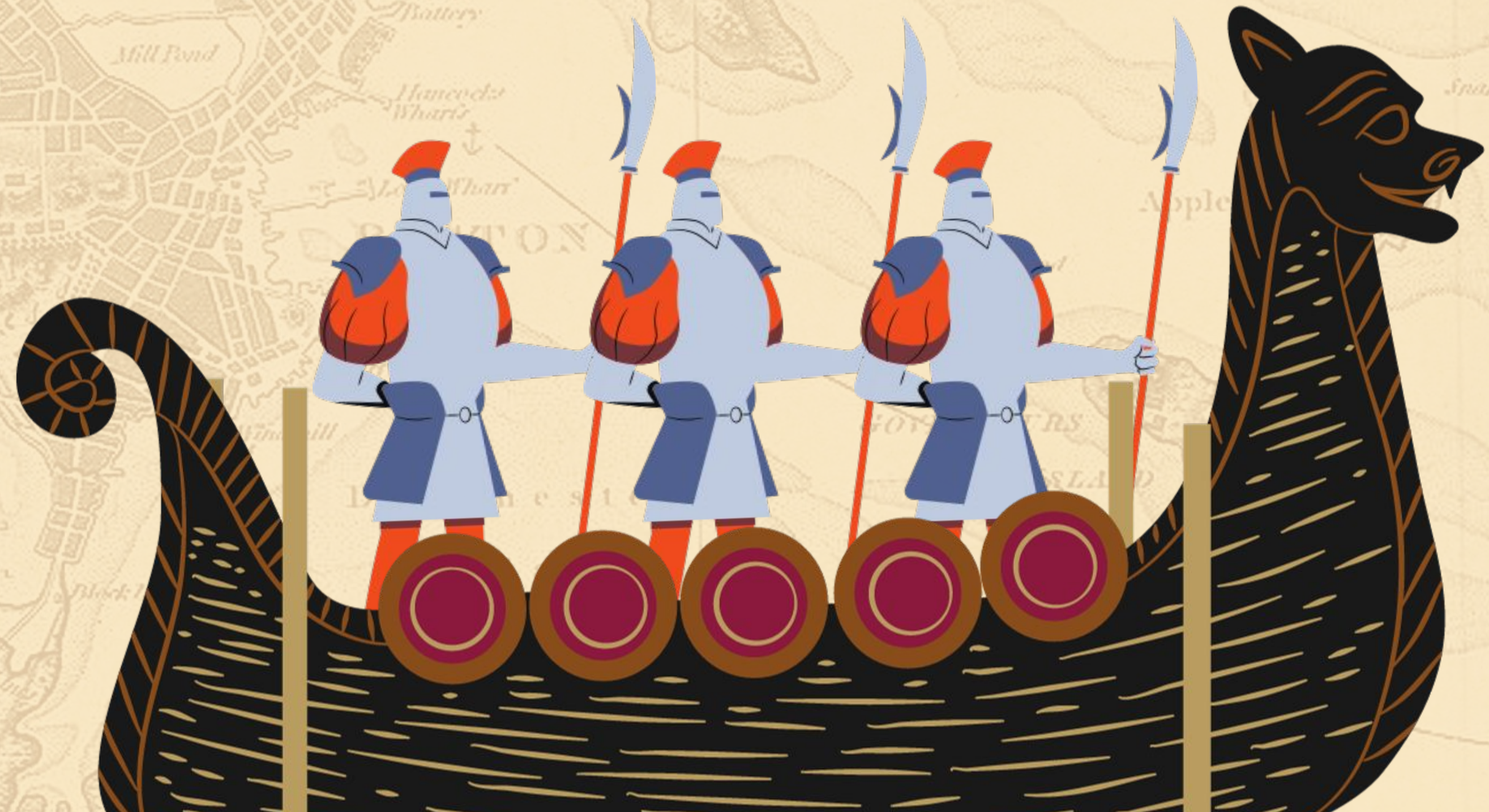
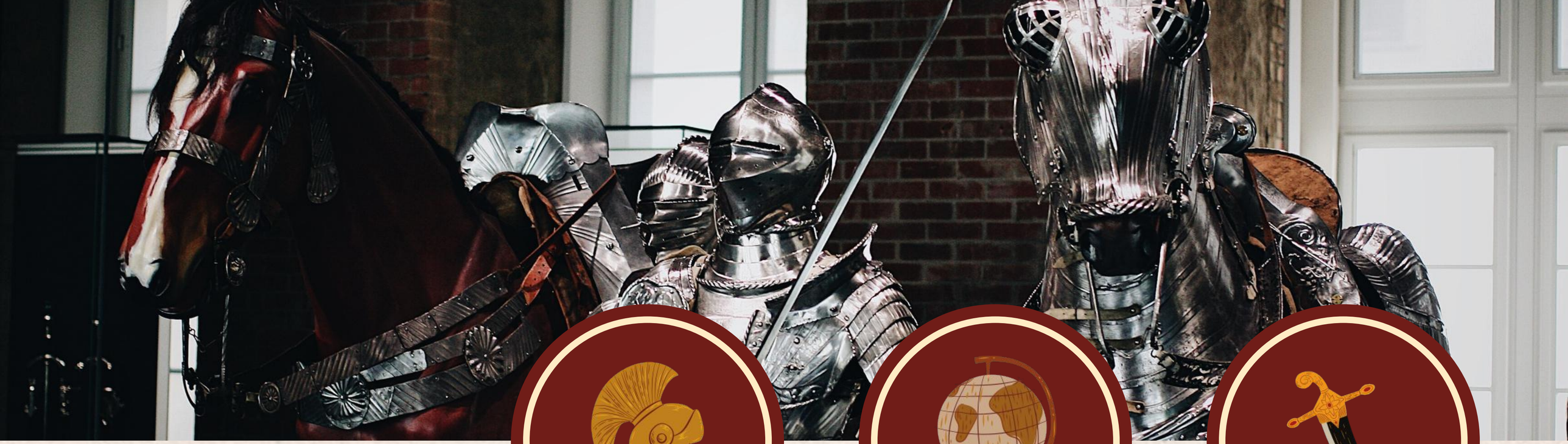
Cyberwarfare

A SIGPwny x SIGPolicy Presentation





THE ETHICAL BOUNDARIES OF DIGITAL CONFLICT

What is Cyberwarfare?

Global Cyberwarfare Policy

Current American Policy on Cyberwarfare

01

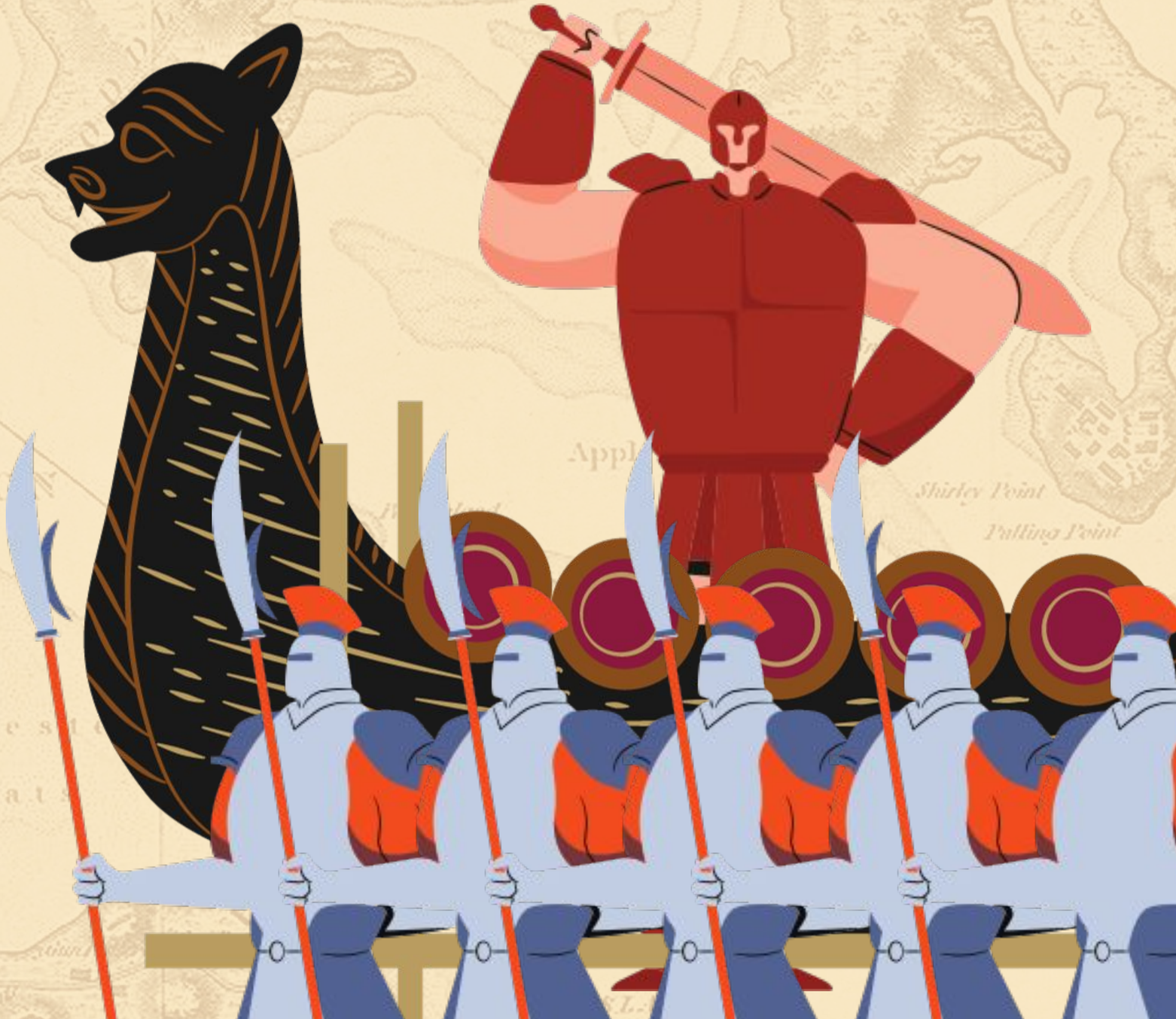
What is Cyberwarfare?

Cyberwarfare

- The use of “technological force” on computer networks
- Aims to disrupt or destroy computer-based systems
- Examples:
  - Spying on adversaries to reduce trust
  - Sabotaging equipment
    - Stuxnet
  - Destroying electrical grids

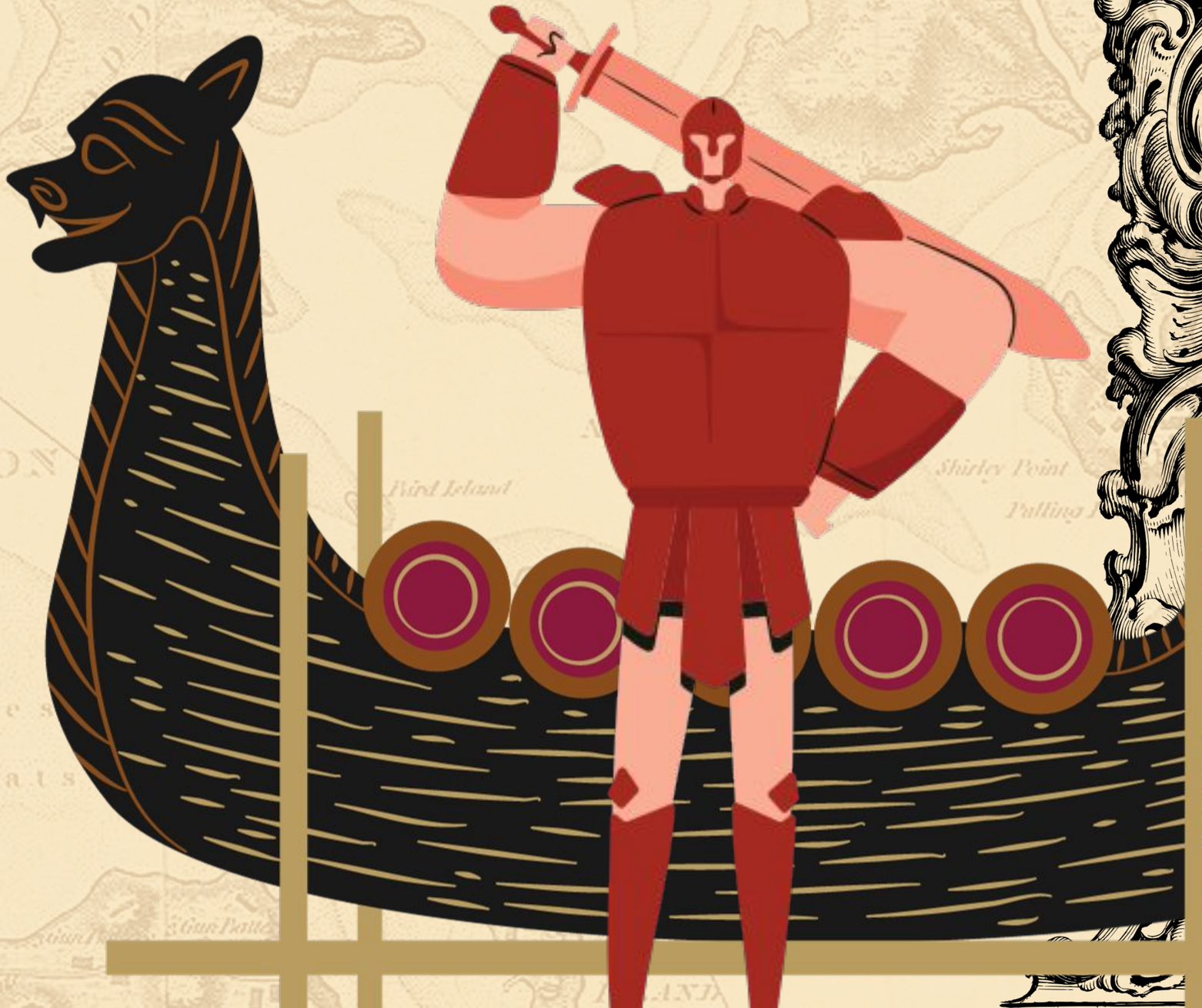
When should cyberwarfare go hot?

Are there any systems that demand war if destroyed? Hospitals? Electrical grids? Military systems?

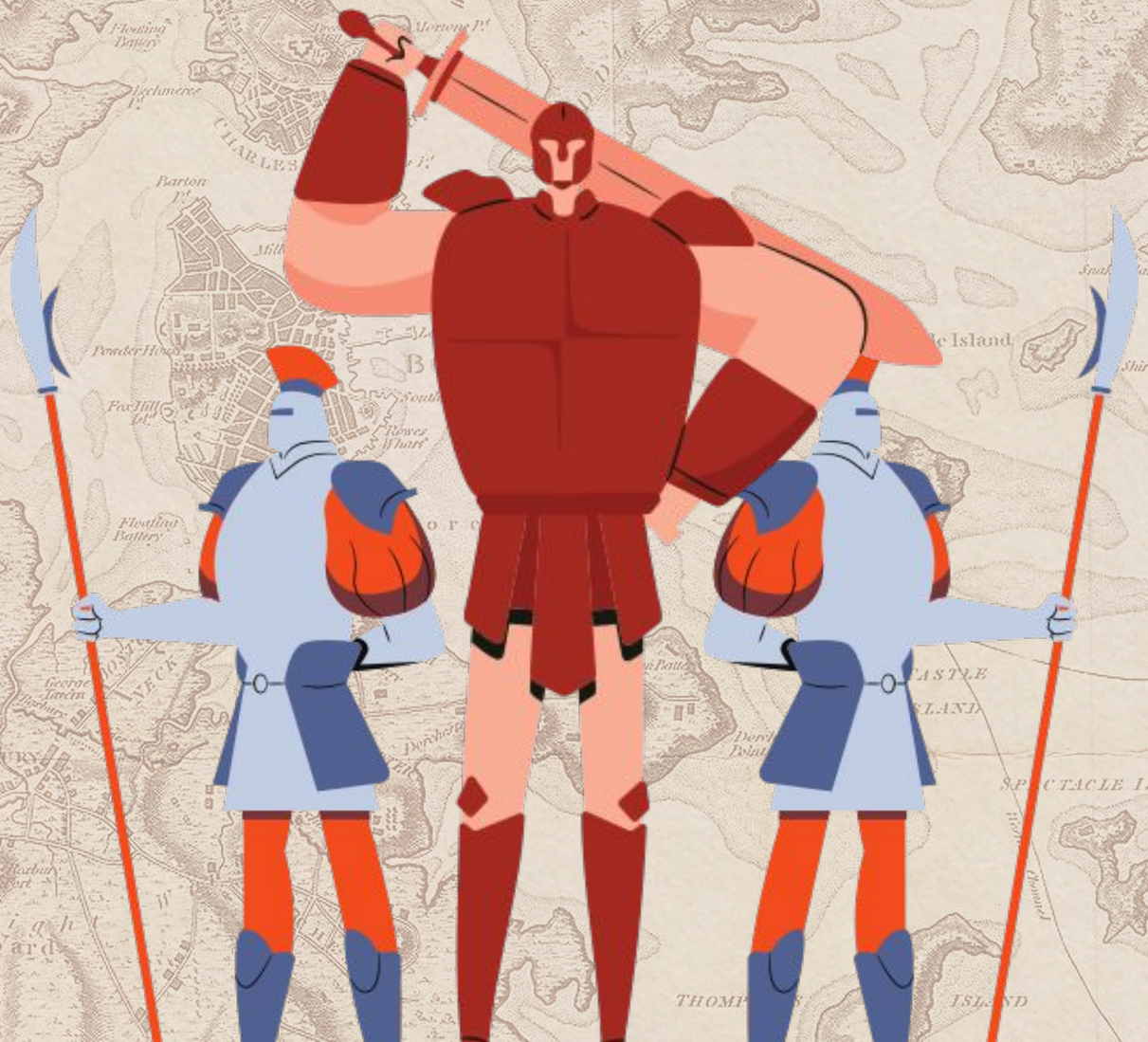


02

GLOBAL POLICY



Characteristics



01 Less than armed conflict

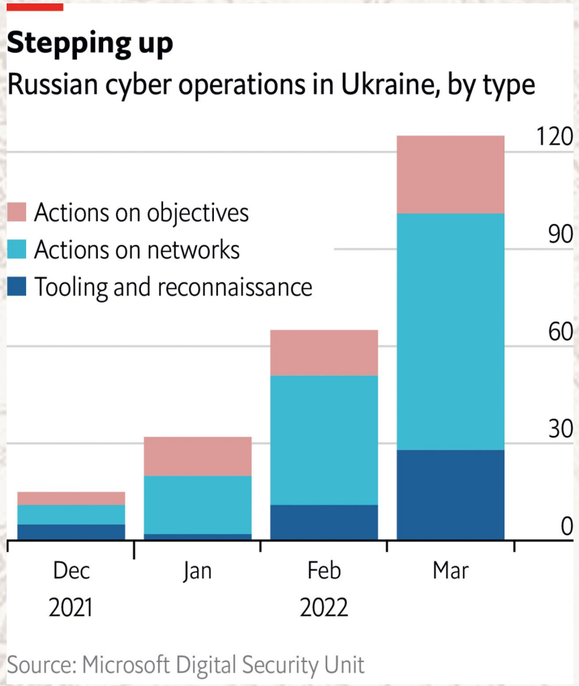
02 More “democratic”

03 “Joint-use” Targets

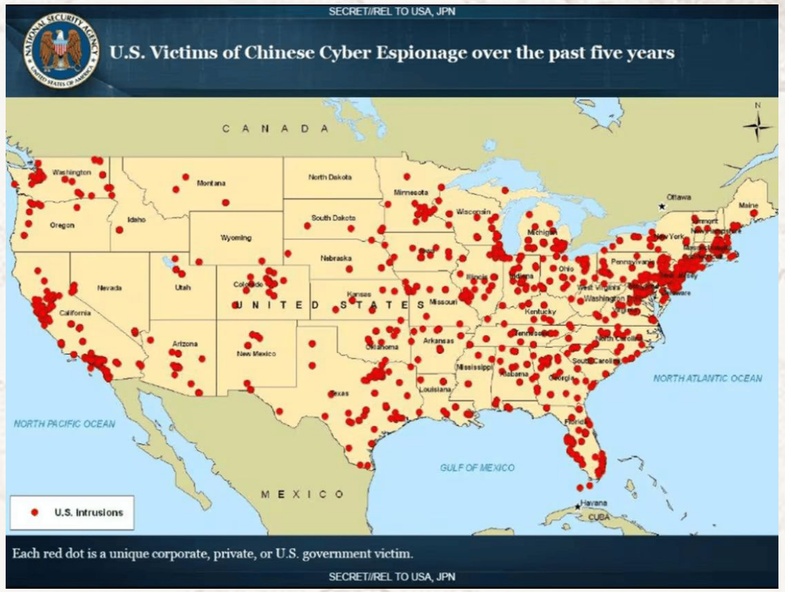
04 Not necessarily bound by the rules of war

Global cyber warfare usage

Russia

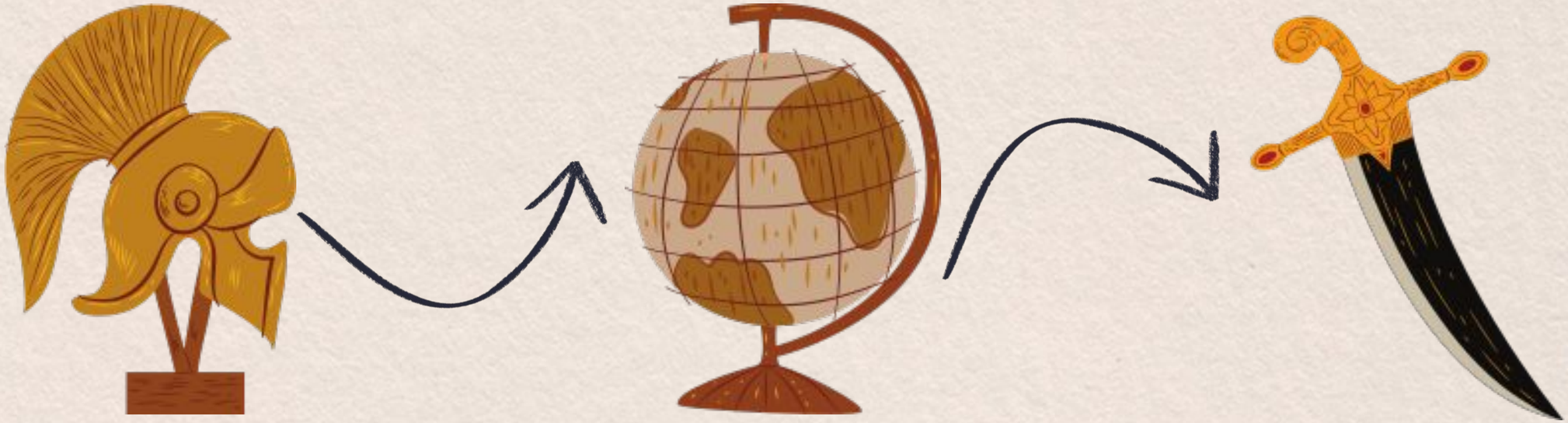


China



North Korea

“NON-STATE” ACTORS



ORIGIN

Countries fund and organize companies that have plausible deniability, yet can share technology and attack vectors.

ATTACK

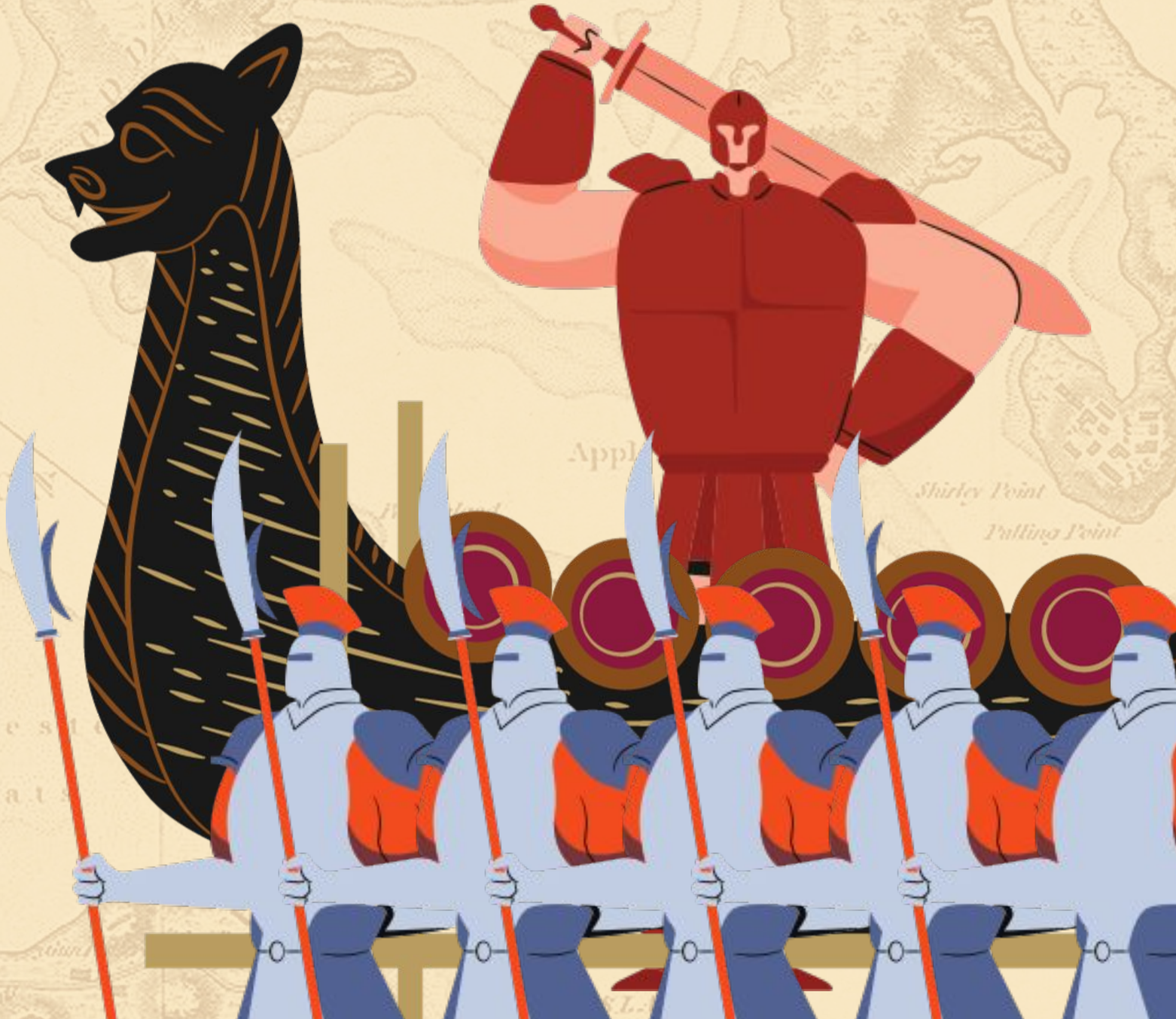
These groups can carry out attacks, such as the Colonial Pipeline attack, disrupting adversaries and collecting funds, without fear of war or sanctions.

REPRISAL?

Target countries are largely unable to reprise, as it is very challenging to prove the link. Some countries, especially the US, go on the offense in response, striking at the companies.

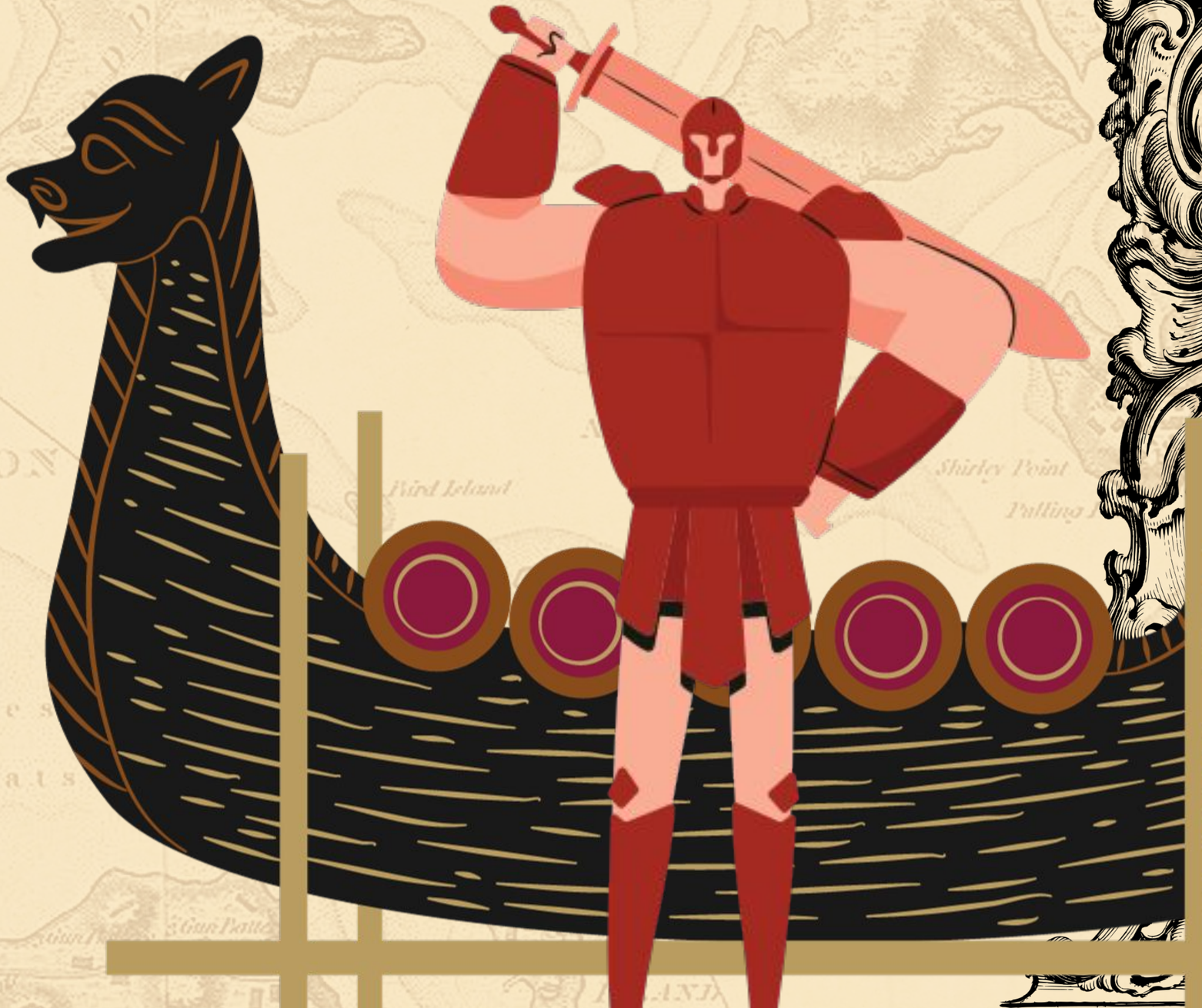
How should nations respond?

What level of confidence is sufficient? 30%, 50%, only 100%?

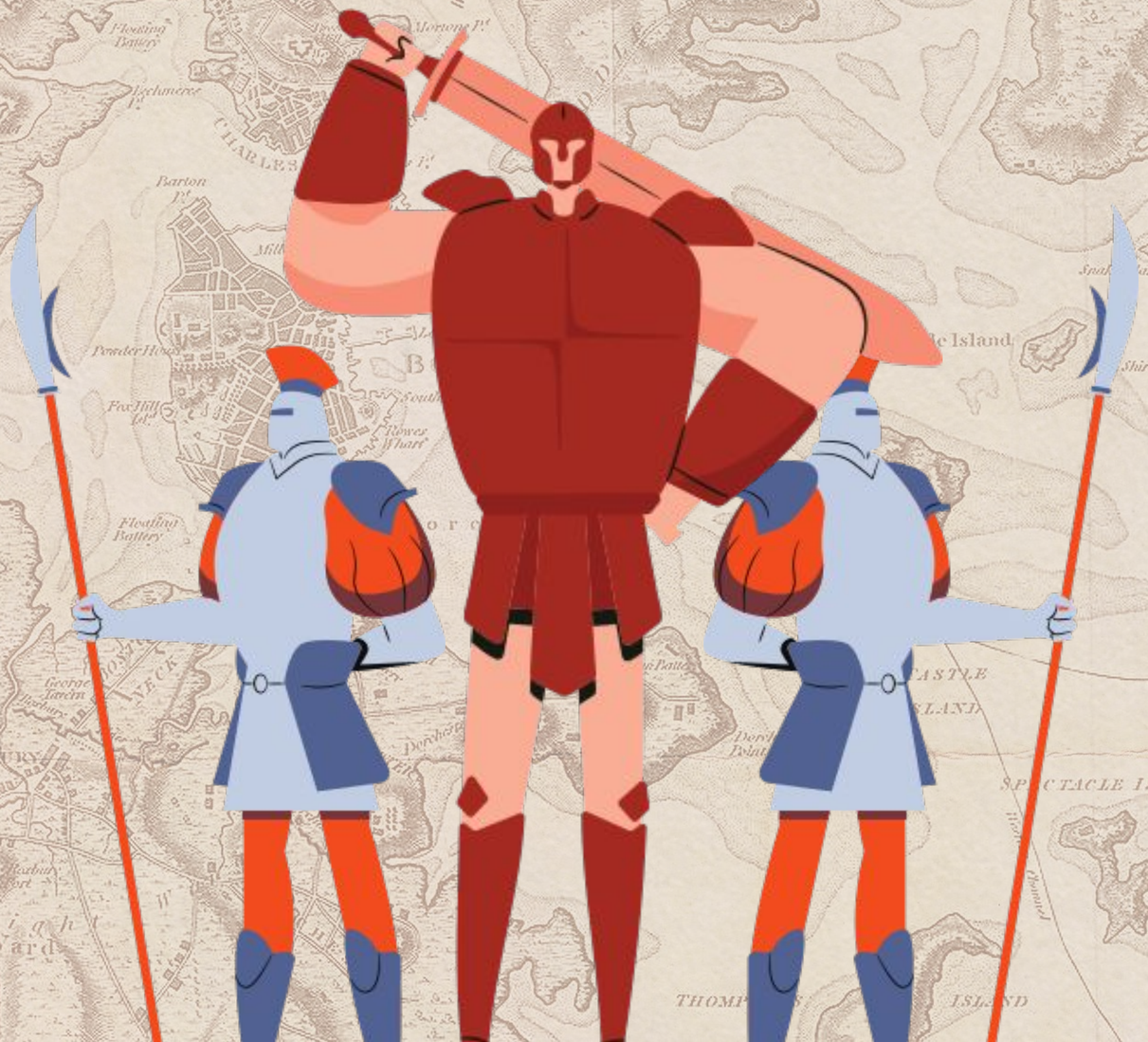


03

AMERICAN POLICY



Characteristics



01 Explicitly less than armed conflict

02 Offense as the best defense

03 “Obey” the rules of war

04 Largely focused on “non-state” actors

US Cyber attacks

Russia

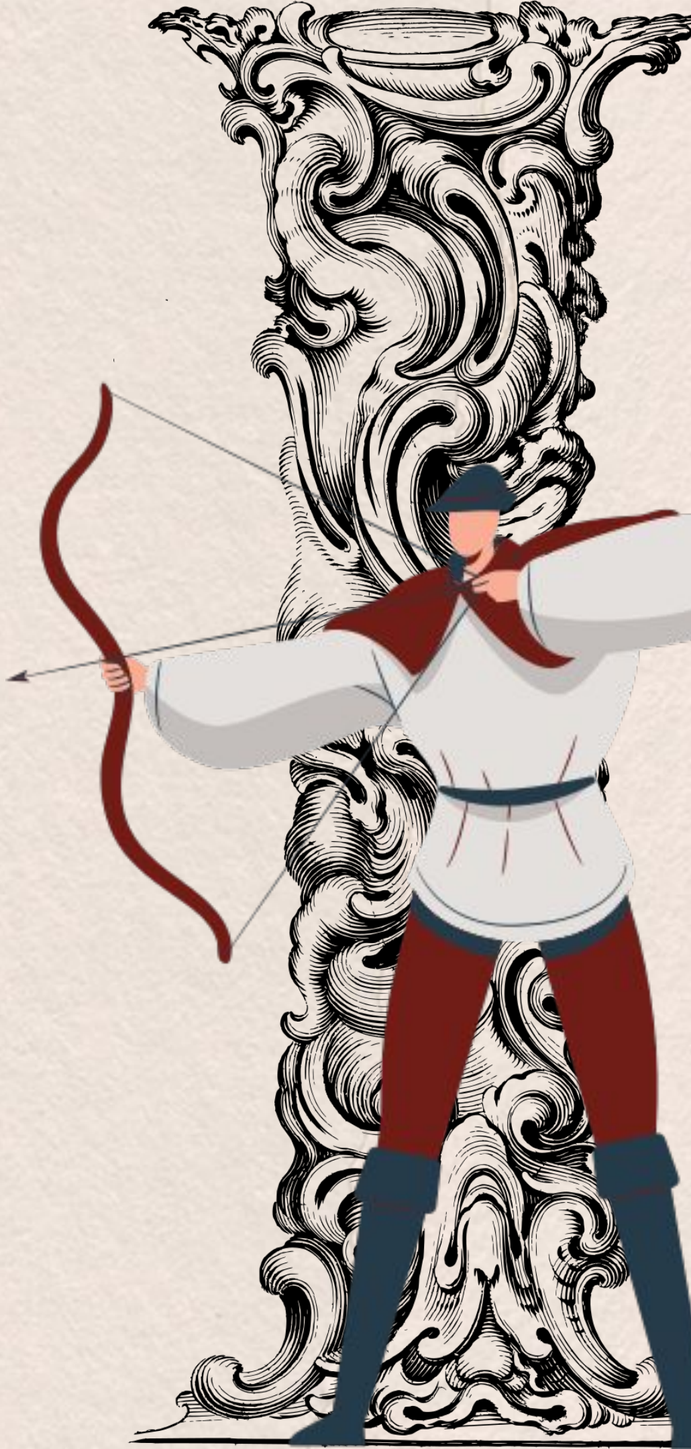
- Continuous strikes on non-state actors
- Counter-offensive in Ukraine-centered cyberwar
- Control over the power grid - possibly

China

- Continuous strikes on non-state actors
- Sanctions on many of these groups
- NSA insertions(especially Huawei)
- CERNET attack
- Spying on universities

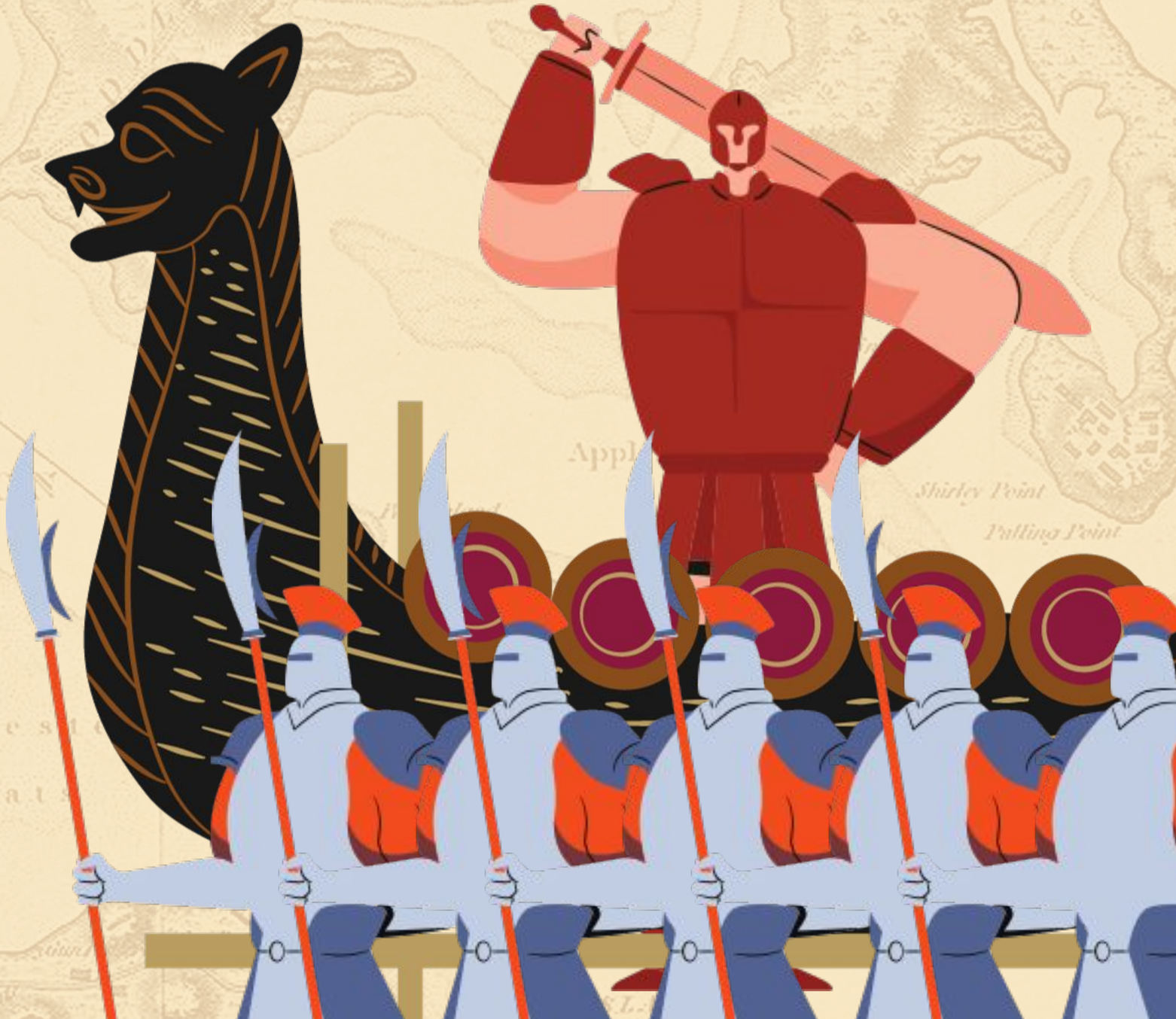
Others

- Stuxnet attack
- Strikes on North Korean groups
- Continuous purging of attacks (hardware, software)



How should we think of cyberwarfare?

Is this the new nuclear threat? Or is this a new frontier for a lower-risk, global cold war?

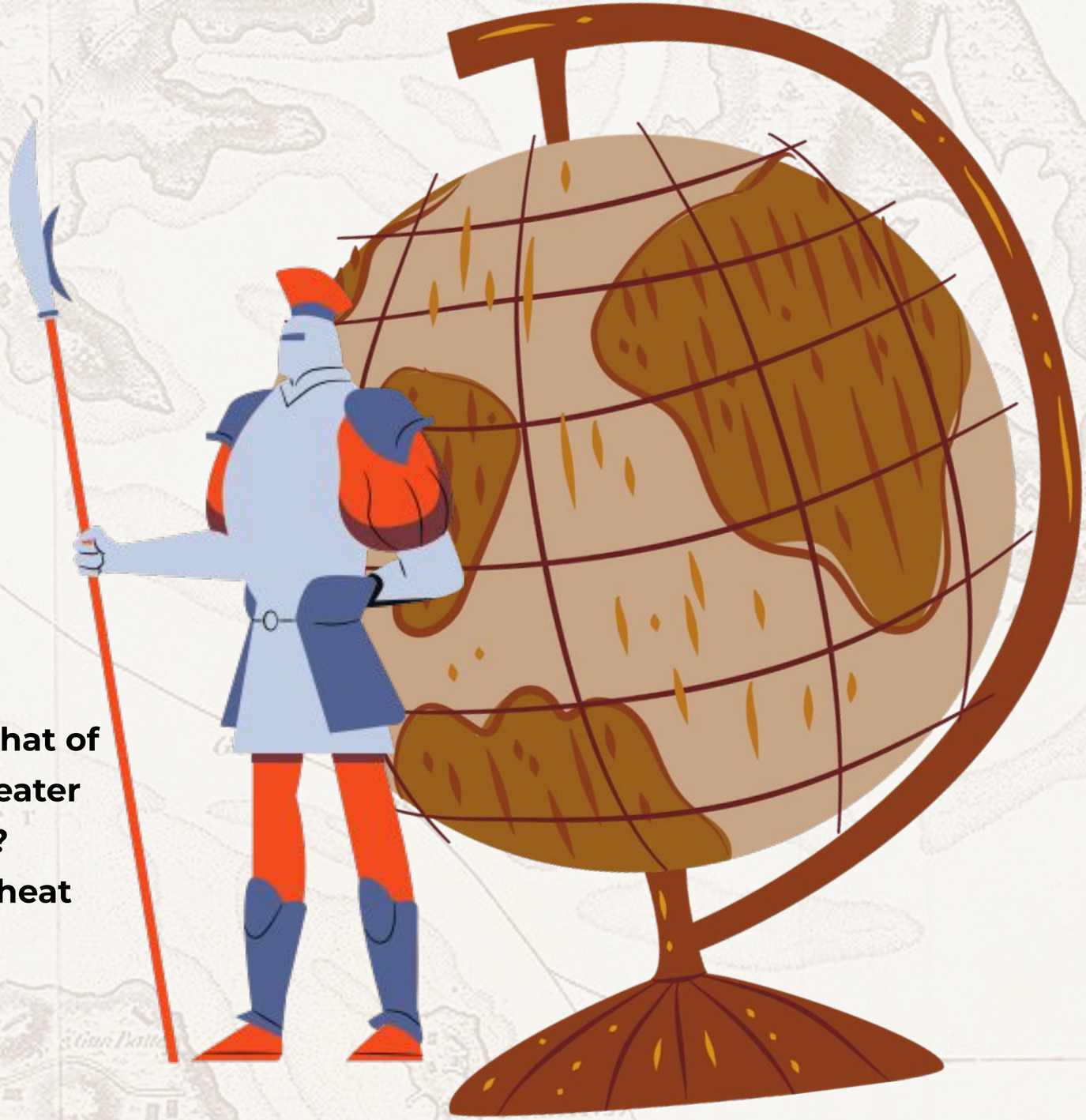


04

SCENARIOS

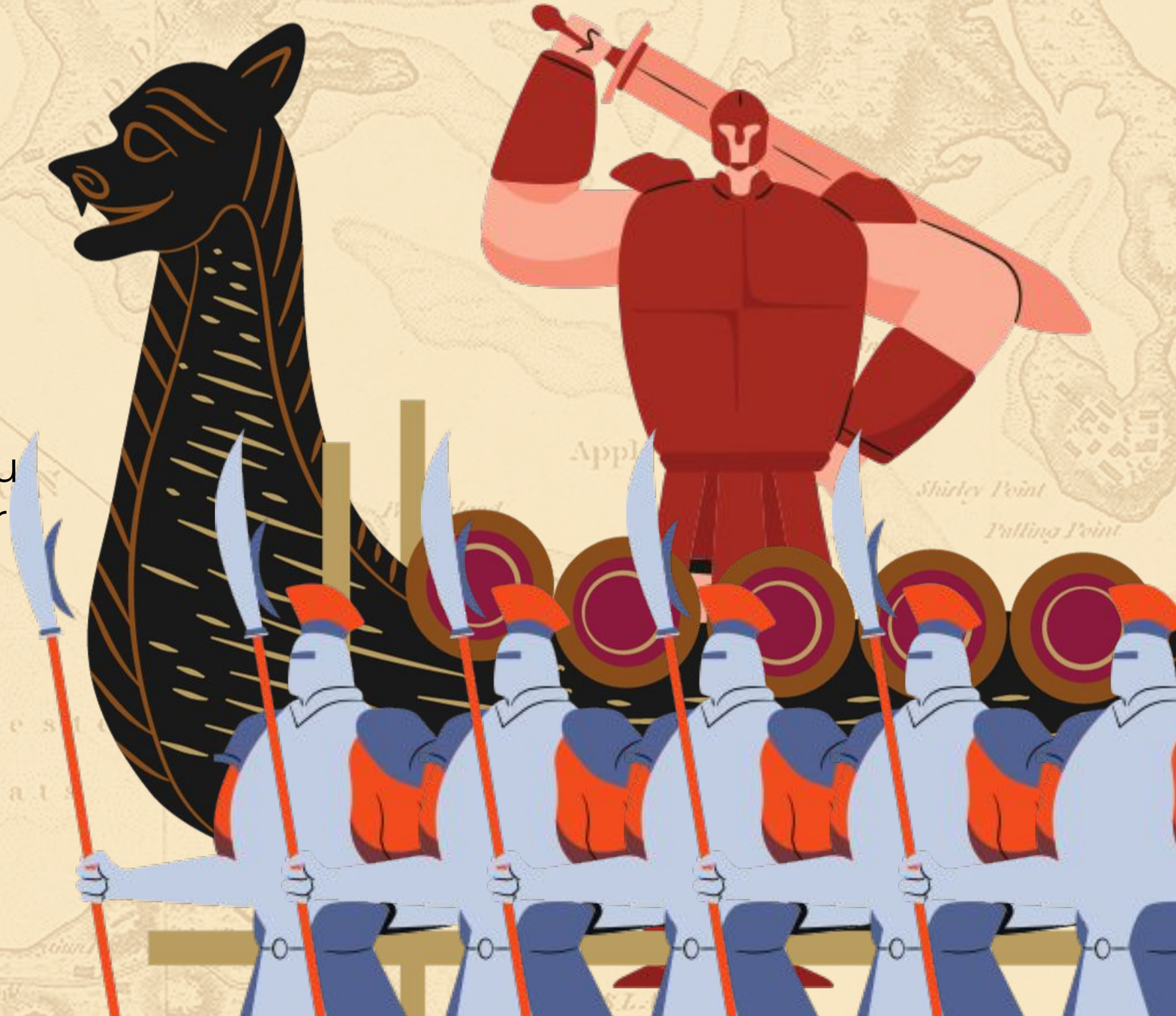
Scenario I

- You are running the cybersecurity department of Narnia
- Your adversary, the nation of Charn, launches a cyber attack that takes out an oil pipeline
- This pipeline supplies 30% of your military's fuel, but also the heating fuel for 70% of your nation
- You know that your military is stronger than that of Charn's, and your cybersecurity prowess is greater
- Do you respond with an attack, or diplomacy?
- Does this answer change if knocking out the heat kills one person? Ten people? A thousand?



SCENARIO 2

- Now, Charn has begun to build up the facilities needed for nuclear weapons
- Your advisors tell you that you can stop this through a cyber attack, but the only possible method will also harm hundreds of millions of other devices
- The conventional option is possible, but will put your country into war
- What do you do, and why?



Scenario 3

- After being defeated, Charn has now begun building a new cyber academy, where you know that many so-called terrorists have been gatherred, who have already launched attacks that resulted in fatalties in the past
- You have 100% reliable intelligence that they are planning an attack aimed to kill thousands
- But, they have learned their lesson and are in a air-gapped environment, immune to cyber methods
- Do you recommend a conventional attack to stop this? Is it ethical? Can it ever be ethical?