Cyber Attack Predictive Index (CAPI)

Becca Badon, Olivia Brown, Hritamber Chakraborty, Michael Hallahan, Christian Helgeson, William Hood, Sebastian Llaca, Alex Osborne, Chris Park

Johns Hopkins University | Whiting School of Engineering | Baltimore, MD
Design Day 2021

JOHNS HOPKINS
WHITING SCHOOL *of* ENGINEERING

Introduction

Cyber attacks by one country against another are a recurring feature of 21st century geopolitics. While earlier visions of "cyber war" have not yet materialized, governments have used cyber attacks to achieve political, economic, and military goals faster, more effectively, and with fewer repercussions than is possible through traditional diplomacy, economic sanctions, or military operations. The use of cyber operations to degrade and disrupt critical infrastructure, send political messages, disrupt economic activities, and shape adversarial national security objectives has led to a new type of conflict among nation-states. As more countries develop cyber capabilities, cyber attacks are likely to become more common in international relations.

https://cyberheatmap.isi.jhu.edu/heat-index

Objectives

The Cyber Attack Predictive Index (CAPI) relies on a 5-part scoring system that seeks to better understand why nation-states engage in cyber conflict and serve as a barometer for predicting future cyber attacks.

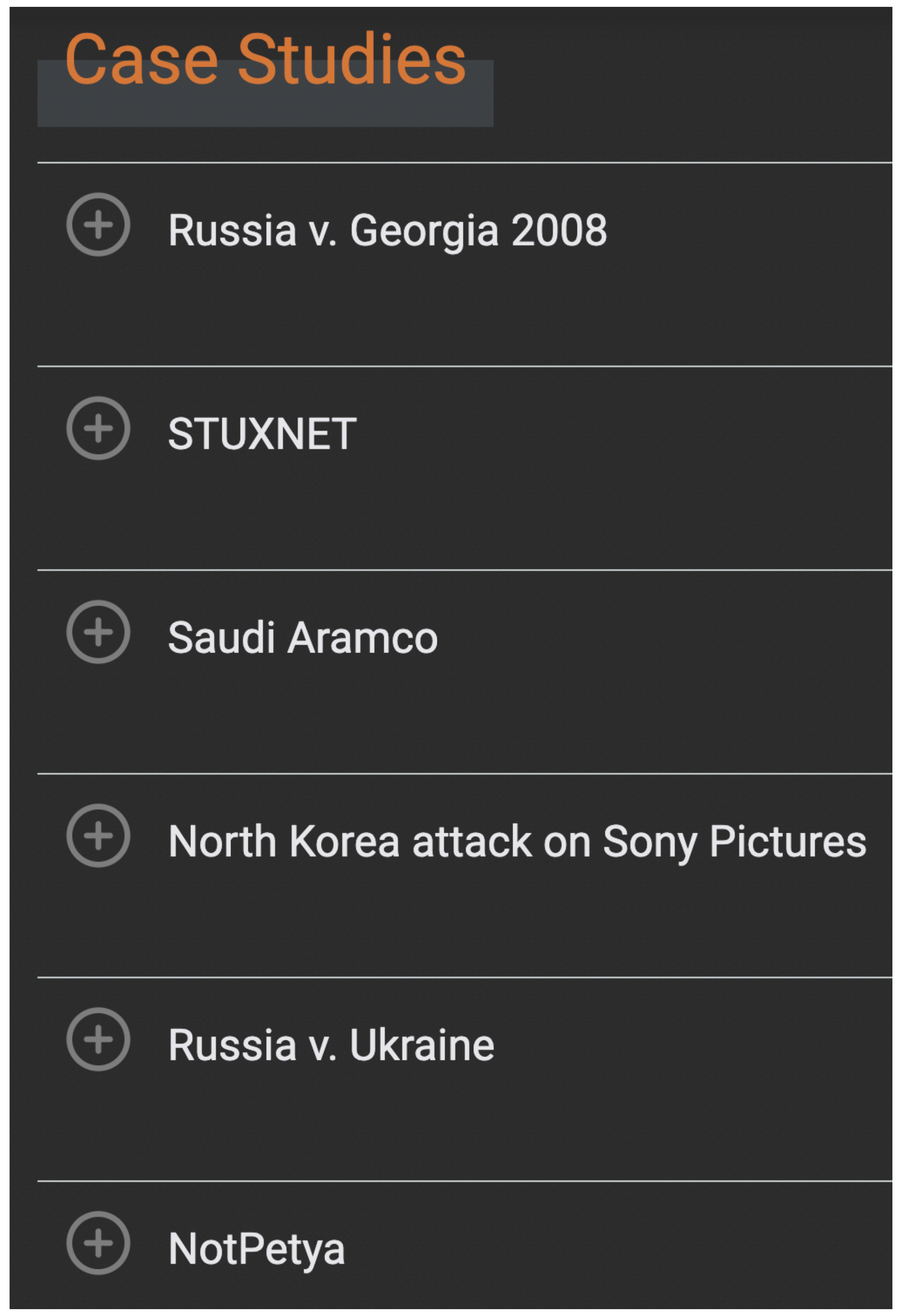
Materials and Methods

After analyzing six well-known cyber attacks that have occurred since 2008, we identified five common factors that contribute to the likelihood of a given nation state choosing to carry out a cyber attack:

1. Possession of a knowledgeable, organized cyber force
2. National motivation
3. Lack of fear of repercussions
4. Consistency with National Security Strategy
5. Technological vulnerability of the target

Based on these five factors, pairs of nation states consisting of an aggressor state (carrying out the cyber attack) and a defender state (the target of the cyber attack) are given scores ranging from 1 to 5 in each of the five areas, for a total score out of 25.

Results



Case Studies

⊕ Russia v. Georgia 2008

⊕ STUXNET

⊕ Saudi Aramco

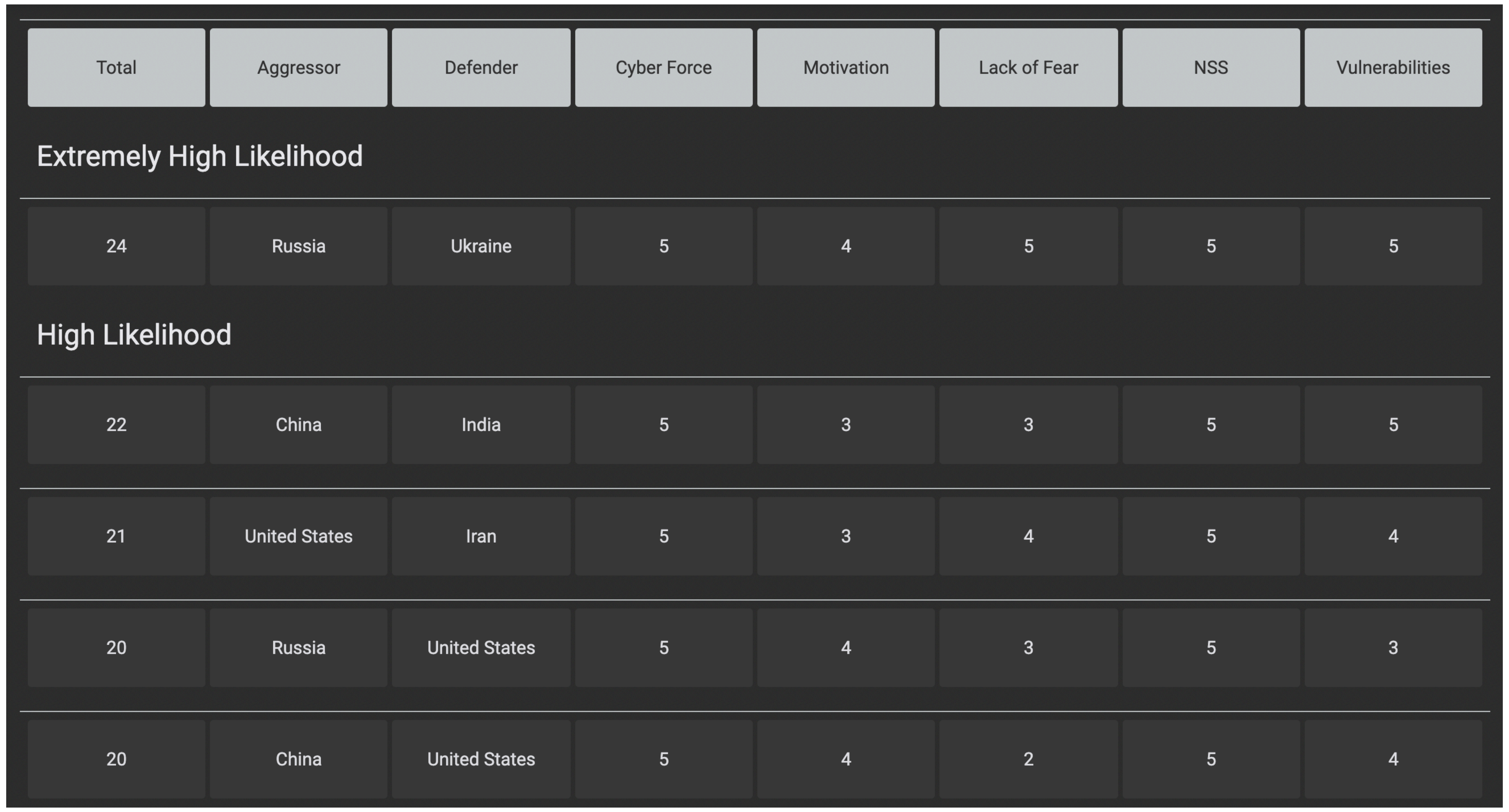
⊕ North Korea attack on Sony Pictures

⊕ Russia v. Ukraine

⊕ NotPetya

Figure 1 - Historical Case Studies

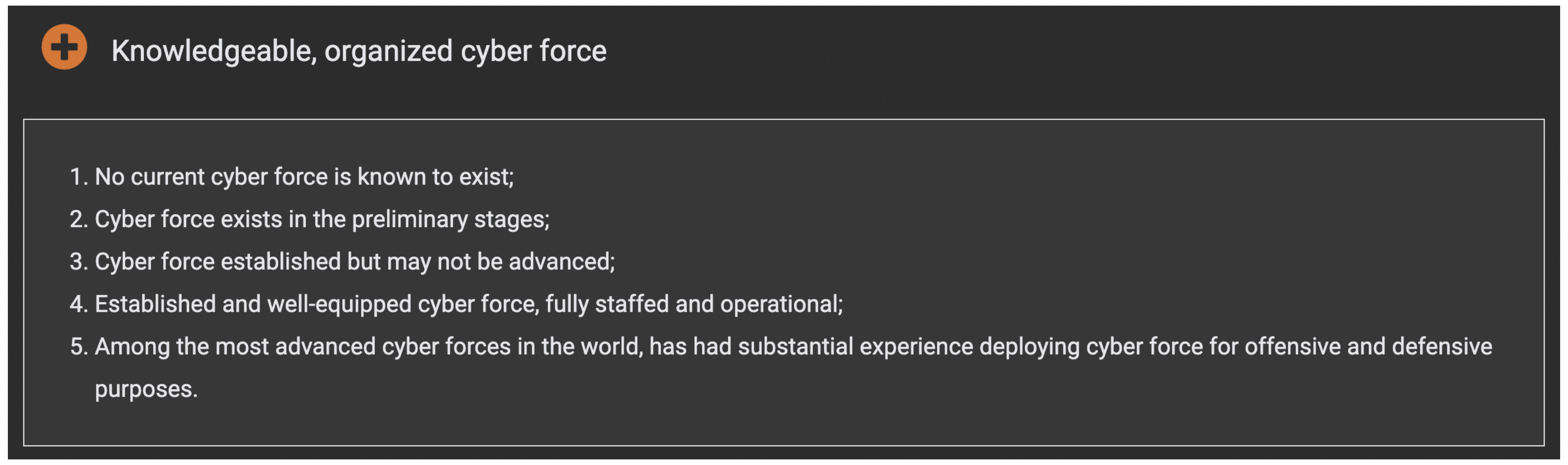
The project previously analyzed six well-known cyber attacks since 2008 that set a precedent or stood out as unique in their intended effects. From these, we were able to identify five common factors that contribute to the likelihood of a cyber attack occurring.



Total	Aggressor	Defender	Cyber Force	Motivation	Lack of Fear	NSS	Vulnerabilities
Extremely High Likelihood							
24	Russia	Ukraine	5	4	5	5	5
High Likelihood							
22	China	India	5	3	3	5	5
21	United States	Iran	5	3	4	5	4
20	Russia	United States	5	4	3	5	3
20	China	United States	5	4	2	5	4

Figure 3 - Cyber Heat Index

Using the 5-factor scoring system, we have built a heat index of aggressor-defender nation state pairs that is updated frequently to reflect the events currently happening in the world. The index is divided into four tiers of likelihood: extremely high likelihood, high likelihood, likely, low likelihood. The index contains pairs ranging from traditional world powers such as China, Russia, and the United States, to smaller, regional powers such as Turkey, Egypt, and Ethiopia. The CAPI advisory board consists of a combination of International Studies and Computer Science students. All members have a regional focus and are actively monitoring political, economic, and security developments in their respective regions.



⊕ Knowledgeable, organized cyber force

1. No current cyber force is known to exist;
2. Cyber force exists in the preliminary stages;
3. Cyber force established but may not be advanced;
4. Established and well-equipped cyber force, fully staffed and operational;
5. Among the most advanced cyber forces in the world, has had substantial experience deploying cyber force for offensive and defensive purposes.

Figure 2 - Scoring

When scoring an aggressor-defender pair, the pair is given a score from 1 to 5 in each of the 5 areas, for a total score out of 25. Each of the 5 areas is further broken down to outline the conditions that must be met to warrant a certain score.

Conclusion

As cybersecurity continues to grow as an important aspect of national security and as cyber attacks become more prominent as offensive measures, it is increasingly important to understand how nation states today understand and prioritize cyber offensive and defensive measures and the implications of these views for international security. It is our hope that the Cyber Attack Predictive Index will continue to be a tool that can be relied upon to understand how the events transpiring in the world today affect the potential for cyber conflict. To see the latest Cyber Heat Index, go to https://cyberheatmap.isi.jhu.edu/heat-index .