New website predicts likelihood of cyber attacks between nations

October 14 2020

Credit: CC0 Public Domain

Where in the world might the next cyberattack between nations take place?

A new online database developed by a team of Johns Hopkins University computer scientists and international studies students predicts that there is an "extremely high likelihood" of a Russian cyberattack on Ukraine.

The second most likely? The United States against Iran.

The Cyber Attack Predictive Index (CAPI) devised by computer science professor Anton Dahbura along with cybersecurity lecturer Terry Thompson and former undergraduate Divya Rangarajan provides a predictive analysis of nations most likely to engage in the surreptitious strategy waged with keyboards, code and destructive malware rather than soldiers, tanks and airplanes.

"The site attempts to anticipate and predict where the next major cyber conflict could break out based on existing data from past attacks," said Dahbura, executive director of the Johns Hopkins Information Security Institute and co-director of the new Johns Hopkins University Institute for Assured Autonomy. "It's a very good approximation of what's hot and what's not."

In 2019 as the rhetoric and record around deploying the malware menace grew more threatening, Dahbura began developing the site with Thompson when he was a lecturer in the Information Security Institute and Rangarajan before she graduated in May. Thompson worked for three decades at the National Security Agency and other federal agencies before moving to the private sector as a vice president at Booz Allen, and teaches graduate courses in global cybersecurity, cyber policy and cybersecurity risk management.

"This is going to be a much more common form of conflict in the future," Dahbura said.

The team devised a methodology for grading nations based on five

common elements identified in all of the national cyberattacks over the past 15 years. Scored on a 1 to 5 scale, they are:

1. The strength and sophistication of the attacker's cyber force (from none to most advanced);
2. The severity of the grievance motivating the attacker against its target (from none to extremely aggrieved);
3. The attacker's lack of fear of serious repercussions (from extreme fear to none);
4. The consistency of an attack with the attacker's national security policy (from no policy to extremely consistent);
5. The degree of technological vulnerabilities within the target (from none to many).

The higher the total score the more likely a nation is to attack. The 12 nation-on-nation scenarios scored on the website range from the very low likelihood of India attacking China to four tied as the third most likely situations: China against the United States, Israel against Iran, Russia against the United States and the United States against Russia.

Dahbura and Thompson have formed a CAPI Advisory Board of project stakeholders that meets regularly to discuss hot-spots around the world that have implications for likely cyber conflict and to update the online CAPI Heat Index.

The website also provides several case studies used to devise the scoring system. The two highest scoring incidents were the cyberattack Russia simultaneously launched with its 2008 invasion of neighboring Georgia, and the STUXNET malware the United States and Israel unleashed on an Iranian nuclear facility.

More information: The project website can be found at

cyberheatmap.isi.jhu.edu/.

Provided by Johns Hopkins University