Harry Radinsky
DISEC: Topic #1 - Cyber Warfare
YUNMUN XXXIV

In the modern world, social media has emerged as a dominant force, with approximately 4.9 billion users as of June 2023. Yet, the proliferation of this powerful tool has not been without its challenges.[1] Social media's ability to swiftly disseminate information has been harnessed to spread fake news, misinformation, and hate speech, with dire consequences in conflict zones. Ongoing and past conflicts have been negatively impacted by the rapid spread of inflammatory content on platforms like Facebook, Twitter, and Instagram. However, it is crucial to recognize that social media can also be a force for good, promoting peace and dialogue among individuals with diverse backgrounds and beliefs.

In this context, we must also consider the dynamic field of cybersecurity, which holds growing importance in the realm of international relations. In the digital age, nations are confronted with an array of threats in cyberspace, including state-sponsored attacks, cybercrime, and hacktivism.

Recent developments in the field of cybersecurity underscore its relevance and urgency. Recent cyberattacks in the Middle East targeting government and news agencies, emergency-alert systems, and even individuals' technology have raised concerns about the need for proactive measures to counter such attacks.[2] Additionally, North Korea's experiments with artificial intelligence in cyber warfare, as reported on October 18, 2023, have significant implications for international security and necessitate a collective response from the international community.[3]

Within the realm of cybersecurity, DISEC can explore several key facets that should guide your research:

- How does one define a cyberattack?

[1] https://www.forbes.com/advisor/business/social-media-statistics/
[2] https://abc7news.com/cybersecurity-cyberwarfare-israel-hamas/13942013/
[3] https://venturebeat.com/ai/north-korea-experiments-with-ai-in-cyber-warfare-us-official/

- Should there be development of international norms and regulations governing state behavior in cyberspace?
- How do we address the challenge of accurately attributing cyberattacks to specific actors or nations in the realm of cybersecurity? What complexities surround the issue of attribution, and what is the role of cyber forensics? Do we see a necessity for international cooperation in investigating cyber incidents?
- Is there interest in exploring the concept of establishing a global cybersecurity framework that outlines best practices for securing critical infrastructure, protecting personal data, and ensuring the integrity of digital communications?
- What strategies can be discussed to navigate the tension between national security and individual privacy in the context of the cybersecurity debate?

I look forward to discussing this pressing issue and having productive dialogue surrounding cybersecurity. Please reach out with questions or comments to hradinsk@mail.yu.edu. As a reminder, your goal as a delegate is to represent the views of your country rather than your own. Additionally, please remember that all writing must be original and that papers will be submitted to Turnitin to detect plagiarism.

Sincerely,
Harry Radinsky
Chair, DISEC