LAMUN XXXVI
LATIN AMERICAN MODEL OF THE UNITED NATIONS

LATIN AMERICAN MODEL OF THE UNITED NATIONS
LAMUN XXXVI

NORTH ATLANTIC TREATY ORGANIZATION

Topic B Handbook

"Cyber and technological threats to the North Atlantic Organization"

Chairwoman: Sarah Fernández de Lara
sarah.fernandezdelarass@udlap.mx

Vice-Chair: Máximo Serdán
maximo.serdando@udlap.mx

Conference Official: Ana Sofia Garanicova
ana.garanicovads@udlap.mx

LAMUN XXXVI
LATIN AMERICAN MODEL OF THE UNITED NATIONS

Dear members of the North Atlantic Treaty Organization,

Allow me to give you a warm welcome to the thirty-sixth edition of the Latin American Model of the United Nations at Universidad de las Américas Puebla.

First and foremost, I appreciate your willingness to represent a nation in this committee, as defence, security, and crisis-management, through political and military cooperation isn't always an easy task. Be aware that NATO is summoning all members with the purpose of dealing with either of the important situations concerning the North Atlantic Area, in hopes of contributing to its security: the relationship between Serbia and Kosovo, and cyber and technological threats to this alliance.

Hoping that this experience will serve you as a means of reflection and awareness about the problems faced worldwide, we seek to make changes in the world by amending what is needed and looking for ways in which to solve the issues around us. Remember to give your best, as this is an opportunity for you to represent your delegations with honour, to contribute, and replicate a legitimate debate, though most importantly, to grow, make new friends, and acquire new skills; your actions, however big or small they may be, can and will portray change.

I exhort you to test your abilities, attempt what others may find impossible. It is up to you to demonstrate that change is possible, and that it can be achieved with the help of every single one of you; I undoubtedly know that you will be part of the change that LAMUN XXXVI will make. Moreover, remember to respect each other, be tolerant, and embrace your uniqueness; recall that all of you play a key role, your ideas and contributions are and will be valuable before, during, and after this event. On behalf of the NATO Chair, we are really looking forward to seeing you.

Kind regards,
Sarah Fernández de Lara, Chairwoman

The North Atlantic Treaty Organization (NATO), is an intergovernmental political and military alliance between European and North American nations, serving as a transatlantic link between both continents, whose purpose is to guarantee freedom, security, and collective defence amongst its members. It gathers daily to consult and cooperate on defence and security issues to achieve peaceful resolutions and prevent further conflicts; given that it has military power, it is able to undertake crisis-management operations, to maintain national, regional, and international integrity (NATO, 2023).

NATO was formed on 4 April 1949 as a response to World War II's events and the ongoing disputes that were developing during the Cold War. Signing members gathered in Washington, D.C., United States to establish their position and create an alliance which would unite them against military aggression and promote political and economic stability in the North Atlantic area; this became the Washington Treaty (NATO, 2023).

It is important to emphasise that NATO works under a principle of collective defence, which is stipulated in Article 5 of the Treaty, where member nations consider that an attack on any of them is considered an attack against all - and must therefore act collectively to safeguard the integrity of the nation and the alliance. The only time in which this article has been invoked was after the 9/11 attacks in the United States in 2001. In 2022, the Organization established a Strategic Concept, which reaffirms NATO's key tasks as crisis prevention and management, deterrence and defence, and cooperative security (NATO, 2023).

Currently, NATO has the following members: Albania, Belgium, Bulgaria, Canada, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, The Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Türkiye, United Kingdom, and United States (NATO, 2023).

TOPIC B

"Cyber and technological threats to the North Atlantic Organization"

In a constantly developed world, where technology advances rapidly, cybersecurity poses a paramount concern when it becomes threatened by malicious individuals. Cyber and technological threats can vary from low-level disruptions to sophisticated attacks, and having a powerful political and military organisation such as NATO, can make it more susceptible to destructive and coercive threats and attacks. The Alliance needs to protect its tasks of crisis prevention and management, through deterrence and defence, having the responsibility to be prepared to defend its networks and operations, not only for its sake, but for its members' as well (NATO, 2023).

In 2016, members implemented a Cyber Defence Pledge, which was enhanced this year, with the purpose of setting new ambitious goals to strengthen stability and reduce cyberspace attacks. On that matter, it launched a Virtual Cyber Incident Support Capability (VCISC) to respond adequately to malicious cyber activities and promote its deterrence and defence position. Furthermore, NATO collaborates with the European Union, United Nations, and the Organization for Security and Cooperation in Europe (OSCE) to address cyber threats and defence collectively. It is important to mention that Allies in the Treaty exchange information in order to have mutual assistance to prevent, mitigate, and resolve conflicts; most of the times, this information, stored in NATO's databases and systems can be very sensitive, therefore making them vulnerable to malign actors who seek to interfere with NATO's stability and infrastructure; likewise, their intellectual property, government services, and military activities can be interfered with (NATO, 2023).

Evidently, this topic is quite complex given that with the development of new technologies and the enhancement of cyberspace, threats and attacks are more recurrent and even more dangerous. It is also of utter importance to recognise that it is not only individuals or groups who seek to conduct cyber espionage and further attacks, but rather nations. These seek to capture information related to new technologies and strategies the

victim country is producing, more specifically regarding military, aerospace, and government tactics. However, espionage isn't the only way in which cyberspace can be threatened, cyber terrorism can also take place, where terrorist groups recruit highly skilled hackers to attack multiple systems and networks for their own mass disruption purposes (Alexander, 2014).

Hacktivist groups can also be part of these threats, relying on the collective power of individuals to communicate and participate in protests and leak government or corporation documents. Nevertheless, there are also cyber criminals whose purpose is to earn a profit from their crime, compromising systems, security, and even military and law enforcement. The last of some possible ways in which cyber threats can take place, as was aforementioned, is by Nation-States - being Russia and China the most concerning for NATO. Governments of these types of countries develop systems in which they collect political, economic, technological, and security/intelligence information to improve their own offensive and defensive capabilities, while destabilising foreign countries' ones (Alexander, 2014).

Due to all these problematic circumstances, the Alliance introduced cyber defence in its political agenda at the 2002 Prague Summit, at least setting a foundation to act accordingly when these attacks arose. However, NATO has suffered from cyber attacks for the past few years, not just as a whole, but its own members, which has in result led to the strengthening of its measures, specifically towards its communication and information systems. Moreover, if a NATO member is victimised by a cyber attack, then the Organization will coordinate assistance, investigate, and if necessary, carry out missions to resolve the issue (Alexander, 2014).

Despite the vulnerability NATO may suffer from, it has been able to boost its capabilities both militarily and politically, opting to collaborate with other groups or organisations to integrate defensive and offensive cyber measures. Its policy focuses on adapting to cyber security, deterrence, and defence policies through concrete action plans and partnerships, where it hopes to foster innovation, analyse threats and malware

information, and strengthen cooperation on training and exercises. One of NATO's commitments is to act accordingly with international law, ensuring that its members are risk-free while also supporting norms of responsible state behaviour in cyberspace (Davis, 2019).

Guiding Questions

1. Since NATO is highly dependent on its members' national information systems and networks, what can members do to develop a more centralised protection?
2. Why is it important for NATO to collaborate with other institutions, groups, or organisations to battle cyber and technological threats and attacks?
3. Does your delegation's nation have a protocol or measures to follow in case of suffering from a cyber and technological attack?
4. What would be the possible effects and consequences of a successful attack against NATO or its members?
5. What cyber capabilities does NATO and your delegation have to defend against technological threats?
6. What are the most significant technological and cyber threats that NATO is currently facing?
7. How could these attacks undermine security and stability in the North Atlantic region?
8. Who are the main groups or actors carrying out cyberattacks against NATO?

References

1. Alexander, D. C. (2014, October). Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses. DergiPark. Retrieved from https://dergipark.org.tr/tr/download/article-file/89251
2. Davis, S., & NATO Parliamentary Assembly. (2019, October). STC General Report 2019 - NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE. NATO Parliamentary Assembly. https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf
3. NATO. (2023). Declassified: Birth of NATO. NATO.int. https://www.nato.int/cps/en/natohq/declassified_137851.htm
4. NATO. (2023). What is NATO? NATO.int. https://www.nato.int/nato-welcome/
5. North Atlantic Treaty Organization. (2023, September 14). Cyber defence. NATO.int. https://www.nato.int/cps/en/natohq/topics_78170.htm