Created by **Joseph Camuso.**

Background Information

In the past 30 years, the concept of state-backed hacking has gone from science-fiction to a tried and tested method of surrogate warfare. Hacking is the deliberate exploitation of weak points in cybersecurity in order to gain unauthorized access to data. The North Atlantic Treaty Organization (NATO) has recognized cyberspace as a military domain while a 2013 study by the UN Institute for Disarmament Research (UNIDIR) concluded that 40 UN member states had military units focused on cyberwar and 12 UN member states maintained assets capable of waging offensive cyberwar.

"State sponsored hacking" refers to situations in which organizations or individuals are coerced by a government or government body into breaching foreign information communication technologies (ICT's) with the intent of spreading propaganda, stealing data, or causing harm in any form. State sponsored cyberattacks are especially dangerous because of their zero-accountability design and their ability to target military, social, political, and economic infrastructure simultaneously.

Lack of accountability is the hallmark of successful state sponsored ICT attacks. Breaches are carefully timed and coordinated so that accusations against the defendant state can be easily labeled as paranoia on behalf of the claimant state. "False flag" attacks describe cybercrime performed by states or organizations under an assumed identity and are utilized widely to "cover tracks" after a coordinated breach.

State sponsored attacks often take place on a national scale, thus, their impact is difficult to quantify and subsequently, limit. For example, if a state sponsored cyberattack aimed at spreading propaganda on social media platforms is successful in swaying a national election, the effects of the cyberattack were not only the election of the chosen candidate, but

also every decision the elected official makes while in public office. The effects of such an attack are not limited to one business or industry, but can affect the stability of entire states or regions.

Tracing state endorsed cyberattacks is extremely difficult. A common method of determining whether a cyberattack was state sponsored or not is to compare the scale of the attack to the amount of traceable material left behind. For example, if a massive cyberattack, spanning multiple platforms, with clear political or infrastructural targets leaves little traceable material, it is safe to hypothesize the attack was state-sponsored.

UN Involvement

A 2012 report by a group of 15 international cybersecurity experts for UN Secretary-General Ban Ki-Moon, highlighted four topics relevant to the prevention of ICT warfare: cooperation, international law, confidence building measures, and improvement in state built ICT capabilities. The “The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security” report stresses international understanding as a means of combating state sponsored cybercrime and lays out recommendations for supranational guidelines.

In 2013, a report by the United Nations Institute for Disarmament Research (UNIDIR) called “The Cyber Index: International Security Trends and Realities” summarizes the status of cyberarms and defines the responsibilities that key international organizations play in the prevention of cyberwarfare.

In 2001, the UN General Assembly passed the widely recognized cybersecurity resolution 55/63 which brought non-state sponsored cybercrime to the attention of the General Assembly and formed a legal groundwork for future UN action regarding cybersecurity.

Questions to Consider

When drafting and writing your resolutions, please consider the following questions:

- How can the guidelines laid out in the "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" report be applied practically in conjunction with the Universal Declaration on Human Rights and the Geneva Conventions to limit the occurrence of state sponsored hacking?
- What other geopolitical factors influence the prevalence of state sponsored ICT aggression and how can delegates use them to their advantage?
- What is the legality of regulations on cyberwarfare capabilities? Are they enforceable? How can they be created and/or improved?
- Do increased defensive capabilities in cyberspace have the potential to spark a cyberarms race? Should your resolution focus on fortifying defenses, bolstering international goodwill, or enforcing strict sanctions?
- Most assets in cyberspace can be used for both good *and* malicious activity. Can a flood of assets designed for ethical activities be eventually used for unethical activity?
- Can delegates find real life situations of speculated or confirmed cases of state sponsored cyber-aggression and use them to further their resolution and enhance debate?

The more you research **your country's** policy regarding a topic, the more confident you'll be in debate and the more fun you'll have! We are looking forward to seeing the resolutions you form!

Sources

- Report by 15 Cybersecurity Experts (UN) - "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security"

  https://digitallibrary.un.org/record/753055?ln=en

- Report by UNIDIR - "The Cyber Index: International Security Trends and Reality"

  https://www.files.ethz.ch/isn/165142/the-cyber-index-international-security-trends-and-realities-en-463.pdf

- UN General Assembly Resolution 55/63

  https://undocs.org/en/A/RES/55/63

- Report : "Information Warfare and International Law"

  http://www.dodccrp.org/files/Greenberg_Law.pdf

- Report by Smeets and Lin - "Offensive Cyber Capabilities: To what ends?"

  https://ccdcoe.org/uploads/2018/10/Art-03-Offensive-Cyber-Capabilities.-To-What-Ends.pdf

- Article by Detlev Wolter - “UN takes big step forward in cybersecurity”

https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity

- Article by Timothy Summers - “Ethical hacker explains how to track down the bad guys”

  http://theconversation.com/hunting-hackers-an-ethical-hacker-explains-how-to-track-down-the-bad-guys-70927

- Article by the Washington Post - Quick statistics on global internet use

  https://www.washingtonpost.com/news/worldviews/wp/2016/11/22/47-percent-of-the-worlds-population-now-use-the-internet-users-study-says/

  https://www.data.gov/