FerMUN

ECRIRE UN TEXTE DE POLITIQUE GENERALE (TPG)

Le texte de politique générale (TPG) est un document d'une ou deux pages qui présente la position de votre pays/organisation concernant les problématiques débattues au sein du comité. Ce document fait office de référence pour votre préparation mais aussi pour celle des autres délégués.

I. ROLE DU TPG :

Il sert :

- **A la délégation qui le rédige** afin de connaitre et maintenir la position de son pays/organisation sur les différentes problématiques.
- **Aux autres délégations** qui pourront s'informer sur les pays/organisations présentes dans leur comité et contacter ces-dernier-ère-s afin d'effectuer des éventuelles alliances avec les pays ayant des positions semblables.
- **Aux présidents de comités** qui vérifieront par le biais de ce document la correcte compréhension des sujets traités par les délégués ainsi que le respect de leurs positions durant les débats.

Chaque délégation doit rédiger un TPG pour chacune des problématiques débattues au sein du comité.

II. REGLES DE REDACTION DU TPG :

1) Votre texte, bibliographie exclue, doit être d'une page minimum, 2 pages maximum police « Georgia », taille 11.

2) Vous ne devez en aucun cas utiliser la première personne du singulier dans votre texte. Vous devez utiliser des expressions telles que « La Finlande », « notre délégation » ou « notre pays » puisque ce texte est une déclaration de votre gouvernement et non pas de votre propre opinion.

3) Votre document ne doit pas comporter de titres mais vous devez indiquer en haut à gauche :
   a) Nom de votre comité (ex : **COMITE** : Forum sur le commerce)
   b) Problématique que vous traitez (ex : **PROBLEMATIQUE :** Combattre la vente de marchandise contrefaites)
   c) Nom du pays/ de l'organisation que vous représentez (ex : **AUTEUR** : Finlande).

4) Le corps de votre texte doit être structuré en 4 paragraphes, tous séparés clairement par un saut de ligne. Au sein d'un même paragraphe, vous pouvez faire un retour à la ligne lorsque vous ajoutez une idée supplémentaire :

a) Le premier paragraphe de votre document doit rapidement présenter la problématique.
b) Le second paragraphe comporte une phrase générale sur la position de votre pays/organisation ainsi qu'un développement sur cette-dernière (vous pouvez notamment citer un traité international, des accords que votre pays a déjà soutenus ou tout autre document international en lien avec la problématique),
c) Le troisième paragraphe contient un développement sur les solutions que votre délégation a déjà mis en place en lien avec la problématique.
d) Le dernier paragraphe sera une présentation des solutions que vous proposerez (**2 au minimum**) en lien avec la problématique.

5) Il est inutile d'avoir une conclusion globale

6) Insérer une « **BIBLIOGRAPHIE** » à la fin de votre document où vous aurez relevé vos sources au fur et à mesure de vos recherches. Vous veillerez à utiliser des sources variées et fiables. Vous pouvez notamment vous appuyez sur la carte réalisée par Best Delegate disponible avec ce lien pour effectuer vos recherches. Vous y trouverez notamment pour chaque pays :
   - Le lien ciafactbook,
   - Les déclarations officielles de votre pays aux Nations Unies,
   - Les liens vers les sites officiels de votre gouvernement,
   - Les liens vers le site de la mission permanente de votre pays aux Nations Unies,
   - Les informations historiques concernant votre pays par la BBC.

Cette liste n'est pas exhaustive et vous pouvez bien évidemment y ajouter des sources manuscrites ou iconographiques.

Vous trouverez en annexe un exemple de TPG (page 3, 4, 5 et 6) qui vous guidera pour votre rédaction.

N'oubliez pas que vos présidents de comités ainsi que le Secrétaire général adjoint chargé de la formation des délégués peuvent facilement être contactés pour tout autre question ou information !

FerMUN

III. UN EXEMPLE DE TEXTE DE POLITIQUE GENERALE :

COMITÉ : Conseil de Sécurité
PROBLÉMATIQUE : Discuter d'un cadre d'intervention internationale pour atténuer l'escalade potentielle des conflits dans le cyberespace
AUTEUR : Arabie Saoudite

Aujourd'hui, Internet, les réseaux, les serveurs font partie de notre vie quotidienne, mais bien qu'ils en aient facilité de nombreux aspects, ils nous ont aussi rendus plus vulnérables, en tant qu'individus et en tant que nations. En effet, les nations, tout comme les individus, ont leurs données stockées sur des réseaux et des serveurs. La plupart des infrastructures essentielles d'un pays dépendent du bon fonctionnement et de la sécurité de ceux-ci. Si une nation décidait de pirater les infrastructures d'une autre pour recueillir des informations confidentielles ou simplement pour les faire arrêter, le pays tout entier pourrait être mis à genoux. En outre, en raison de la relative nouveauté de cette technologie, il existe un grave manque de lois, de normes et de sanctions, ce qui entraîne une escalade rapide des conflits entre les nations. Le coût annuel des cyber crimes sur l'économie mondiale est estimé à environ 400 milliards de dollars US. Par conséquent, il est impératif d'établir de nouveaux cadres, institutions, normes et lois pour garantir la sécurité de toutes les nations et de leur population.

Le Royaume d'Arabie saoudite (RAS/Royaume) est l'un des pays les plus développés en termes de cyber-sécurité, car "la taille, la richesse et l'importance géopolitique de l'Arabie saoudite en font une cible privilégiée pour les hackers" (ARAB NEWS). Le Royaume a, ces dernières années, investi de manière drastique, dans différents domaines et secteurs, dans la création de nouvelles technologies, normes, lois, institutions pour se protéger contre les menaces internes et externes.

Le RAS a créé l'Autorité national de la cyber sécurité (ANCC), l'organisme responsable des questions de cybersécurité au sein du RAS. Bien que les entités individuelles restent responsables de leur propre cybersécurité, les entités gouvernementales ainsi que les entreprises privées fournissant des services/infrastructures nationaux essentiels sont tenues de se conformer aux contrôles de l'ANCC en matière de cyber sécurité.

En ce qui concerne les institutions financières, l'ANCC comprend que la société numérique actuelle a des attentes élevées en matière d'expérience client sans faille, de disponibilité continue des services et de protection efficace des données sensibles. Les actifs d'information et les services en ligne sont désormais importants pour toutes les organisations publiques et privées, ainsi que pour la société en général. Ces services sont essentiels à la création d'une économie numérique dynamique. Ils sont devenus essentiels pour l'économie et pour la sécurité nationale au sens large. Tout cela souligne la nécessité de protéger les données et les transactions sensibles, et donc de garantir la confiance dans l'ensemble du secteur financier saoudien. C'est pourquoi l'Autorité monétaire d'Arabie Saoudite (AMAS) a élaboré et mis en œuvre un "cadre de sécurité cybernétique".

Par ailleurs, le Royaume a établi une "loi sur la lutte contre la cybercriminalité" et une grille indiquant la nature de la cybercriminalité, l'amende et la peine d'emprisonnement à laquelle le ou les coupables sont soumis. Cette loi est orientée vers des attaques plus individuelles et suppose que le coupable est un seul individu ou un petit groupe d'individus.

En plus de la NCA, le gouvernement saoudien a investi plus de 487,4 millions de dollars dans la création de comités au sein des gouvernements, spécialisés dans la cybersécurité et la lutte contre la cybercriminalité. Ces comités sont principalement composés de membres de la Société saoudienne des technologies de l'information (SSTI), de la Commission des communications et des technologies de l'information (CCTI) et du ministère de l'intérieur.

En outre, le RAS organise une conférence annuelle, " La conférence sur la sécurité de l'information au Moyen-Orient et en Afrique du Nord ", afin de sensibiliser et de discuter des nouvelles technologies qui pourraient être adoptées pour améliorer la cyber sécurité. Un grand nombre de marques internationales de sécurité participent également à cette conférence.

L'Arabie saoudite suggère la création d'une entité internationale, l'Autorité internationale de CyberSécurité (AICS), un organisme responsable des questions de cybersécurité dans le monde entier. En cas d'une éventuelle guerre cybernétique entre pays, l'AICS serait l'organe chargé d'atténuer le conflit. Pour ce faire, cet organisme créerait une "unité d'enquête internationale" qui enquêterait en cas de cyber-crimes entre pays. L'AICS mettrait également en place une nouvelle unité/section à la Cour internationale de justice, chargée de déterminer la nature du ou des cyber-crimes et de veiller à la bonne application des sanctions appropriées. En outre, l'AICS introduirait une "loi internationale contre la cybercriminalité" énumérant les différents délits informatiques et les sanctions qui s'y rattachent. En outre, l'Arabie saoudite propose que l'AICS soit fondée par les nations désireuses d'adhérer à l'organisation et aux Nations unies.

Enfin, l'AICS proposera à ses membres un "cadre de sécurité cybernétique". Ce cadre permettrait de créer une approche commune de la cybersécurité, d'atteindre un niveau de maturité approprié pour les contrôles de cyber sécurité et de garantir que les risques de cyber sécurité sont correctement gérés. Le cadre sera basé sur les exigences et les normes de l'AICS. Il s'agirait également d'un cadre général visant à empêcher toute normalisation "profonde" qui pourrait affaiblir la cyber sécurité des membres ; des obligations générales seront imposées, laissant le pays libre de décider quelles technologies/infrastructures potentiellement confidentielles il décide d'utiliser pour répondre à ces attentes. Tout pays rejoignant l'entité - membre - se verra garantir, en cas de cyberattaque, un procès équitable, une assistance (si nécessaire) et des compensations, s'il est reconnu comme victime de l'attaque et si celui-ci a correctement appliqué le "Cadre de sécurité cybernétique" au moment de l'attaque.

BIBLIOGRAPHIE :

- 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

--- SCS (stratégie de Cybersécurité) de l'Arabie Saoudite

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

--- bilan de la SCS des pays européens

- https://www.wipo.int/edocs/lexdocs/laws/en/sa/sa047en.pdf

--- Loi anti cyber-crime Arabie Saoudite

- https://www.congress.gov/bill/114th-congress/senate-bill/754

--- Le congrès américain améliore sa cybersécurité

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

--- Comment les hackers sont tracés ?

- https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799

--- SDI (Systèmes de détection d'intrusion)

- 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

--- Estimation de l'impact économique de la cybercriminalité

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

--- Le cadre de cybersécurité de l'Arabie saoudite

- https://www.simmons-simmons.com/publications/ck0az2ekrns6h0b33e9o3ntvf/120219-cybersecurity-in-the-kingdom-of-saudi-arabia

---ANCC

- 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