Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Seul le texte prononcé fait foi
Check against delivery

Conseil de sécurité
Débat ouvert : Cybersécurité

New York, le 20 juin 2024
Déclaration prononcée par la Suisse

Monsieur le Président,

Je remercie la République de Corée d'avoir organisé ce débat important sur les défis de la cybersecurité. Je remercie également le Secrétaire général, la professeure Nnenna Ifeanyi-Ajufo, et M. Stéphane Duguin, Directeur du CyberPeace Institute à Genève, pour leurs contributions.

La Suisse observe deux évolutions déterminantes dans le cyberespace qui nous préoccupent. D'une part, la numérisation accrue des conflits et le recours à des opérations cyber pendant les conflits armés sont en train de transformer la nature de ceux-ci. D'autre part, l'intensité croissante des attaques par des logiciels de rançon et des cyberattaques parrainées par des États contre des infrastructures critiques est une préoccupation majeure pour la Suisse. L'utilisation de rançongiciels pour extorquer de devises et cryptomonnaies ou encore le ciblage d'infrastructures critiques menacent de paralyser des structures clés de nos sociétés. Ces activités affectent également la capacité de la communauté internationale à atteindre les objectifs du développement durable à cause de la vulnérabilité accrue des Etats en voie de développement. Elles peuvent poser une menace pour la paix et la sécurité internationales et relèvent donc de la compétence de ce Conseil.

La note conceptuelle proposée par la République de Corée s'interroge sur le rôle que peut avoir le Conseil par rapport aux menaces qui découlent des activités malveillantes dans le cyberespace. Permettez-moi d'esquisser quelques options à cet égard.

Premièrement, le Conseil devrait régulièrement prendre note des évolutions et des menaces actuelles en termes de cybersécurité. Étant donné les implications multidimensionnelles et la portée géographique de la question, il serait opportun pour le Conseil de tenir une séance d'information régulière. Lors de cette session, des présentations pourraient être faites par des représentantes et représentants des entités onusiennes, du secteur privé, de la société civile et du monde académique, ainsi que d'autres entités concernées. Cette sensibilisation lui permettrait de prendre des décisions en toute connaissance de cause, notamment sur des dossiers géographiques spécifiques et dans le cadre des opérations de maintien de la paix.

Deuxièmement, le Conseil devrait réaffirmer certains principes reconnus. Nous attachons une importance toute particulière à l'applicabilité du droit international dans le cyberespace, et notamment du droit international humanitaire aux activités dans l'espace cybernétique dans le cadre de conflits armés. Le Conseil devrait également souligner l'importance de la responsa-

bilité des États et de leur devoir de précaution ainsi que reconnaitre les onze normes de comportement responsable des États dans le cyberespace. Ces éléments, complétés par des mesures de confiance et de renforcement des capacités, constituent le cadre pour un comportement responsable des États dans l'utilisation des Technologies de l'information et de la communication (TIC), qui a été adopté par consensus par l'ensemble des États membres des Nations unies. Nous soutiendrions un produit du Conseil qui affirmerait ce cadre et contribueraient ainsi au rétablissement de la confiance.

Finalement, l'activité du Conseil doit être complémentaire aux activités d'autres organes. Il ne s'agit pas pour le Conseil de développer de règles de comportement ou accords. Ceci est l'apanage de l'Assemblée générale et des processus d'experts qu'elle a mandatés. Le Conseil devrait focaliser son attention à développer sa compréhension des risques et à les atténuer, y compris dans des cas de figure concrets.

Monsieur le Président,

L'utilisation responsable du cyberespace présente de vastes opportunités pour relever les défis de demain, malgré les risques reconnus. Dans son Nouvel agenda pour la paix, le Secrétaire général nous encourage à trouver de nouveaux moyens de nous prémunir contre ces nouvelles menaces. Si les négociations du Pacte pour l'avenir nous offrent la possibilité de développer une compréhension commune à cet égard, le Conseil a également un rôle clé à jouer. Le débat de ce jour le confirme.

Je vous remercie.

Unofficial translation

Mr President,

I would like to thank the Republic of Korea for organizing this important debate on the challenges of cybersecurity. I would also like to thank the Secretary-General, Professor Nnenna Ifeanyi-Ajufo, and Mr. Stéphane Duguin, CEO of the CyberPeace Institute in Geneva, for their contributions.

Switzerland is witnessing two decisive developments in cyberspace that are of concern to us. On the one hand, the increasing digitization of conflicts and the use of cyber operations in armed conflicts are transforming the nature of these conflicts. On the other, the growing intensity of ransomware and state-sponsored cyberattacks against critical infrastructure is a major concern for Switzerland. The use of ransomware to extort currency and cryptocurrencies, or the targeting of critical infrastructures, threatens to paralyze key structures in our societies. These activities also affect the international community's ability to achieve the Sustainable Development Goals, due to the heightened vulnerability of developing countries. They can pose a threat to international peace and security, and therefore fall within the mandate of this Council.

The concept note proposed by the Republic of Korea asks what role the Council can play in addressing threats arising from malicious activities in cyberspace. Let me outline some options in this regard.

First, the Council should regularly take note of current cybersecurity developments and threats. Given the multidimensional implications and geographical scope of the issue, it would be appropriate for the Council to hold a regular briefing. The briefing could include presentations by representatives of UN entities, the private sector, civil society and academia, as well as other relevant entities. This awareness-raising would enable the Council to make fully informed decisions, particularly on specific geographical issues and in the context of peacekeeping operations.

Second, the Council should reaffirm certain established principles. We attach particular importance to the applicability of international law in cyberspace, and in particular international humanitarian law, to activities in cyberspace in the context of armed conflict. The Council should also emphasize the importance of State responsibility and due diligence, and recognize the eleven norms of responsible State behavior in cyberspace. These elements, complemented by confidence-building and capacity-building measures, constitute the framework for responsible state behavior in the use of ICTs that has been adopted by consensus by all UN Member States. We would support a Council product that affirms this framework and thus contributes to rebuilding trust.

Finally, the Council's activities must be complementary to those of other bodies. It is not for the Council to develop rules of behavior or agreements. This is the prerogative of the General Assembly and the expert processes it has mandated. The Council should focus its attention on developing its understanding of risks and their mitigation, including in specific cases.

Mr. President,

The responsible use of cyberspace offers enormous opportunities to meet tomorrow's challenges, despite the recognized risks. In his New Agenda for Peace, the Secretary-General encourages us to find new ways to protect ourselves from these new threats. While the negotiations on the Pact for the Future provide us with an opportunity to develop a common understanding in this regard, the Council also has a key role to play. Today's debate confirms this.

I thank you.