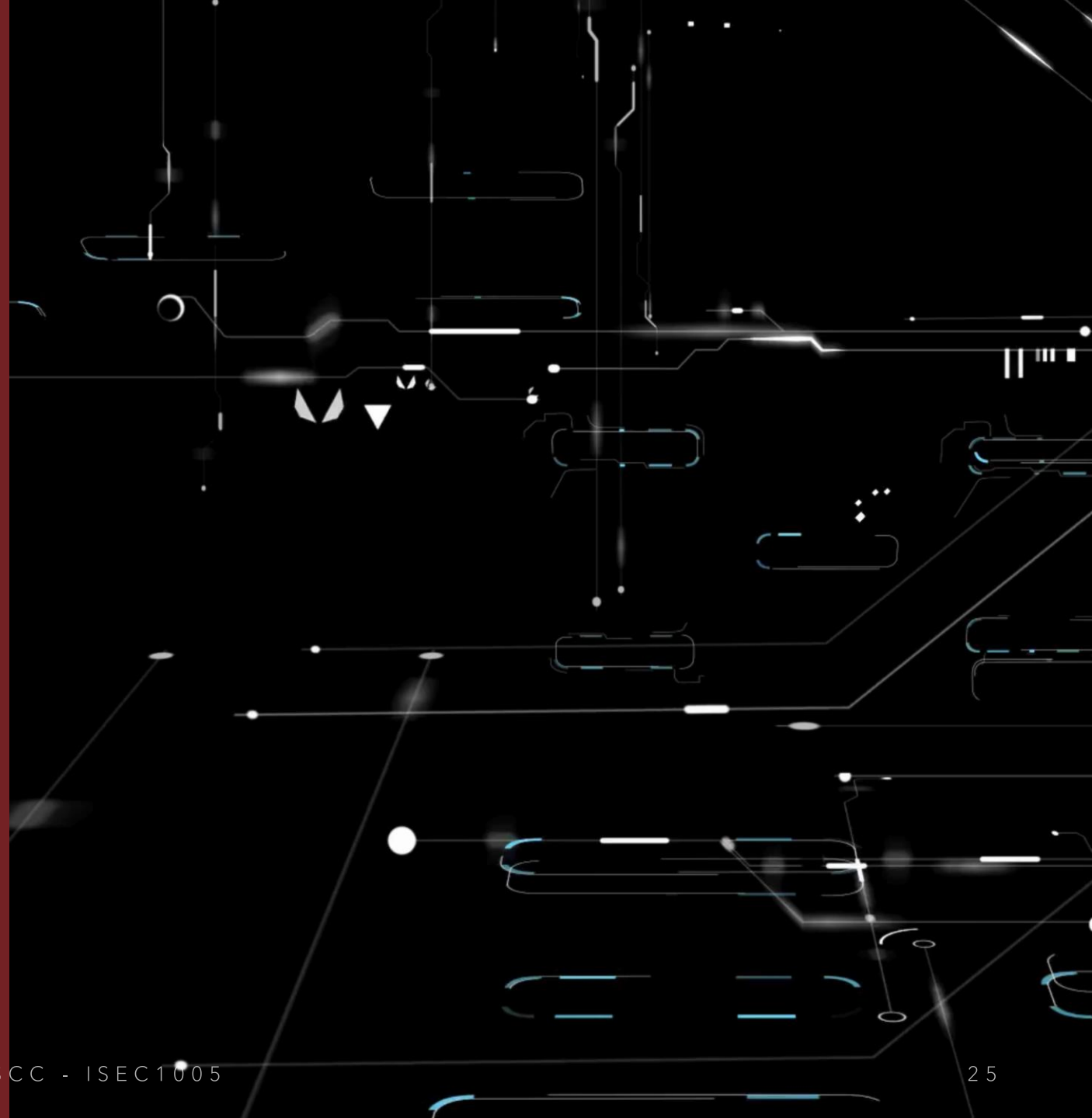
PEOPLE FOR SUCCESSFUL
COREAN REUNIFICATION

THREAT ACTOR'S MOTIVATIONS

- Early Motivations *(2009 - 2014)*
  - *Cyber espionage and disrupt communications on hostile nation states*
  - *Overtly support the North Korea regime and leader Kim Jong-Un*
- Current Motivations *(2016 – 2024)*
  - *Targeting the financial sectors of foreign organizations and government agencies*
  - *Funds contributes 50% of North Korea's Gross National Income*

LAZARUS GROUP

- Umbrella term for public reporting on North Korea Cyber Threat Actors
- Operates under protection of North Korea's Reconnaissance General Bureau
- Notable Sub-Groups of Lazarus:
  - BlueNorOff - *Financial*
  - AndAriel - *Development*
  - Kimsuky - *Intelligence*



KNOWN INDIVIDUALS

- 3 ‘Lazarus’ members indicted by US DOJ in Feb. 2021
- 1 Member of sub-group ‘AndAriel’ indicted by US DOJ in July 2024
- 3 individuals have been indicted for working as ‘Money Mules’ for North Korea cyber operations
  - Tian Yinyin (Chinese) – *Indicted in March 2020*
  - Li Jiadong (Chinese) – *Indicted in March 2020*
  - Ghaleb Alaumary (Canadian) – *Indicted in Feb. 2021*

Park Jin Hyok

Jon Chang Hyok

Kim Il

Rim Jong Hyok

COMMON ATTACK TECHNIQUES

- Social Engineering
  - *Spear-phishing attacks on employees of target organization*
  - *Use of credential-harvesting websites*
- Insider Attacks
  - *Sending IT-trained individuals abroad to work for target organization under cover*

COMMON ATTACK TECHNIQUES

- Vulnerability Exploitation
  - *'EternalBlue' NetBIOS Exploitation*
  - *Cross-Bridge Blockchain Exploitation*
- Use of Malware
  - *Creation or purchasing of various malicious software.*

ATTACK TIMELINE

2009-2013

DDoS Attacks

Target: South Korea, USA
Vector: DDoS via Botnet
Result: Data Leak

2014

Sony Breach

Target: Sony Pictures
Vector: Social Engineering
Result: Data Leak

2016

Bangladesh Bank Heist

Target: Bangladesh Bank
Vector: SWIFT Exploit
Result: USD$81M

2017

WannaCry Ransomware

Target: Global
Vector: Crypto-Worm
Result: USD$130M

2020-2021

Spear Phishing

Target: Tech & Pharma
Vector: Social Engineering
Result: *Unconfirmed*

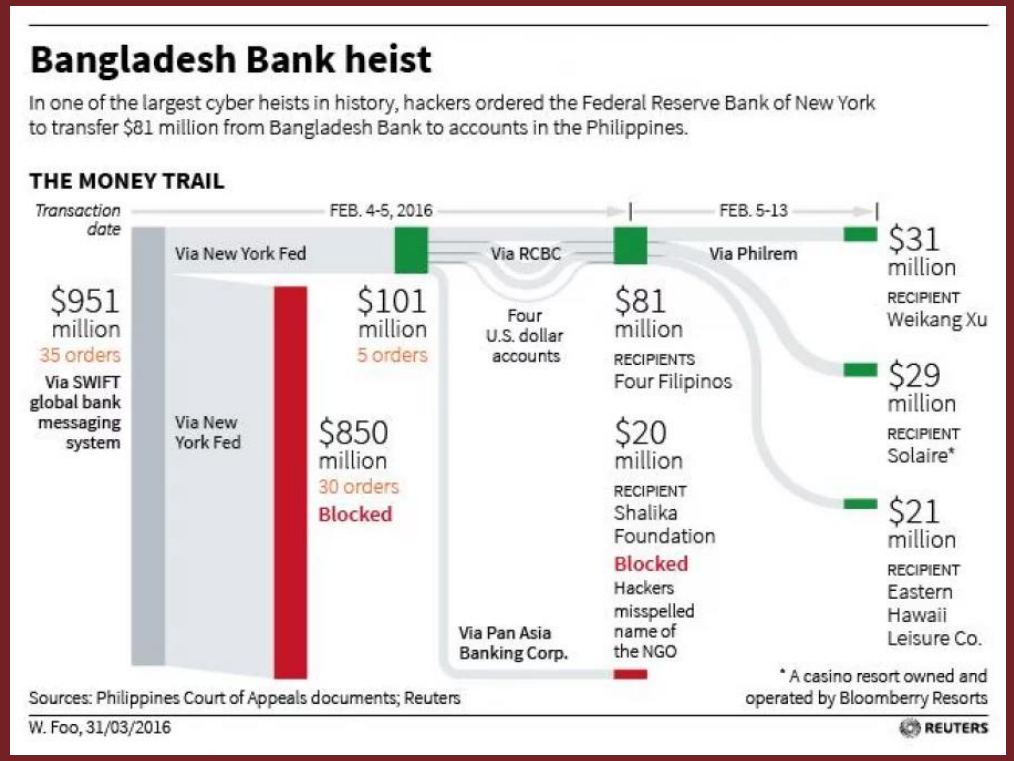
Current

Crypto Theft

Target: Crypto-Finance
Vector: Blockchain Exploit
Result: ~USD$2B

BANGLADESH BANK

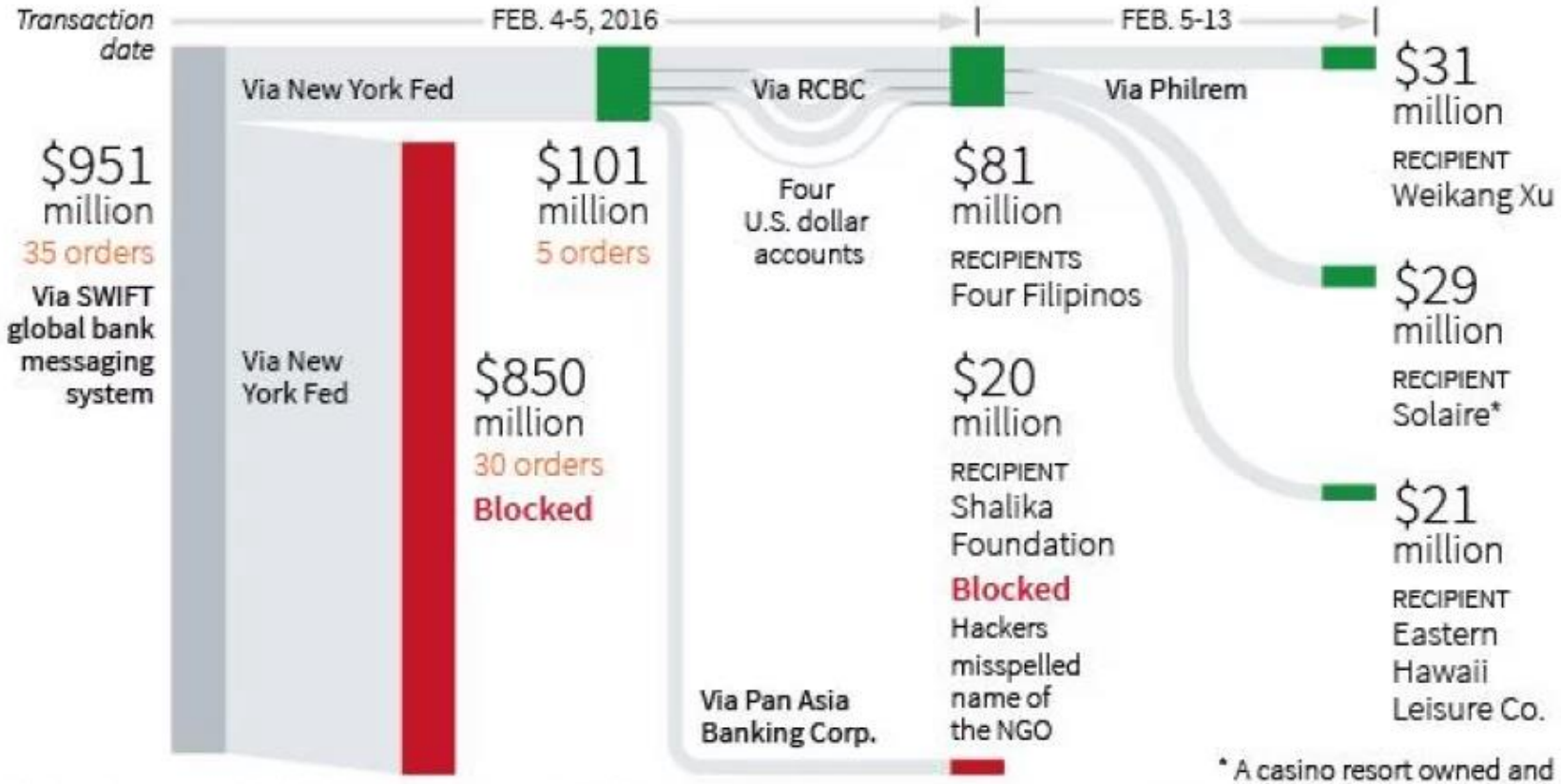
- Lazarus gained access to the banks SWIFT software
- Similar techniques to the Sony breach
- Requested 35 transfers totaling USD$951M
- USD$100M in transfers were finalized
- USD$851M was held
  - USD$20M transfer to Sri Lanka was held because of a typo



Bangladesh Bank heist

In one of the largest cyber heists in history, hackers ordered the Federal Reserve Bank of New York to transfer $81 million from Bangladesh Bank to accounts in the Philippines.

THE MONEY TRAIL



Sources: Philippines Court of Appeals documents; Reuters

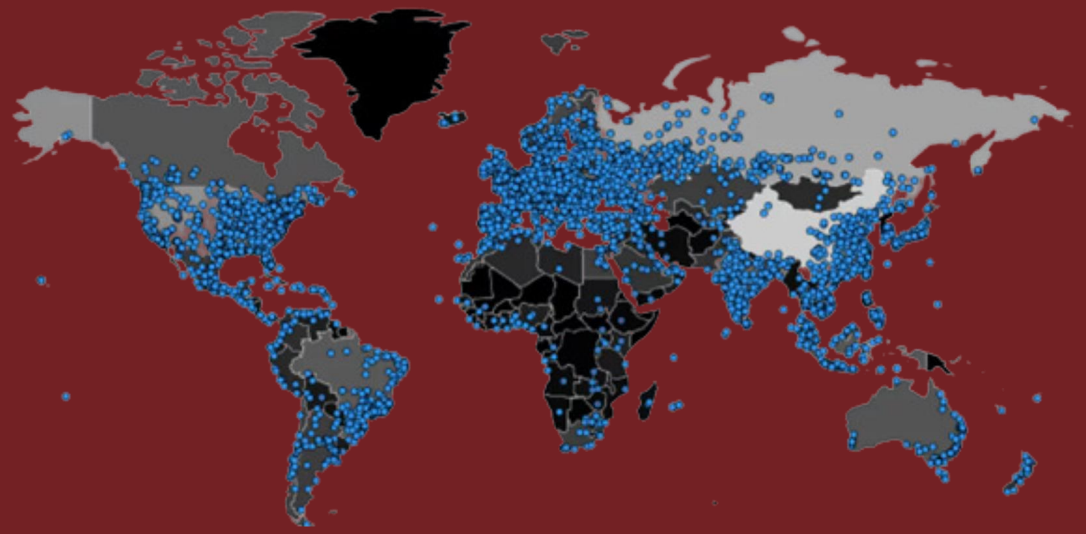
* A casino resort owned and operated by Bloomberry Resorts

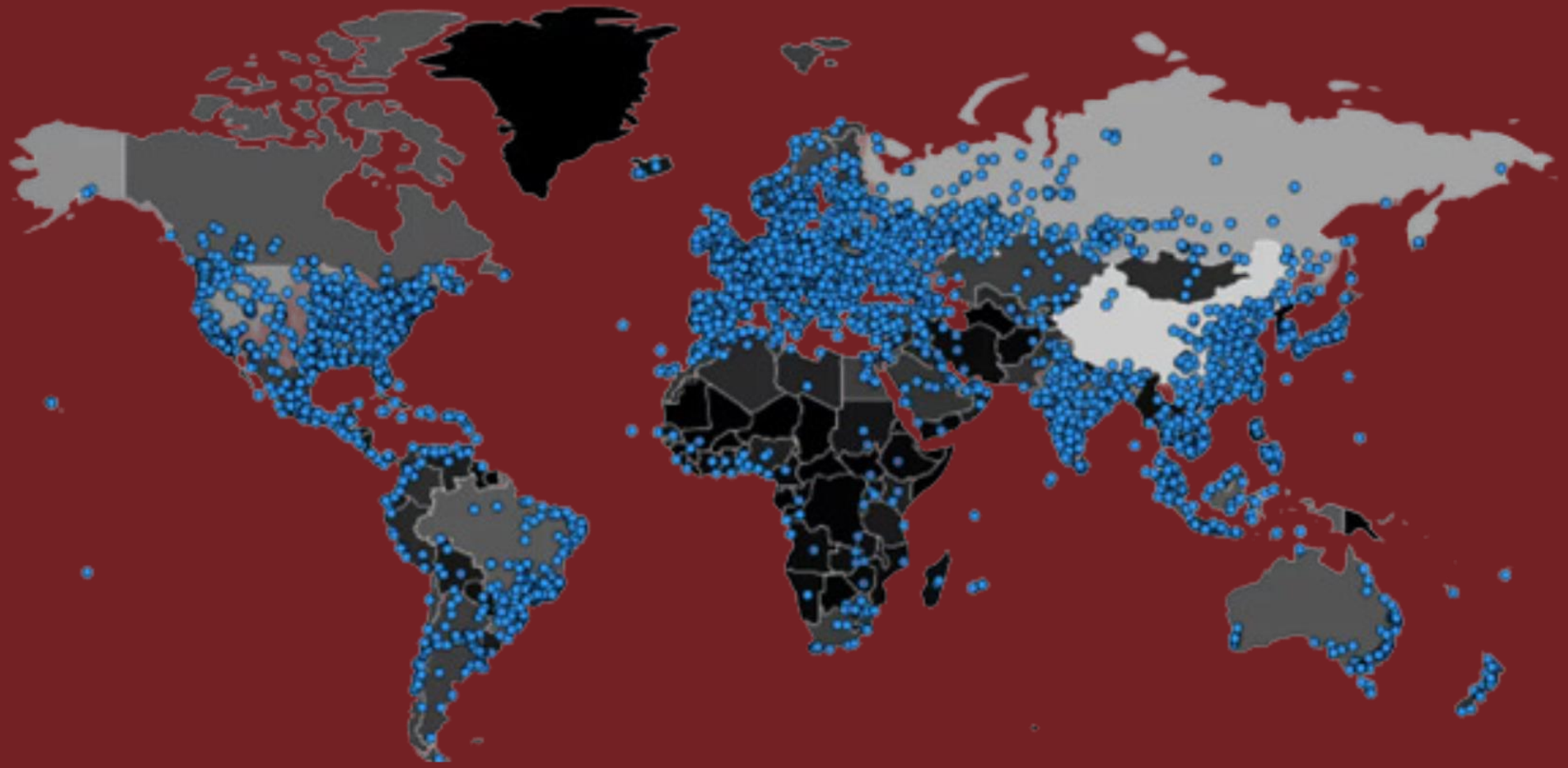
W. Foo, 31/03/2016

REUTERS

WANNACRY

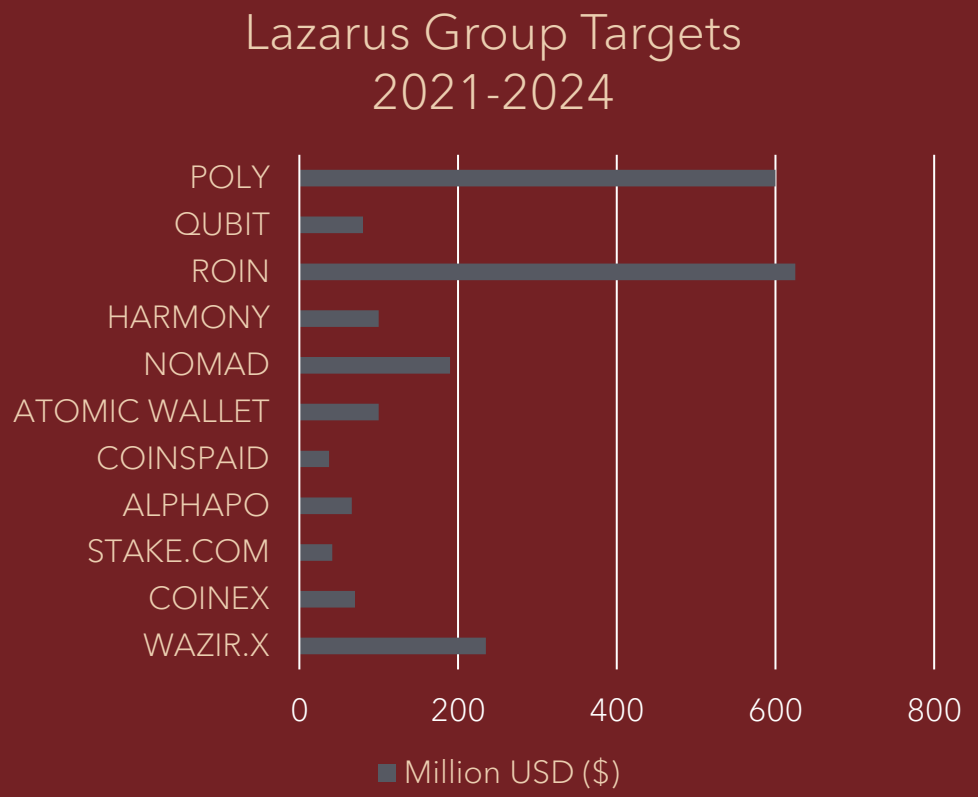
- May 2017 – Lazarus used a crypto-worm malware named “WannaCry”
- Used EternalBlue vulnerability to execute code on the target’s computer, downloading “DoublePulsar”
- It encrypted and deleted the shadow copies of all the data
- Infected over 300,000 computers within seven hours
- Over $4 Billion in damages
- Kim Jong-Un authorized WannaCry’s release





CRYPTO ATTACKS

- Over USD$2B Stolen since 2021
- Majority of recent cyber attacks target:
  - *Crypto exchanges/payment processors*
  - *Crypto-based casinos*
- Common Methods:
  - *Social Engineering/Spear-Phishing*
  - *Cross-Bridge Blockchain Protocol Exploitation*
  - *Crypto 'Hot Wallet' Vulnerability*
  - *Use of Crypto-Tumbler Malware*




NORTH KOREA