© Leila Rais

Das Team der Schweizer Mission in Wien, das für die erste, die politisch-militärische Dimension der OSZE zuständig ist (unsere Autorin und die Autoren von links: Luc Despotovic, Leila Rais und Christian Steiner – März 2026).

Les membres de l'équipe de la Mission suisse à Vienne chargée de la première dimension (dimension politico-militaire) sont, à partir de la gauche : Luc Despotovic, Leila Rais, Christian Steiner – mars 2026.

Risikoreduktion statt Rüstungskontrolle: Die OSZE stärkt Vertrauen im Cyberraum

Réduction des risques versus maîtrise des armements : l'OSCE renforce les mesures de confiance dans le cyberespace

Deutsch

Text Leila Rais, Chefin der politisch-militärischen Dimension, Luc Despotovic, politischer Berater und Christian Steiner, Militärberater VBS bei der Ständigen Vertretung der Schweiz bei der OSZE, den Vereinten Nationen und anderen internationalen Organisationen in Wien

Der Krieg gegen die Ukraine hat die europäische Sicherheitsordnung grundlegend verändert und Rüstungskontrollmechanismen geschwächt. Umso bedeutender sind vertrauensbildende Massnahmen im Cyberraum. Im Rahmen ihres OSZE-Vorsitzes setzt sich die Schweiz dafür ein Risiken zu reduzieren, Kommunikationskanäle offenzuhalten und unbeabsichtigte Eskalationen zu verhindern.

Die europäische Sicherheitsarchitektur der vergangenen Jahrzehnte wurde durch den Krieg Russlands gegen die Ukraine erschüttert. In diesem Kontext sind Rüstungskontrollregime weitgehend erodiert und bestehende vertrauensbildende Massnahmen bleiben in ihrer Wirkung oft sehr begrenzt. Vertrauensförderung zwischen den Teilnehmerstaaten der OSZE ist derzeit eine enorme Herausforderung. Ihr Mehrwert liegt deshalb nicht in der Wiederbelebung klassischer Rüstungskontrolle, sondern in pragmatischer Risikoreduktion. Vertrauensbildende Massnahmen im Cyberraum bieten dafür eine praktische Einstiegstür.

Der Cyberraum ist kein Feld der traditionellen Rüstungskontrolle. Cyberfähigkeiten sind schlecht sichtbar, häufig charakterisiert als dual-use (englisch für zivil und militärisch nutzbar) und eng mit zivilen Infrastrukturen, privaten Unternehmen und staatlichen Stellen verflochten. Anders als bei Panzern oder Raketen lassen sich Fähigkeiten, Absichten und Urheberschaft nur begrenzt beobachten. Die Zuschreibung von Angriffen bleibt technisch und politisch komplex. Gleichzeitig können Cybervorfälle innert Sekunden Grenzen überschreiten, kritische Infrastrukturen treffen und Spannungen auslösen, bevor Ursprung, Absicht und Wirkung geklärt sind. Die Operationen im Cyberraum sind integraler Bestandteil der hybriden Kriegsführung. Sie können der Beeinflussung von Gesellschaften dienen und kinetische Aktionen von Streitkräften wirkungsvoll unterstützen. Das Risiko liegt deshalb nicht nur im Vorfall selbst, sondern auch in der Wahrnehmung, der Attribution und der politischen Reaktion. Dies macht eine enge Abstimmung zwischen EDA und VBS erforderlich.

Als Folge davon haben die OSZE-Teilnehmerstaaten 2013 und 2016 bereits sechzehn vertrauensbildende Massnahmen für Sicherheit in den Bereichen Cyber sowie Informations- und Kommunikationstechnik verabschie-

Français

Texte Leila Rais, cheffe de la dimension politico-militaire, Luc Despotovic, conseiller politique, et Christian Steiner, conseiller militaire DDPS, de la Mission permanente de la Suisse auprès de l'OSCE, des Nations Unies et des autres organisations internationales à Vienne

Face à la guerre contre l'Ukraine, qui a bouleversé l'ordre de sécurité européen et affaibli les mécanismes de contrôle des armements, les mesures de confiance dans le cyberespace revêtent une importance croissante. Dans le cadre de son mandat de présidence de l'OSCE, la Suisse se mobilise pour contribuer à la réduction des risques, maintenir les canaux de communication et prévenir toute escalade involontaire.

L'architecture de sécurité européenne mise en place au cours des dernières décennies a été ébranlée par le souffle de la guerre menée par la Russie contre l'Ukraine. Dans ce contexte, les régimes de maîtrise des armements apparaissent grandement fragilisés et les mesures existantes visant à instaurer la confiance, défi de taille auquel les États participants de l'OSCE sont actuellement confrontés, ont souvent un impact très limité. À cet égard, une approche basée sur la réduction pragmatique des risques présente une valeur ajoutée que n'offre pas la relance des régimes traditionnels de contrôle des armements. Les mesures de confiance dans le cyberespace constituent un bon point de départ.

Le cyberespace est un domaine auquel le modèle classique de la maîtrise des armements ne s'applique pas. Les cybercapacités sont difficilement identifiables, souvent associées aux technologies à double usage (c'est-à-dire pouvant servir à des fins civiles et militaires) et étroitement liées à des infrastructures civiles, des entreprises privées et des organismes publics. S'il est possible d'investiguer sur des chars ou des missiles, il n'en va pas de même pour les capacités, les intentions et les responsabilités. L'imputation des incidents touchant à la cybersécurité reste complexe, tant sur le plan technique que politique. Les cyberattaques peuvent, en quelques secondes, traverser les frontières, toucher des infrastructures critiques et provoquer des tensions, avant même que leur origine, leurs objectifs et leurs conséquences n'aient été expliqués. Les opérations menées dans le cyberespace font partie intégrante de la guerre dite hybride. Elles peuvent influencer l'opinion publique dans les pays visés et soutenir efficacement les mouvements des forces armées. Le risque réside donc non seulement dans l'incident lui-même, mais également dans sa gestion, dans l'attribution des responsabilités et dans la réponse politique. D'où la nécessité d'une coordination étroite entre le DFAE et le DDPS.

det. Diese sollen den Cyberraum berechenbarer machen und konkrete Instrumente zur Vermeidung möglicher Missverständnisse bereitstellen. Der Wert dieser Massnahmen liegt primär in der praktischen Ausrichtung: Sie fördern Transparenz, Krisenkommunikation, den Schutz kritischer Infrastrukturen, öffentlich-private Partnerschaften und den Austausch von Erfahrungen. Dabei ersetzen sie nicht die klassische Abrüstung, sondern schaffen Kanäle und Verfahren, die im Krisenfall ungewollte Eskalationen vermeiden können. Besonders relevant ist dabei der Austausch von Informationen über Akteure und ihr Vorgehen über das OSZE-eigene Kommunikationsnetzwerk.

Für die Schweiz ist die Risikoreduktion in Europa ein zentrales Anliegen. Die Schweizer Vorsitzkonferenz zu antizipierenden Technologien vom 7. und 8. Mai 2026 in Genf bildete den Ausgangspunkt zur Umsetzung der Vorsitzprioritäten im Cyberraum. Der Anlass stellte künstliche Intelligenz, Quantencomputing und digitale Vernetzung in den Kontext kooperativer Sicherheit und endete mit der Erkenntnis, dass sich Technologie deutlich schneller verändert als die politisch gewollte Kontrolle. Daran knüpfte die Vorsitzkonferenz vom 29. und 30. September 2026 unter dem Titel «Deeskalation im Cyberraum» an. Im Fokus der Diskussionen zwischen den Delegationen standen Eskalationsrisiken und die Umsetzung der vertrauensbildenden Massnahmen. Mit diesen Konferenzen bot die Schweiz den OSZE-Teilnehmerstaaten eine Plattform die zunehmende Bedeutung des Cyberraums auf höchster Ebene zu diskutieren.

Parallel dazu beteiligt sich die Schweiz in Wien aktiv an Diskussionen über den Schutz vor Cyberrisiken in einer informellen Arbeitsgruppe unter dem Sicherheitsausschuss des Ständigen Rates. Dass dabei alle 57 Teilnehmerstaaten über konkrete Vorfälle im Cyberraum diskutieren, ist bereits transparenzbildend.

Insgesamt generiert die Zusammenarbeit von EDA und VBS einen Mehrwert für alle Akteure und versinnbildlicht die Dual-Use-Natur von Cyberrisiken. Ziel dieser Bemühungen ist es Kontakte zwischen den Teilnehmerstaaten zu aktivieren, Konsultationsmechanismen einzuüben, Missverständnisse zu klären und Netzwerke zwischen Diplomatie, Streitkräften, technischen Behörden, Wissenschaft sowie Privatsektor zu stärken und so einen Beitrag zur europäischen Sicherheit zu leisten. Dieser Ansatz ist schweizerisch bescheiden, aber in der aktuellen Lage umso relevanter.

Pour y faire face, les États participants de l'OSCE ont déjà adopté, en 2013 et 2016, seize mesures de confiance dans le domaine de la sécurité des technologies de l'information et de la communication (TIC). Ces mesures visent à renforcer la prévisibilité dans le cyberespace et à fournir des outils concrets pour réduire les risques de malentendus pouvant découler de l'utilisation des TIC. Leur intérêt réside avant tout dans leur vocation pragmatique : elles favorisent la transparence, la communication de crise, la protection des infrastructures critiques, les partenariats public-privé et l'échange de bonnes pratiques. Elles ne remplacent pas les programmes classiques de désarmement, mais permettent de mettre en place des canaux et des procédures susceptibles de prévenir les risques d'escalade involontaire en cas de crise. À cet égard, l'échange d'informations sur les acteurs et leurs activités par le réseau de communication de l'OSCE revêt une importance particulière.

La réduction des risques en Europe représente pour la Suisse une préoccupation majeure. Organisée les 7 et 8 mai 2026 à Genève, la conférence de l'OSCE consacrée à l'anticipation des nouvelles technologies constitue le point de départ de la mise en œuvre des priorités dans le cyberespace que la Suisse a définies pour son année de présidence. Replaçant l'intelligence artificielle, l'informatique quantique et la connectivité numérique dans le contexte de la sécurité coopérative, cet événement a mis en avant le retard que peuvent avoir, par rapport à l'évolution de la technologie, les mécanismes de contrôle mis en place par les responsables politiques. Consacrée à la désescalade dans le cyberespace, la conférence que la Suisse a organisée dans le cadre de sa présidence de l'OSCE, les 29 et 30 septembre 2026, faisait écho à celle du mois de mai. Les discussions entre les délégations ont principalement porté sur les risques d'escalade ainsi que sur la mise en œuvre des mesures de confiance. L'organisation de ces conférences a permis à la Suisse d'offrir aux États participants de l'OSCE une plateforme pour débattre, au plus haut niveau, de l'importance croissante du cyberespace.

En parallèle, à Vienne, la Suisse participe activement aux échanges sur la protection contre les cyberrisques au sein d'un groupe de travail informel relevant du Comité de sécurité, rattaché au Conseil permanent de l'OSCE. Le fait que l'ensemble des 57 États participants discutent d'incidents concrets survenus dans le cyberespace contribue déjà à améliorer la transparence.

Globalement, la collaboration entre le DFAE et le DDPS apporte une valeur ajoutée à tous les acteurs et met en lumière la nature à double usage, civile et militaire, des cyberrisques. Elle vise en outre à dynamiser les contacts entre les États participants, à mettre en place des mécanismes de consultation, à prévenir les risques de malentendus et à renforcer les réseaux entre les services diplomatiques, les forces armées, les autorités techniques, le monde scientifique et le secteur privé. Aussi modeste soit-elle, cette contribution de la Suisse à la sécurité européenne n'en demeure pas moins essentielle dans le contexte actuel.

© EDA

Catherine Fearon (in Grün), Direktorin des OSZE-Zentrums für Konfliktprävention, an einer OSZE-Paneldiskussion am CERN in Genf: Im Rahmen der Schweizer Vorsitzkonferenz im Mai 2026 standen neue Technologien und ihre Bedeutung für Frieden und Sicherheit innerhalb der OSZE-Region im Fokus (links im Bild: Tobias Privitelli, Schweizer Direktor des GICHD).

Catherine Fearon (en vert), directrice du Centre de prévention des conflits de l'OSCE, a également participé à la quatrième table ronde de la conférence de l'OSCE qui s'est tenue au CERN, à Genève, en mai 2026. La discussion a porté sur les enseignements liés aux nouvelles technologies et leur importance pour la sécurité et la coopération dans la région de l'OSCE (à gauche sur la photo, le Suisse Tobias Privitelli, directeur du GICHD).