Houston Area Model United Nations

Standard Committee

NATO

Chair | Hamsini Ajjan

Defending NATO Countries from Cyberattacks

Houston Area Model United Nations 48

February 2-3, 2022

Copyright Notice

Note to Delegates

Delegates,

My name is Hamsini Ajjan and I am currently a senior at the University of Texas at Dallas, majoring in healthcare management and minoring in biology, on the pre-med track. I have been with HAMUN ever since my senior year of high school. Phew, it's been a while since I've been with the organization, and have seen it grow from many angles from the delegate, Logistics, and Secretary General position. I'm super excited to be chairing the NATO committee this year. I have previous experience being a director for different committees and really enjoyed writing y'alls background guides!

HAMUN has personally helped me grow and develop into a strong speaker with great research skills. I look forward to seeing each delegate bring a fresh perspective from their country and debate the topics on hand with confidence. Encouraging all delegates to step-out of their comfort zone to propose bold ideas, I am curious to see which delegates will create actionable resolutions and amass cooperative discussion groups. I'm hoping to see everyone have an enjoyable experience and make HAMUN as exciting as always, especially in-person!

Hamsini Ajjan
Chair of NATO
hxa180013@utdallas.edu

Background Information

We live in one of the most technologically advanced societies today, to say at the least. With big tech becoming the buzz of every headline and cloud based data systems empowering individuals and organizations around the world, nations have been able to spread and secure information quickly and efficiently. The flip side of having these intricate data systems are data breaches. With an average data breach for a company costing anywhere around $4.35 million, cybersecurity has become the top priority for all businesses around the world and nations.

National governments hold the data of every single individual in their country, from the most private information, financial secrets, to the most intricate analytics on how a country is performing and their foreign relations, all information that can play a big role in the downfall of a country when placed in the wrong hands. To counteract these issues, nations have integrated a wide variety of new technologies like anti-malware, next-generation firewalls, and artificial intelligence.

The North Atlantic Treaty Organization (NATO) has world leaders from many influential countries supporting its efforts (i.e. United States, United Kingdom, France, Canada with its newest members Finland and Sweden). With a promise to protect

https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en and stand by each other, all the countries in NATO cooperate on defense matters to solve problems, prevent conflict, and create peaceful resolutions to disputes, if necessary undertake crisis management through military powers too. Cyber defense is one of the core tasks of the collective defense commitment, also known as Article 5, within NATO through which they have also established a strong defense system that can adapt to growing threats and defend networks. NATO helped expand the application of international law to cyberspace and signed the Cyber Defence Pledge in 2016 to ensure national resilience is given high priority by countries around the world. Furthermore, establishing programs and policies like the Cyberspace Operations Centre, Comprehensive Defense Policy, and the Technical Arrangement on Cyber Defense have helped NATO take precautionary attempts to stop cyber attacks.

History: Since the 2002 Prague Summit Declaration, cyber attacks were first placed on NATO's agenda. The 2014 Wales Summit Declaration was the first time countries had acknowledged that cyber attacks have the potential of seriously affecting ally countries, which could possibly lead to the invocation of Article 5.

The first time Article 5 was invoked was after the 9/11 terrorist attacks initiated by Afghanistan on the United States. Where NATO had military forces from all the ally countries work together to enter Afghanistan under the Operation Active Endeavor to deter, detect, and resolve any terrorist activity taking place in the nation. To further prevent incidents like 9/11 from reoccurring, NATO created the Defense Against Terrorism Programme of Work (DAT POW) which is currently being used to develop advanced technology, counter-measures, policies, prototypes, etc. to prepare the ally countries with the best security measures in the face of future terrorist or other asymmetric threats as such.

Earlier this year was the first time Article 5 almost got invoked for the purpose of a cyber attack. Albania was faced with a huge cyber strike caused by Iranian hackers in July, which the Prime Minister Edi Rama compared the situation to be like bombing a country. With approximately 95% of the country's national duties utilizing technology and the internet, Albania was forced to shut down all duties across the government. The government was again attacked in September by Iranian hackers which led to the country disabling their border and customs processing systems. While attempts to rob the nation's sensitive government information were unsuccessful, Rama believes future cyber attacks from these hackers are bound to reoccur. While this incident spurred rumors around the idea of invoking Article 5 and utilizing cyber forces from NATO's ally nations to take action on Iran for their wrongdoings, both Rama and NATO were resistant to further pursue those efforts as Albania is a more remote country and the hackers hadn't caused any damage that led to the death of individuals. NATO did however pass a statement condemning the hackers, supporting Albania's defense system, and the US helped sanction Iran's intelligence agency.

More recently, Montenegro has been hit with cyber attacks from hackers believed to be from Russia. The large-scale ransomware (a malware attack where the attacker locks the target's data and files and demands money in return to lock it) attack led to the websites of the ministries of defense, finance, and interior becoming inaccessible. Only through the help of the FBI, Montenegro was able to overcome these cyberattacks. There has also been an increase in cyber attacks seen in countries like Finland and Sweden this year, which are believed to be caused by Russian forces. Russia has constantly been increasing their cyber attacks on Ukraine, and hacker groups in conjunction with Russia have also been attacking countries around the world more often. Ally countries have built cyber defense systems that are capable of overtaking some attacks. However, NATO is pushing for these countries to begin integrating new efforts to integrate intelligence agencies and cooperation among the countries.

Questions

- What are some countries that should be convinced to join/work with NATO to improve their cyber defense systems?
- What efforts can NATO take to build a proper cyber defense system and integrate ally countries to ensure proper security measures are installed to take action against future cyber attacks?

Questions, con't

- Under what circumstances should NATO invoke Article 5 in the cyber defense space?
- With rising Russian hacking efforts, how can NATO best prepare its ally countries from their hacking attacks? Any new allies or negotiations that should take place with Russia or Ukraine to ensure the rising war tensions between these nations do not have a global impact.

References

Albania weighed invoking NATO's article 5 over Iranian cyberattack. POLITICO. (n.d.). Retrieved November 2, 2022, from https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347#:~:text=Albania%20was%20hit%20by%20cyberattacks,Prime%20Minister%20Edi%20Rama%20said.

Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO. CCDCOE. (n.d.). Retrieved November 2, 2022, from https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/

How countries use cybersecurity for defense. University of Miami. (2022, September 21). Retrieved November 2, 2022, from https://digitalskills.miami.edu/cybersecurity/how-countries-are-using-cyber-security-for-defense-2/

Lohrmann, D. (2022, September 4). *NATO countries hit with unprecedented cyber attacks*. GovTech. Retrieved November 2, 2022, from https://www.govtech.com/blogs/lohrmann-on-cybersecurity/nato-countries-hit-with-unprecedented-cyber-attacks

McLaughlin, J., & Inskeep, S. (2022, September 13). *Examining 2 recent cyberattacks against NATO members*. NPR. Retrieved November 2, 2022, from https://www.npr.org/2022/09/13/1122621461/examining-2-recent-cyberattacks-against-nato-members

NATO establishes program to coordinate rapid response to cyberattacks. POLITICO. (n.d.). Retrieved November 2, 2022, from https://www.politico.com/news/2022/06/29/nato-cyberattacks-russia-00043149

Nato. (2022, September 27). *Cyber defence*. NATO. Retrieved November 2, 2022, from https://www.nato.int/cps/en/natohq/topics_78170.htm

Nato. (2022, September 30). *Homepage*. NATO. Retrieved November 2, 2022, from https://www.nato.int/cps/en/natohq/

U.S. Department of Health and Human Services. (n.d.). *The importance of Cyber Technologies in Government*. National Institutes of Health. Retrieved November 2, 2022, from https://nitaac.nih.gov/resources/articles/importance-cyber-technologies-government

What is a cyberattack? IBM. (n.d.). Retrieved November 2, 2022, from https://www.ibm.com/topics/cyber-attack

HAMUN