Comparaison des politiques d'infrastructures critiques

Les attaques russes contre l'Ukraine et d'autres crises survenues ces dernières années ont entraîné des évolutions majeures des politiques liées aux infrastructures critiques au sein de l'UE, de l'OTAN et de la Suisse. Les efforts récemment déployés pour faire face aux risques mettent l'accent sur la résilience et la coopération afin de réduire l'impact des événements perturbateurs.

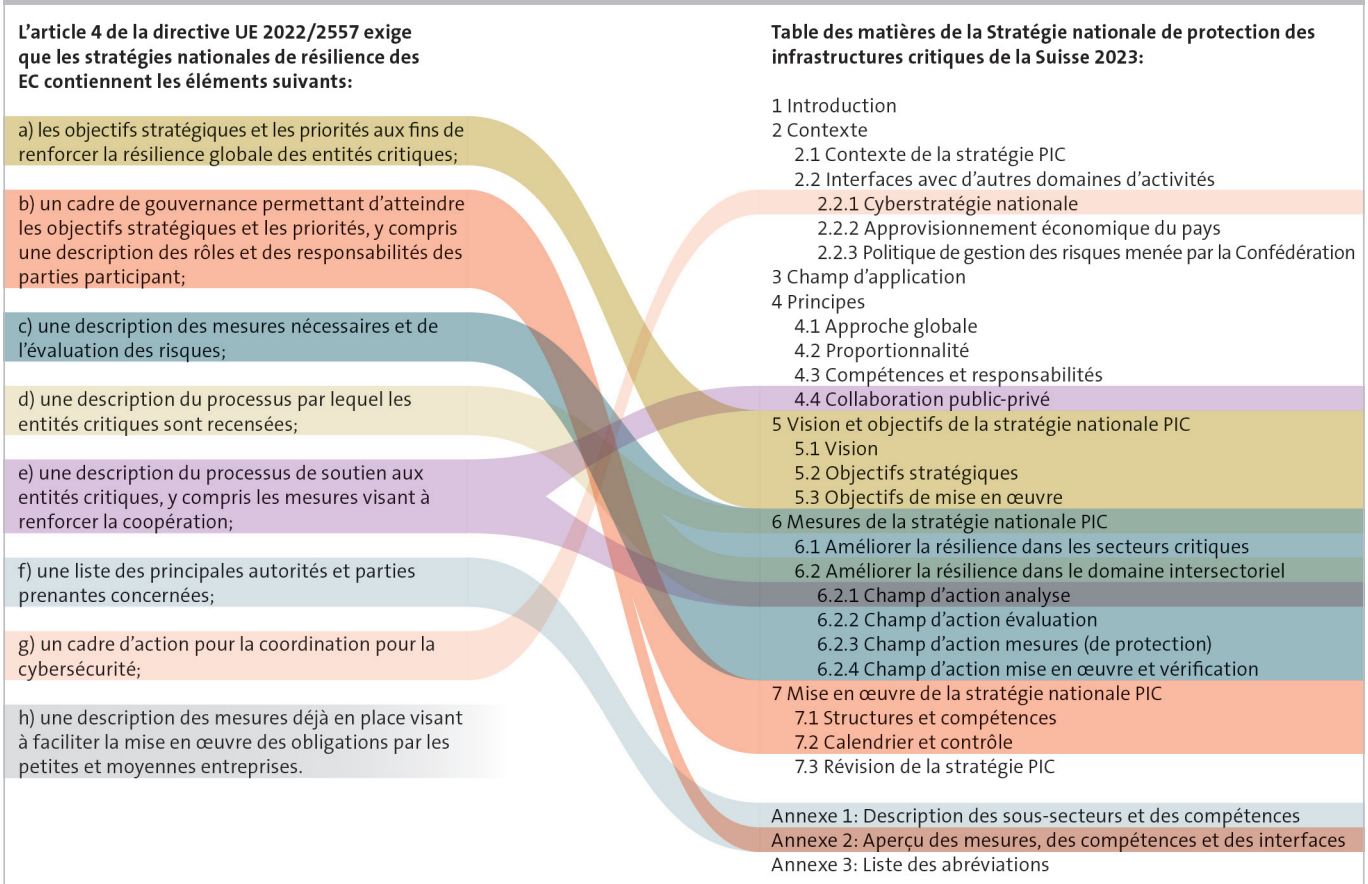
Par Simon Aebi

Une présentation, entre autres, de la *task-force* UE-OTAN sur la résilience des infrastructures critiques le 11 janvier 2023. *Johanna Geron / Reuters*

Les actions menées par la Russie en Ukraine depuis 2014, y compris l'invasion massive du pays en 2022, ont mis en évidence l'importance des infrastructures critiques (IC) et les conséquences de leurs vulnérabilités. Par exemple, la Russie a délibérément ciblé les infrastructures d'énergie et de communication afin d'obtenir un avantage militaire en désorganisant des services vitaux pour le pays. La plupart des menaces pesant sur les IC n'atteignent cependant pas le seuil d'un conflit armé et sont souvent qualifiées de «menaces hybrides». Celles-ci peuvent prendre différentes formes: cyberattaques, espionnage, désinformation, investissements étrangers dans des infrastructures, etc. En 2022, le sabotage du gazoduc Nord Stream en mer Baltique a ainsi révélé une vulnérabilité dans l'infrastructure énergétique européenne.

Les IC font référence aux équipements, aux systèmes, aux réseaux et aux opérateurs qui assurent les services nécessaires au fonctionnement des pouvoirs publics, des économies et des sociétés dont dépend la vie quotidienne des populations. Si la définition et le périmètre des IC varient légèrement en fonction des pays et des organisations, elles sont généralement considérées d'un point de vue sectoriel. Par exemple, en faisant la distinction entre les infrastructures énergétiques, les services de communication et les réseaux de transport, la vision sectorielle des IC offre un moyen de structurer et d'organiser leur recensement, leur gestion et leur protection. Aujourd'hui, les IC se caractérisent par de fortes dépendances découlant de la mondialisation, de l'urbanisation, de la numérisation et de l'omniprésence du cyberespace, ce qui brouille les frontières entre les différents secteurs et accroît leur vulnérabilité. Ainsi, les réseaux énergétiques actuels sont tributaires des réseaux de télécommunication, et vice versa. Une désorganisation de l'approvisionnement énergétique pourrait avoir des incidences néfastes sur les télécommunications. En général, la perturbation des services assurés par les IC peut porter gravement atteinte aux capacités des pouvoirs publics, aux activités économiques et au bien-être des populations. Ces interférences peuvent émaner de menaces antagonistes, mais aussi d'un large éventail de risques d'ordre naturel et géophysique, tels que des inondations ou des séismes, et d'incidents liés à des pannes techniques ou aux activités humaines. Par exemple, le déraillement

Recoupements entre les exigences de l'UE en matière de stratégies nationales CER et la stratégie PIC de la Suisse



Source: Directive de l'UE 2022/2557 et stratégie nationale suisse de protection des infrastructures critiques 2023 (adaptées par l'auteur).

d'un train de marchandises dans le tunnel du Gothard en août 2023 a mis en évidence l'impact d'une perturbation sur le réseau de transport ferroviaire suisse. En outre, du fait de la libéralisation des IC en Occident, surtout depuis les années 1990, celles-ci sont souvent détenues ou exploitées par des acteurs privés. Cette situation complique la surveillance, le contrôle et la normalisation des mesures de sécurité par les pouvoirs publics, face à des modèles économiques à la rentabilité optimisée.

Dans un contexte international marqué par une dégradation de la situation de sécurité, les IC et leur protection occupent une place de plus en plus importante pour les pays et les institutions en Occident. Le rapport complémentaire au rapport sur la politique de sécurité 2021 de la Suisse, publié en 2022, met l'accent sur l'examen et l'adaptation des stratégies de résilience et de coopération en matière de protection des infrastructures critiques (PIC) afin de préparer le pays aux défis qui l'attendent. Le rapport précise également qu'une coopération internationale accrue, en particulier avec l'OTAN et l'UE, offrirait de nouvelles possibilités de renforcer la protection civile, qui englobe la protection et la résilience des infrastructures critiques. Par conséquent, une réflexion sur les dernières évolutions au sein de l'OTAN et de l'UE et sur la compréhension actuelle de la résilience des IC offre un point de référence précieux pour soutenir une coopération éventuelle ou existante. L'examen de la nouvelle stratégie nationale PIC de la Suisse permet d'observer les chevauchements et les divergences entre les concepts de protection et de résilience des IC mis en place par la Suisse, l'UE et l'OTAN.

De la protection à la résilience

Au cours des vingt dernières années, la protection des IC a évolué vers la notion de résilience des IC, qui représente un véritable changement de paradigme. La protection des IC est devenue un pilier des politiques de sécurité après la Seconde Guerre mondiale et pendant la guerre froide. Elle visait à préserver les infrastructures critiques des aléas naturels, des problèmes technologiques, des accidents d'origine humaine et des attaques délibérées. Cette approche souvent «multirisque» consistait à identifier l'ensemble des risques et menaces pesant sur les IC, puis à atténuer ces dangers. Elle présentait toutefois des limites liées à son caractère irréaliste et, dans certains cas, à son inapplicabilité sur le plan économique.

La résilience des IC met plutôt l'accent sur l'identification et la réduction des vulnérabilités des IC. Une IC résiliente est capable de prévenir les perturbations, de les supporter et de se rétablir rapidement afin de garantir, dans l'idéal, la continuité des services en cas d'incident et de crise. Au lieu de chercher à protéger les IC contre l'ensemble des risques ou menaces envisageables, l'approche axée sur la résilience part du principe qu'il est impossible de connaître ou d'anticiper toutes les sources de perturbation. Ce constat est d'autant plus vrai si l'on considère le niveau d'interdépendance et les effets domino entre les

IC, ainsi que la nature des menaces dans le cyberespace. Le passage de la protection à la résilience des IC a également permis de voir les IC non plus comme des actifs physiques, mais comme des systèmes et réseaux assurant la fourniture de services vitaux. Aujourd'hui, la Suisse, l'UE et l'OTAN ont intégré la résilience dans leurs positions sur la sûreté et la sécurité des IC et s'efforcent d'atteindre cet objectif.

L'OTAN

En sa qualité d'alliance intergouvernementale conçue pour assurer la défense collective, l'OTAN se concentre principalement sur la sécurité mutuelle et la coopération entre ses États membres. Au fil du temps, les objectifs historiques de l'OTAN, à savoir la dissuasion et la défense, la prévention des crises et la sécurité coopérative, sont de plus en plus associés à la préparation civile et à la résilience nationale de ses États membres. Lors du sommet de Varsovie de 2016, les États membres de l'OTAN ont défini sept exigences fondamentales en matière de résilience, notamment la solidité des fonctions de l'État, de l'approvisionnement énergétique, des systèmes de communication et des infrastructures de transport.

L'idée de parvenir à une préparation civile et à une résilience nationale qui se traduisent par la continuité de l'action des pouvoirs publics, la fourniture de services essentiels à la population et le soutien du secteur civil aux armées est réitérée dans le concept stratégique 2022 de l'OTAN. L'OTAN comptant 21 pays qui font également partie de l'UE, une *task-force* UE-OTAN sur la résilience des infrastructures critiques a été créée en janvier 2023 pour tirer parti des liens étroits et des priorités communes des deux institutions. Jusqu'à présent, cette *task-force* s'est attachée à renforcer la résilience inter-institutionnelle dans les domaines des transports, de l'énergie, des infrastructures numériques et de l'espace en intensifiant la coopération, le partage d'informations et les systèmes d'alerte rapide. Son rapport d'évaluation final, publié en juin 2023, présente 14 recommandations visant à harmoniser les approches de l'UE et de l'OTAN en matière de résilience des IC. Reconnaissant le caractère interconnecté des IC, ces recommandations incluent l'élaboration de réponses rapides et de haut niveau aux menaces, la réalisation d'évaluations régulières des menaces pesant sur les IC, l'intégration des questions liées à la résilience des IC dans les exercices et la promotion d'un engagement stratégique entre les alliés, les États membres et le secteur privé.

L'Union européenne

En décembre 2022, la Commission européenne a remplacé sa directive de 2008 sur la protection des infrastructures critiques par une nouvelle directive sur la résilience des entités critiques (REC). L'on notera que dans la directive REC, le terme d'«entités critiques» (EC) s'est substitué à celui d'«infrastructures critiques». Complétée par la liste non exhaustive des services essentiels publiée en 2023, la directive REC se concentre sur les opérateurs d'IC et leurs services, qui constituent l'objet ultime des préoccupations, plutôt que sur les secteurs généraux des IC. La directive REC reflète les efforts déployés par l'UE pour renforcer la résilience des EC et de leurs services en tant que composantes centrales de la sécurité et de la défense, du marché intérieur de l'UE et des moyens de subsistance des citoyens européens. Cet objectif nécessite d'harmoniser les politiques nationales en matière d'EC dans tous les secteurs. C'est pourquoi la directive impose aux États membres des lignes directrices qui conduiront, à terme, à une réglementation accrue des EC.

Le temps relativement court dont disposent les États membres de l'UE pour adopter et mettre en œuvre cette directive témoigne de l'urgence de la question. Dans le contexte international marqué par une dégradation perçue de l'environnement de sécurité, la directive REC met également en relief la vulnérabilité des EC aux menaces hybrides. De surcroît, elle souligne l'importance du numérique et du cyberespace ainsi que les risques associés à ces domaines, ce qui montre une fois de plus que les IC ne sont pas simplement vues comme des actifs physiques. Enfin, la directive REC prescrit des mesures visant à renforcer la résilience des EC, telles que l'élaboration d'une stratégie nationale, des évaluations régulières des risques, des plans d'urgence, la notification des incidents ou des activités d'appui de la part des autorités. En outre, il apparaît essentiel de coordonner le renforcement de la collaboration et l'échange d'informations entre les États, les autorités et les entités, en particulier concernant la gestion des urgences.

La Suisse

En juin 2023, le Conseil fédéral a publié la troisième version de la Stratégie nationale de protection des infrastructures critiques de la Suisse. Cette stratégie vise à mettre au diapason toutes les parties prenantes, du niveau fédéral au niveau cantonal, en passant par le secteur privé. Pour cela, elle définit les objectifs et les principes généraux qui régiront l'approche suisse en matière d'IC. Bien que son intitulé évoque la «protection des infrastructures critiques», cette stratégie, comme sa version précédente de 2017, repose sur la notion de résilience des IC, comme en témoigne l'énoncé de sa vision: «La Suisse est résiliente du point de vue de ses infrastructures critiques de sorte à éviter les pannes de grande ampleur et à limiter les dommages suite à un événement.» Pour atteindre cet objectif, la stratégie propose huit mesures, dont sept mesures intersectorielles, visant à renforcer la résilience et à promouvoir la coopération entre les différents niveaux, secteurs et domaines d'activité des parties prenantes.

Différences de mandat et de niveau

Il n'est pas aisé de mettre en parallèle la stratégie nationale suisse, les recommandations de l'OTAN en sa qualité d'alliance de défense multinationale et la réglementation de l'UE, contraignante pour ses États membres. Une comparaison entre les différents niveaux de gouvernance, d'application et de mandats permet cependant d'obtenir une image plus complète des positions et des priorités de chaque institution sur la question des IC. En premier lieu, il apparaît difficile de transférer la conception de la résilience de l'OTAN dans la stratégie PIC de la Suisse, car les exigences fondamentales de l'OTAN portent essentiellement sur les capacités de défense collective de l'alliance. En outre, les exigences énoncées dans le rapport d'évaluation final de la *task-force* UE-OTAN semblent se calquer sur l'approche de l'UE en matière d'EC, mais en se limitant aux domaines en rapport avec les ambitions de l'OTAN.

> Une IC résiliente est capable de prévenir les perturbations, de les supporter et de se rétablir rapidement.

Il existe toutefois des similitudes: la stratégie PIC de la Suisse met également l'accent sur la résilience des infrastructures d'approvisionnement énergétique, des ressources alimentaires et hydriques, des systèmes de communication civils et des réseaux de transport. En deuxième lieu, l'OTAN conçoit la résilience des infrastructures comme un facteur permettant aux gouvernements d'agir et de communiquer. La stratégie suisse, en revanche, souligne le rôle que peuvent jouer des autorités préparées et

résilientes pour soutenir les opérateurs d'IC en cas d'événement perturbateur, ce qui reflète la nature fédérale du système politique suisse. En troisième lieu, alors que l'OTAN et l'UE donnent la priorité à la collaboration transfrontalière, la stratégie suisse n'aborde que brièvement les dépendances internationales en matière d'IC et vise plutôt à décrire et orienter les efforts de résilience internes de la Suisse sur cette question. En outre, le discours de l'OTAN et de l'UE sur les vulnérabilités potentielles met fortement l'accent sur les «menaces hybrides». La stratégie suisse, en comparaison, définit ces menaces et risques en des termes relativement vagues et s'appuie plutôt sur des évaluations au niveau du pays, des secteurs, des autorités et des opérateurs.

La coopération entre toutes les parties prenantes, notamment les relations entre le secteur privé et le secteur public, joue un rôle primordial.

En quatrième lieu, l'UE a adopté un langage qui marque une évolution claire de la protection des IC vers la résilience des EC et des services essentiels qu'elles fournissent. Si la stratégie suisse décrit, vise et met en œuvre un programme de résilience, elle conserve toutefois les notions d'IC et d'opérateurs d'IC et met moins l'accent sur les services que la directive REC. En cinquième lieu, la directive REC est contraignante pour les pays membres de l'UE et intègre des lignes directrices à mettre en œuvre par les EC identifiées. La stratégie PIC de la Suisse a, au contraire, une portée nationale. Il s'agit d'une recommandation et les éventuelles exigences ou règles sont fixées par la législation spécifique à chaque secteur (énergie, transports, finances, etc.) pour les opérateurs d'IC.

Conceptions communes

L'on relève donc un certain nombre de différences entre les orientations de l'OTAN, la réglementation de l'UE et la stratégie de la Suisse. Néanmoins, il existe une compréhension commune de l'importance des IC et de leur résilience. La Suisse, par exemple, a établi et mis en œuvre de façon indépendante des approches et des mesures de résilience des IC qui sont en adéquation avec celles de l'OTAN et de l'UE. Cette concordance est encore plus évidente si l'on compare les exigences de l'UE vis-à-vis de ses pays membres et la stratégie PIC de la Suisse. Ainsi, l'article 4 de la directive REC exige que les membres de l'UE adoptent une stratégie nationale. Or, la Suisse dispose non seulement d'une stratégie depuis 2012, mais celle-ci intègre les éléments requis par la directive REC. Les similitudes entre les trois approches ne se limitent pas à l'existence d'une stratégie nationale.

En premier lieu, les secteurs identifiés comme liés à des EC et à des IC, et qui permettent de définir les services jugés essentiels ou critiques, se chevauchent en très grande partie. En deuxième lieu, la directive REC comme la stratégie PIC de la Suisse exigent un recensement et des évaluations régulières des EC ou des IC, notamment la tenue d'un inventaire de celles-ci. En troisième lieu, les évaluations régulières des risques doivent envisager une perturbation potentielle des services et les mesures de résilience les plus efficaces à mettre en œuvre. En quatrième lieu, la directive REC exige que les États membres désignent les autorités qui seront chargées de superviser la mise en œuvre et le suivi de la stratégie. Leur rôle doit également consister à soutenir les parties prenantes et un point de contact unique doit être mis en place pour les questions transfrontalières liées aux EC. La stratégie suisse procède de la même manière en définissant les autorités de référence et en désignant l'Office fédéral de la protection de la population comme pôle de coordination pour les questions en rapport avec les IC. En cinquième lieu, l'accent est mis sur le partage d'informations et la notification des incidents qui pourraient perturber les services fournis par les opérateurs d'EC ou d'IC. La coopération entre toutes les parties prenantes, notamment les relations entre le secteur privé et le secteur public, joue un rôle primordial et la mise en place de plateformes intersectorielles est considérée comme un élément essentiel pour atteindre cet objectif. Enfin, la directive de l'UE préconise une réglementation nationale pour renforcer la résilience. À cet égard, la stratégie suisse de PIC recommande l'examen d'une proposition visant à ancrer les lignes directrices sur la résilience intersectorielle dans la loi.

Perspectives

Une compréhension mutuelle des priorités communes peut servir de point de départ pour simplifier ou renforcer la coopération entre la Suisse, l'OTAN et l'UE, comme le souligne le rapport complémentaire au rapport sur la politique de sécurité 2021 de la Suisse. Cela peut s'avérer utile, en particulier sur les questions ou les missions transfrontalières. Compte tenu du caractère interconnecté des IC, la Suisse doit au minimum observer les évolutions au sein de l'OTAN et de l'UE dans ce domaine, car l'expérience de ces organisations fournit de précieux enseignements. Les idées de l'OTAN concernant la résilience nationale et la préparation civile peuvent présenter un intérêt particulier. Dans le même esprit, la Suisse peut également tirer des enseignements de la proposition de recommandation de l'UE relative à un schéma directeur pour les infrastructures critiques visant à améliorer les réponses coordonnées et transfrontalières en cas d'incidents importants touchant des IC. L'objectif de cette recommandation, en cours d'examen par le Conseil européen, est de renforcer la connaissance commune de la situation, de mieux coordonner la communication au grand public et d'apporter des réponses efficaces aux incidents majeurs. Elle s'appliquerait en cas d'événement perturbateur touchant au moins six États membres ou lorsque l'impact de cet événement nécessite une coordination des politiques au niveau de l'UE.

Voir le site thématique du CSS pour en savoir plus sur la résilience sociotechnique.

Simon Aebi est Senior Researcher au sein de l'équipe «Risk and Resilience» du Center for Security Studies (CSS) à l'ETH de Zurich.

Les **analyses de politique de sécurité** du CSS sont publiées par le Center for Security Studies (CSS) de l'ETH de Zürich. Le CSS est un centre de compétence en matière de politique de sécurité suisse et internationale. Deux analyses paraissent chaque mois en allemand, français et anglais.

Éditrice: Névine Schepers
Relecture: Névine Schepers
Layout et graphiques: Miriam Dahinden-Ganzoni

Feedback et commentaires: analysen@sipo.gess.ethz.ch
Plus d'éditions et abonnement: www.css.ethz.ch/cssanalysen

ISSN: 2296-0228; DOI: 10.3929/ethz-b-000671765