Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Conseil de sécurité

Briefing: Threats Posed by Ransomware Attacks Against Hospitals and Other Healthcare Facilities and Services

New York, le 8 novembre 2024

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

Monsieur le président,

Je remercie le Dr. Tedros, Directeur-général de l'OMS ainsi que Monsieur Conrad de leurs contributions détaillées.

La Suisse salue que le Conseil de sécurité se penche à nouveau sur le thème important de la cybersécurité. Les menaces dans le cyberespace, en particulier celles émanant d'acteurs étatiques ou tolérées par des États, peuvent menacer la paix et la sécurité internationales, comme le reconnaît le Pacte pour l'avenir.

Les nombreuses opportunités que nous offrent les développements dans le domaine des technologies de l'information et de la communication sont incontestables.

La diversité des dangers et des acteurs étatiques et non étatiques qui exploitent les vulnérabilités des systèmes pour mener des cyberactions malveillantes est tout aussi connue.

Parmi eux, les attaques par rançongiciels contre le système de santé sont une tendance extrêmement inquiétante qui s'accroît globalement depuis 2020.

La numérisation du système de santé permet de grands progrès au profit de la population, sa cyber-infrastructure devient de plus en plus complexe et donc plus coûteuse à sécuriser. La nécessité de rester opérationnel en tout temps accroît la pression tant sur les prestataires de soins eux-mêmes que sur les organismes publics. De telles attaques sont donc un moyen particulièrement perfide de viser l'infrastructure critique et la souveraineté d'un État. Des rapports récents faisant état d'une collaboration entre un groupe parrainé par la République Populaire Démocratique de Corée et le réseau de ransomwares Play soulèvent de sérieuses inquiétudes en matière de sécurité, car cela pourrait conduire à des attaques plus répandues et plus dommageables à l'échelle mondiale.

Permettez-moi de souligner trois aspects :

Premièrement, nous réitérons que le droit international, notamment la Charte des Nations unies, les conventions internationales sur les droits de l'homme et, en cas de conflit armé, le droit international humanitaire, s'applique et doit être respecté aussi dans le cyberespace.

En particulier, le principe de diligence raisonnable, qui s'est développé sur une longue période et qui, selon la Suisse fait partie du droit international coutumier, appelle tous les États à ne pas permettre sciemment que leur territoire soit utilisé pour des actions contraires aux droits d'autres États. Cela s'applique au monde physique comme au cyberespace. Les États sont invités à faire preuve de la diligence requise pour empêcher les groupes criminels d'utiliser leur infrastructure TIC et à coopérer aux niveaux national et international pour entraver les activités de ces groupes. Ce principe est par ailleurs reconnu dans le Cadre normatif en faveur d'un comportement responsable des États dans le cyberespace, adopté par consensus. Ces normes exigent en outre des États de ne pas mener ou soutenir sciemment des opérations cyber contre les infrastructures critiques, telles que les services de santé.

Deuxièmement, la répression des groupes criminels actifs dans le cyberespace est importante ; des actions de police récentes ont eu un effet considérable sur ces groupes. Mais la répression ne suffit pas à faire disparaître le phénomène. Les États doivent agir et prendre des mesures adéquates pour prévenir des attaques contre leurs infrastructures critiques. Nous attachons une importance tout particulière à renforcer la résilience et le dispositif sécuritaire du secteur des soins dans le domaine de la cybersécurité

Troisièmement, dans ce contexte souvent transnational, nous ne pouvons réussir qu'ensemble. La coopération internationale et le renforcement des capacités dans tous les États doivent être encouragés afin d'accroître la résilience et la sécurité du cyber-écosystème mondial. L'initiative Counter Ransomware, dont la Suisse fait partie, est un forum important à cet égard.

En outre, les États doivent davantage respecter leurs obligations internationales en matière de demandes d'entraide judiciaire, afin de permettre des poursuites pénales là où l'auteur est identifié.

Au niveau multilatéral, je tiens à souligner l'importance du *« Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale».* L'année prochaine, il sera important que le Groupe puisse recommander la création d'un mécanisme unique au sein de l'Assemblée générale pour continuer les travaux en s'appuyant sur l'acquis de ces dernières années.

Madame la Présidente,

« Gérer l'incertitude et renforcer l'humanité » était le thème posé par la 34ème Conférence internationale du Mouvement de la Croix-Rouge et du Croissant-Rouge. L'une des résolutions adoptées dans ce cadre, a souligné l'importance du droit international humanitaire pour protéger la population civile et les biens civils dans le contexte des conflits armés dans l'univers numérique.

Le Conseil de sécurité, pour sa part, a également un rôle à jouer. Il doit promouvoir le respect du droit international et la mise en œuvre du Cadre normatif en faveur d'un comportement responsable des États dans le cyberespace, afin que nos populations puissent bénéficier des vastes opportunités offertes par celui-ci, notamment dans le domaine de la santé.

Je vous remercie.

Unofficial translation

Mister President,

I would like to thank Dr. Tedros, Director-General of the WHO, and Mr. Conrad for their detailed contributions.

Switzerland welcomes the Security Council's renewed focus on the important issue of cybersecurity. Threats in cyberspace, particularly those emanating from state actors or tolerated by
States, can threaten international peace and security, as recognized in the Pact for the Future.

The many opportunities offered by developments in information and communication technologies are undeniable.

Equally well known is the diversity of threats and state and non-state actors who exploit system vulnerabilities to conduct malicious cyber actions.

Among these, ransomware attacks against the healthcare system is a very worrying trend that has been growing globally since 2020.

As the digitization of healthcare enables great progress for the benefit of the population, its cyber infrastructure is becoming increasingly complex and costly to secure. The need to remain operational at all times increases the pressure on both healthcare providers and public authorities. Such attacks are therefore a particularly insidious way of targeting a state's critical infrastructure and sovereignty. Recent reports of collaboration between a group sponsored by the Democratic People's Republic of Korea and the Play ransomware network raise serious security concerns, as this could lead to more widespread and damaging attacks on a global scale.

Let me highlight three aspects:

First, we reiterate that international law, including the UN Charter, international human rights conventions, and, in the event of armed conflict, international humanitarian law, applies and must be respected in cyberspace.

In particular, the principle of due diligence, which has been developed over a long period of time and, in Switzerland's view, is part of customary international law, calls on all States not to knowingly allow their territory to be used for actions contrary to the rights of other States. This applies to the physical world as well as to cyberspace. States are called upon to exercise due diligence to prevent criminal groups from using their ICT infrastructure, and to cooperate nationally and internationally to hinder the activities of such groups. This principle is also recognized in the *UN framework of responsible state behaviour in cyberspace*, adopted by consensus. These norms also require States not to knowingly conduct or support cyber operations against critical infrastructure, such as health services.

Second, repression of criminal groups operating in cyberspace is important; recent police actions have had a significant impact on such groups. But repression alone will not eliminate the phenomenon. States must act and take appropriate measures to prevent attacks on their critical infrastructure. In the area of cybersecurity, we attach particular importance to strengthening the resilience and security of the health sector.

Third, in this often transnational context, we can only succeed together. International cooperation and capacity building in all States must be promoted in order to increase the resilience and security of the global cyber ecosystem. The Counter Ransomware initiative, of which Switzerland is a member, is an important forum in this respect.

In addition, States must comply more fully with their international obligations regarding requests for mutual legal assistance to enable prosecution wherever the perpetrator is identified.

On a multilateral level, I would like to emphasize the importance of the "*Open-ended Working Group on developments in the field of information and telecommunications in the context of international security*". Next year, it will be important for the Group to be able to recommend the creation of a single mechanism within the General Assembly to continue the work, building on the achievements of recent years.

Madam President,

"Navigate Uncertainty, Strengthen Humanity" was the theme of the 34th International Conference of the Red Cross and Red Crescent Movement. One of the resolutions adopted in this context emphasized the importance of international humanitarian law in protecting civilians and civilian objects in the context of armed conflicts in the digital universe.

The Security Council also has a role to play. It must promote respect for international law and the implementation of the Normative Framework of responsible state behaviour in cyberspace, so that our populations can benefit from the vast opportunities that cyberspace offers, notably in the field of health.

I thank you.