Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Conseil de sécurité
Arria-formula: Evolving Cyber Threat Landscape and its Implications for the Maintenance of International Peace and Security

New York, le 4 avril 2024

Déclaration prononcée par la Suisse
Adrian Hauri, Représentant permanent adjoint de la Suisse

Madame la Présidente,

Je remercie la République de Corée d'avoir organisé ce débat important. Je remercie également les intervenants, M. Adedeji Ebo, M. Robin Geiss, et Mme Valeria Kennedy, du Chainalysis Inc., de leurs contributions détaillées. Les diplomates dans cette salle ont beaucoup à apprendre de vous.

Ces dernières années, le cyberespace a connu des évolutions inquiétantes. Nous avons déjà discuté des défis de la cybersécurité au sein de ce Conseil en mai dernier. Il est important d'aborder également la dimension spécifique que viennent de décrire les intervenants, dans laquelle des États menacent la paix et la sécurité internationales en recourant à des moyens cybercriminels. Cette menace nous touche à de multiples égards. De l'argent comme des cryptomonnaies et des données sont volées ou extorquées, des infrastructures critiques, telles que l'approvisionnement en énergie ou le système de santé, sont paralysées. Cette menace nous touche aussi lorsque les fonds ainsi obtenus sont utilisés à des fins qui violent le droit international et les résolutions de ce Conseil.

Le droit international s'applique dans le cyberespace. Il s'applique à tous les États et inclut également les obligations de diligence existantes. Celles-ci exigent notamment que les États prennent des mesures raisonnables et nécessaires pour empêcher les activités d'acteurs non-étatiques sur leur territoire qui violent les droits d'autres États.

Il est également évident que les mesures de sanctions décidées par ce Conseil doivent être pleinement appliquées, dans tous les domaines, y compris dans le cyberespace.

En tant que communauté internationale, nous ne sommes pas impuissants face à ces agissements malveillants. Le Groupe d'action financière sur le blanchiment de capitaux (GAFI) a édicté des standards internationaux pour lutter contre le blanchiment d'argent et le financement du terrorisme et de la prolifération. Il appartient aux États de mettre en œuvre ces recommandations. Mais dans un domaine aussi interconnecté que le cyberespace, le secteur privé a également un rôle préventif important à jouer. Le Geneva Manual - géré par la DiploFoundation - donne des indications sur la manière dont les normes de comportement responsable dans le cyberespace peuvent être mises en œuvre par des acteurs non gouvernementaux.

La mise en œuvre du « cadre des Nations unies pour un comportement responsable des États dans le cyberespace » est un élément clé pour identifier les menaces existantes et émergentes pour la paix et la sécurité et pour relever ces défis. Je tiens aussi à souligner l'importance du travail du *« Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications »* et le développement du *« Programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale »* qui ouvrira la voie pour des actions futures dans ce domaine. Le Conseil de sécurité – et cela a été mentionné - a également un rôle à jouer. Il peut envoyer un message fort en promouvant le respect du droit international et le Cadre sur le comportement responsable des États dans le cyberespace et en tenant

compte dans son travail - par exemple en ce qui concerne les sanctions - des réalités et des dangers du cyberespace. Le groupe d'experts du comité 1718 sur la RPDC est un bon exemple de la manière dont des informations importantes peuvent être collectées et analysées sur les activités malveillantes dans le cyberespace en violation des sanctions.

Il est donc d'autant plus regrettable que son mandat n'ait pas été prolongé la semaine dernière en raison d'un veto.

Madame la Présidente,

Malgré les risques, les nouvelles technologies et le cyberespace représentent également des opportunités pour relever les défis de demain. Dans son Nouvel agenda pour la paix, le Secrétaire général nous encourage à trouver de nouveaux moyens de nous prémunir contre ces nouvelles menaces. Par ailleurs, les négociations du Pacte pour l'avenir nous offrent la possibilité de développer une compréhension commune, notamment en matière de cybersécurité, de renforcer la confiance et de progresser vers une paix durable.

Je vous remercie.

Unofficial translation

Madam President,

I would like to thank the Republic of Korea for organizing this important debate. I would also like to thank the speakers, Mr Adedeji Ebo, Mr Robin Geiss, and Ms Valeria Kennedy, from Chainalysis Inc, for their detailed contributions. The diplomats in this room have a lot to learn from you.

Recent years have seen some worrying developments in cyberspace. We have already discussed the challenges of cybersecurity within this Council last May. It is also important to address the specific dimension that the speakers have just described, in which states threaten international peace and security by resorting to means of cybercriminals. This threat affects us in many ways. Money, such as cryptocurrencies, and data are stolen or extorted, and critical infrastructures such as energy supplies and healthcare systems are paralyzed. This threat also affects us when funds obtained in this way are used for purposes that violate international law and the resolutions of this Council.

International law applies in cyberspace. It applies to all States and also includes existing obligations of due diligence. These require states to take reasonable and necessary measures to prevent the activities of non-state actors on their territory that violate the rights of other States.

It is also clear that the sanctions measures decided by this Council must be fully implemented in all areas, including cyberspace.

As an international community, we are not powerless in the face of this malicious behavior. The Financial Action Task Force on Money Laundering (FATF) has set international standards to combat money laundering and the financing of terrorism and proliferation. It is up to governments to implement these recommendations. But in an area as interconnected as cyberspace, the private sector also has an important preventive role to play. The Geneva Manual - managed by the DiploFoundation - provides guidance on how standards of responsible behavior in cyberspace can be implemented by non-state actors.

The implementation of the "UN norms of responsible State behavior in cyberspace" is a key element in identifying and addressing existing and emerging threats to peace and security. I would also like to emphasize the importance of the work of the "Open-ended Working Group on Developments in the Field of Information and Telecommunications" and the development of the "Programme of Action to advance responsible State behavior in the use of ICTs in the context of international security ", which will pave the way for future action in this area. The Security Council – and this was mentioned - also has a role to play. It can send out a strong signal by promoting respect for international law and the norms of responsible State behavior in cyberspace, and by taking account of the realities and threats in cyberspace in its work - for example with regard to sanctions. The 1718 Committee's panel of experts

on DPRK is a good example of how important information can be gathered and analyzed on malicious activities in cyberspace in violation of sanctions. It is therefore all the more regrettable that its mandate was not extended last week because of a veto.

Madam President,

Despite the risks, new technologies and cyberspace also represent opportunities to meet the challenges of tomorrow. In his New Agenda for Peace, the Secretary-General encourages us to find new ways of protecting ourselves against these new threats. In addition, the negotiations on the Pact for the Future offer us the opportunity to develop a common understanding, notably in the area of cybersecurity, to strengthen trust and to make progress towards a lasting peace.

I thank you.