FerMUN

WRITING A POSITION PAPER (PP)

The position paper (PP) is a one or two-pages document which presents your country's/organization's position regarding the issues debated in your committee. This document serves as a reference for your preparation as well as that of another delegate.

I. PURPOSE OF A POSITION PAPER

It serves:

- **To the delegation** that drafts it in order to know and maintain the position of its country/organization on the different issues**.**
- **To other delegations** who will be able to find out about the countries/organizations present in their committee and contact them in order to make possible alliances with countries with similar positions.
- **To committee chairpersons,** who will use this document to check the correct understanding of the subjects dealt with by the delegates and the respect of their positions during the debates.

Each delegation must draft a PP for each issue debated in the committee.

II. RULES FOR WRITING A POSITION PAPER:

1) Your text, excluding the bibliography, must be a minimum of one page, 2 pages maximum, font "Georgia", size 11.

2) Since this text is a statement from your government and not from your own opinion, you must, under no circumstance, use the first person in your paper. You should use expressions such as «Finland », « our delegation » or «our country».

3) Your document shall not include titles, but you must indicate in the top left corner:
   a) Name of your committee (e.g. **COMMITTEE:** Forum on trade)
   b) Issue that you treat (e.g. **ISSUE:** Fighting the sale of Counterfeit Goods)
   c) Name of the country/organization that you are representing (e.g. **AUTHOR:** Finland)

4) The body of your paper must be structured in 4 paragraphs, all clearly separated by a line break. Within the same paragraph, you can go back to the line when you add an additional idea:
   a) The first paragraph of your document should present the issue in a few words.
   b) The second paragraph includes a general sentence on the position of your country/organization and a development on it (you may quote an

international treaty, agreements that your country has previously supported, or any other international document related to the issue).

c) The third paragraph should detail solutions implemented by your country to solve the issue.

d) The last paragraph should elaborate on the solutions your delegation is suggesting (**2 minimum**).

5) It is unnecessary to have a global conclusion.

6) At the end of your document, insert a **"BIBLIOGRAPHY**" where you will have identified the sources used during your research. You will ensure that you use varied and reliable sources. You may use the map produced by Best Delegate available with this link to do your research. For each country, you will be able to find:
   - A link to your country's ciafactbook
   - Your country's official statements at the United Nations,
   - Links to your government's official website,
   - Links to the website of your country's permanent mission to the United Nations.
   - Historical information about your country by the BBC.

This list is non-exhaustive, and you can of course add handwritten or iconographic sources.

Bellow, you will find an example of PP (page 3, 4, 5 and 6) that will guide you during your writing.

Remember that your chairs and the Deputy Secretary General in charge of delegates can easily be contacted for any additional information.

III. AN EXAMPLE OF POSITION PAPER

COMMITTEE: Security Council
ISSUE: Discussing a framework for international response in mitigating potential conflict escalation in cyberspace.
AUTHOR: Saudi Arabia

Nowadays, the internet, networks, servers are part of our daily lives but although these have facilitated numerous aspects of it, it also has made us individuals and nations more vulnerable. Indeed, nations, just like individuals, have their data stored on networks and servers. With most critical infrastructures of a country depending on the well-functioning and security of these, if a nation decided to hack another one's infrastructures to gather confidential information or simply to shut them down, the entire country could be brought to its knees. Furthermore, due to the relative newness of this technology, a serious lack in laws, norms and sanctions is present, resulting in conflict between nations to escalate quickly. The annual cost of cybercrimes on the global economy is estimated to be around 400 billion US Dollars. Consequently, it is imperative to establish new frameworks, institutions, norms and laws to guarantee safety to all nations and their population.

The Kingdom of Saudi Arabia (KSA/Kingdom) is one of the most developed countries in terms of cyber security, since, "Saudi Arabia's size, wealth, and geopolitical prominence makes it a prime target for cyberattackers" (ARAB NEWS). The Kingdom has, in recent years, drastically invested, in a variety of different domains and sectors, in the creation of new technologies, norms, laws, institutions to protect itself against internal and external threats.

KSA has introduced the National Cybersecurity Authority (NCA), the body responsible for matters regarding cyber security in KSA. Although individual entities remain responsible for their own cyber security, government entities as well as private companies delivering critical national services/infrastructures are required to comply with the NCA's essential cyber security controls.

Regarding financial institutions, KSA understands that the current digital society has high expectations of flawless customer experience, continuous availability of services and effective protection of sensitive data. Information assets and online services are now strategically important to all public and private organizations, as well as to broader society. These services are vital to the creation of a vibrant digital economy. They are also becoming systemically important to the economy and to broader national security. All of which underlines the need to safeguard sensitive data and transactions, and thereby ensure confidence in the overall Saudi Financial Sector. Therefore, Saudi Arabian Monetary Authority (SAMA) has developed and implemented a "Cyber Security Framework".

Additionally, the Kingdom has established an "Anti-Cyber Crime Law" and grid, stating the nature of the cyber crime, the fine and the imprisonment term the culprit(s) are subject to. This law is orientated to more individual-based attacks and assumes the culprit is a single individual or a small group of individuals.

On top of the NCA, the Saudi Arabian government has invested over 487.4 million USD in the creation of intra-government committees, specialized in cyber security and combating cyber crimes. These committees mainly consist of Saudi Information Technology Company (SITCO), Communications and Information Technology Commission (CITC) and Ministry of Interior members.

Moreover, KSA organizes a yearly conference, “The Middle East and North Africa Information Security Conference”, in order to raise awareness and discuss the new technologies which could be adopted to improve cyber security. A large number of international security brands also attend this conference.

Saudi Arabia suggests the creation of an international entity, International Cybersecurity Authority (ICA), a body responsible for matters regarding cyber security throughout the world. In case of an eventual cyber warfare between countries, the ICA would be the body incharge of mitigating the conflict. To do so, this organization would create an “international investigation unit” that would investigate in the event of cyber crimes between countries. The ICA would also introduce a new unit/section to the International Court of Justice, dedicated to determining the nature of the cyber crime(s), and ensure the proper application of the correct sanctions. Besides, the ICA would introduce an “International Anti-CyberCrime Law” listing the different cyber crimes and the sanctions that go along with it. Furthermore, Saudi Arabia proposes that the ICA shall be founded by the nations willing to join the organization and the United Nations.

Finally, the ICA shall propose to its members a “Cyber Security Framework”. Within the members, this one would: help create a common approach for addressing cyber security, help achieve an appropriate maturity level of cyber security controls, and help ensure cyber security risks are properly managed. The framework shall be based on the ICA requirements and standards. This one would also be a general framework to prevent any “deep” standardization that could result in weakening the cyber security of the members; general obligations shall be imposed, leaving the country free to decide which potentially confidential technologies/infrastructures this one decides to use to meet these expectations. Any nation joining the entity - member - shall be guaranteed, in case of a cyber attack, a fair trial, assistance (if needed) and compensations, if recognized as victim of the attack and if this one had correctly applied the “Cyber Security Framework” at the time of the attack.

BIBLIOGRAPHY:

- https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/

- https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-saudi-arabia/view
  --- Saudi Arabia CSS

- https://www.enisa.europa.eu/topics/national-cyber-security-strategies

--- record of CSS of European countries

- https://www.wipo.int/edocs/lexdocs/laws/en/sa/sa047en.pdf
  --- Saudi Arabia Anti-Cyber Crime Law

- https://www.congress.gov/bill/114th-congress/senate-bill/754
  --- USA Congress Improve cybersecurity

- http://theconversation.com/hunting-hackers-an-ethical-hacker-explains-how-to-track-down-the-bad-guys-70927
  --- How hackers are traced ?
- https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799
  --- IDS (Intrusion Detection Systems)

-

  https://www.researchgate.net/publication/309040131_Cyber_Crime_in_Kingdom_of_Saudi_Arabia_The_Threat_Today_and_the_Expected_Future

- https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf
  --- Estimated economic impact of cybercrime

- http://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf
  --- Saudi Arabia's cybersecurity Framework

- https://www.simmons-simmons.com/publications/ck0az2ekrns6h0b33e903ntvf/120219-cybersecurity-in-the-kingdom-of-saudi-arabia
  --- NCA
- https://uh-ir.tdl.org/bitstream/handle/10657/3107/ALABDULATIF-THESIS-2018.pdf?sequence=1&isAllowed=y

- https://www.export.gov/article?id=Saudi-Arabia-information-communications-technology