



UNIDIR



Financé par
l'Union européenne

La cyberbiosécurité : une question de paix et de sécurité internationales ?

LOUISON MAZEAUD • ANDRAZ KASTELIC



Résumé

La bioéconomie mondiale connaît une croissance rapide, notamment grâce à la convergence entre la biotechnologie et les technologies de l'information et de la communication (TIC). Ce lien entre les **domaines numérique et biologique** apporte de nombreux avantages à un large éventail de secteurs, de l'agriculture à la médecine. Parallèlement, le nombre d'installations de recherche et de développement biologiques augmente également à l'échelle mondiale.

Cette convergence engendre de nouveaux risques potentiellement importants. Parmi ceux-ci figurent d'éventuelles attaques contre des installations de recherche et de développement biologiques, visant la **confidentialité, l'intégrité et l'accessibilité** des informations. Dans le contexte de la paix et de la sécurité internationales, les incidents liés aux TIC peuvent avoir des conséquences allant de mineures à significatives. Par exemple, un incident mineur pourrait consister en l'usurpation, par un acteur malveillant, des capteurs d'une installation agricole afin de transmettre de fausses données à l'exploitant, ce qui aurait un impact sur la production annuelle des cultures. À l'inverse, un incident majeur pourrait impliquer l'infiltration, par un acteur malveillant, des systèmes TIC d'un centre de recherche et de développement biologique, dans le but de perturber un système de production automatisé, en modifiant à distance les composés, rendant ainsi le produit inefficace, voire, pire encore, nocif.

Divers chercheurs et praticiens ont tenté de nommer et de définir un concept reconnaissant les caractéristiques uniques de l'infrastructure, des données, des vecteurs et des implications en matière de risques à cette intersection. **La cyberbiosécurité** désigne un ensemble de pratiques visant à faire face aux menaces informatiques

potentielles pesant sur ces systèmes, à la croisée des domaines numérique et biologique. Plus précisément, elle comprend des méthodes, des procédures et des mesures visant à lutter contre les menaces liées aux TIC qui pèsent sur la biosécurité.

Afin de mieux comprendre le lien entre les TIC et le domaine biologique, le présent document commence par exposer certains des avantages apportés par l'intégration des TIC de pointe dans la recherche et le développement biologiques. Il présente ensuite la définition susmentionnée du concept de « cyberbiosécurité » et poursuit en décrivant certains des principaux risques liés à cette intersection.

Le **Nouvel agenda pour la paix** lancé par le Secrétaire général des Nations Unies en 2023 souligne la nécessité pour les États membres de prévenir la militarisation des domaines émergents et de promouvoir une innovation responsable (Action 11). Le **Sommet de l'avenir de 2024** a été l'occasion pour les États membres de réaffirmer leur engagement en faveur de la prévention des risques biologiques et de l'utilisation abusive des technologies émergentes. Cela s'est notamment reflété dans le **Pacte pour l'avenir**, plus précisément dans l'action 26 (respecter les obligations et engagements en matière de désarmement) et l'action 27 (saisir les opportunités liées aux technologies nouvelles et émergentes et faire face aux risques potentiels posés par leur utilisation abusive).¹ La cyberbiosécurité se situe à la croisée de ces deux objectifs.

Cette notion n'a toutefois fait l'objet que d'une attention marginale dans les discussions multilatérales sur la sécurité internationale des TIC, notamment au sein des organes subsidiaires

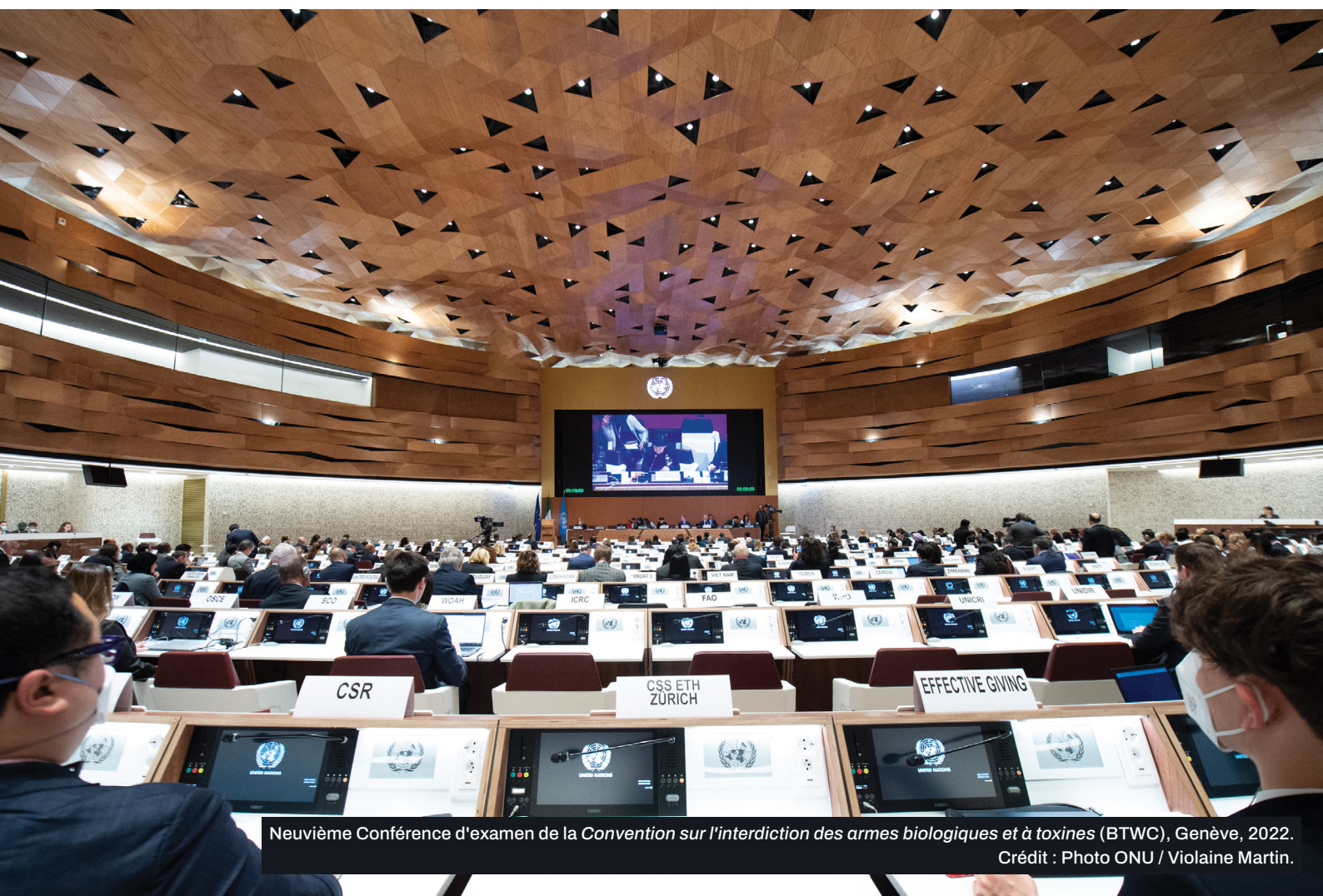
1 Nations Unies. (septembre 2024). Pacte pour l'avenir, Pacte numérique mondial et Déclaration sur les générations futures. https://www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf

de l'Assemblée générale, à savoir les groupes d'experts gouvernementaux de 2004 à 2021 et les groupes de travail à composition non limitée depuis 2019. Dans le cadre de la **Convention sur les armes biologiques et à toxines (CABT)**, une attention limitée a été accordée aux questions liées à la cyberbiosécurité. On trouve toutefois des éléments liés à la cybersécurité mentionnés dans des documents et déclarations des dix dernières années.

Enfin, au sein du **Conseil de sécurité des Nations unies**, plusieurs États ont exprimé leur inquiétude face à la multiplication des cyberattaques visant des infrastructures critiques, notamment dans le secteur de la santé, en particulier pendant la pandémie de COVID-19. Bien qu'elles n'englobent pas tous les aspects

de cette question, ces discussions peuvent contribuer à sensibiliser la communauté internationale et les professionnels à la nécessité de mettre en place de meilleures mesures.

Une piste à explorer pourrait consister à clarifier la portée du concept de cyberbiosécurité par le biais d'échanges avec les communautés concernées, et à prendre en compte la cyberbiosécurité dans le cadre du **groupe de travail de la Convention sur les armes biologiques** actuellement en place, notamment lors des discussions sur les avancées scientifiques et technologiques. Cette approche pourrait permettre un échange de points de vue et de bonnes pratiques dans le domaine cybernétique, ainsi que sur leur applicabilité aux installations de recherche et de développement biologiques.



Neuvième Conférence d'examen de la Convention sur l'interdiction des armes biologiques et à toxines (BTWC), Genève, 2022.
Crédit : Photo ONU / Violaine Martin.



Palais des Nations
1211 Genève, Suisse

© UNIDIR, 2025

WWW.UNIDIR.ORG