

LES PPP DANS LA POLITIQUE DE SÉCURITÉ: CHANCES ET LIMITES

La collaboration entre acteurs publics et privés est devenue un instrument important dans le domaine politique de la sécurité intérieure. Les partenariats publics-privés (PPP) se chargent de tâches essentielles dans la protection des infrastructures critiques, la cyber-sécurité ou la garantie de la sécurité de l’approvisionnement. Il ne faut cependant pas sous-estimer les difficultés rencontrées lors de la mise en place de tels partenariats.



La coopération publique-privée gagne aussi de l’importance dans la politique de sécurité.

Les frontières entre le secteur privé et l’Etat sont devenues de plus en plus perméables depuis les années 1990. La politique du *New Public Management* a entraîné la privatisation des services publics les plus divers. L’idée de base derrière cette réforme du secteur public est d’exploiter aussi les méthodes de production efficaces du secteur privé dans la mise à disposition de services publics. Les autorités se concentrent, dans ce modèle, sur le contrôle politique et stratégique et confient la réalisation opérationnelle à des acteurs privés. Des partenariats publics-privés (PPP) ont vu le jour dans de nombreux domaines politiques dans ce contexte. Le terme de PPP est utilisé pour désigner différentes formes de coopération. Il désigne couramment les coopé-

rations à long terme entre acteurs privés et publics en vue d’accomplir une tâche publique.

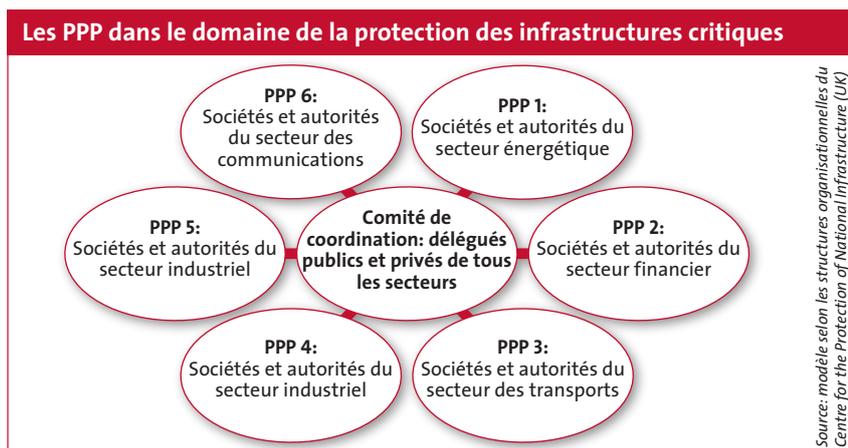
On n’a pendant longtemps guère remarqué la tendance à de nouvelles formes de coopération publique-privée en politique de sécurité. La garantie de la sécurité n’est pas simplement un service parmi d’autres que doit fournir un Etat. Parce que la sécurité est directement liée à la question du monopole de puissance, la politique sécuritaire est traditionnellement considérée comme le domaine exclusif de l’Etat. Il existe malgré tout aussi dans ce domaine une tendance à une coopération plus grande entre l’Etat et l’économie. L’externalisation de tâches militaires à des prestataires de sécurité privés telle qu’on peut

l’observer en particulier dans les forces armées américaines en est l’exemple le plus connu mais aussi le plus controversé.

On accorde habituellement moins d’attention à la coopération dans le domaine de la sécurité intérieure. Mais cette collaboration est devenue de plus en plus importante. Il y a aujourd’hui dans de nombreux pays des PPP qui se chargent des tâches relatives à la protection de la population. Des exemples en sont les partenariats en vue de protéger les infrastructures critiques, de prévenir les cyber-attaques ou de garantir la sécurité de l’approvisionnement.

Augmentation d’importance en politique de sécurité

Comment expliquer le fait que l’Etat recherche de plus en plus la coopération avec le secteur privé même dans le domaine sensible de la sécurité intérieure? Deux facteurs sont déterminants. Premièrement, l’intensification de la coopération est une conséquence de la libéralisation économique. La privatisation des entreprises publiques a eu pour corollaire le fait que l’Etat n’a plus d’influence directe sur certaines entreprises qui exercent des fonctions supportant le pouvoir, ce qu’illustre bien l’exemple du secteur des télécommunications. Les télécommunications ont longtemps été placées sous le contrôle étatique direct. Les gouvernements pouvaient déterminer directement à quelles normes de sécurité devait répondre les réseaux correspondants. Aujourd’hui, sur le marché libéralisé des télécommunications, l’Etat ne peut plus exercer qu’une influence indirecte en intervenant de ma-



nière régulatrice, en mettant en place des mesures d'incitation ou même en recherchant la coopération des exploitants.

Le deuxième facteur contribuant à l'importance croissante des PPP dans la politique de sécurité est la complexité du contexte socio-économique. Les sociétés actuelles sont caractérisées par une grande interdépendance des domaines les plus divers. Si l'alimentation électrique tombe par exemple en panne, cela peut facilement entraîner la panne des systèmes de transport, ce qui a à son tour pour conséquence l'absence de certaines personnes à leur lieu de travail et donc la non-exécution de tâches importantes. L'utilisation généralisée des technologies d'information et de communication a encore accru la mise en réseau et la dépendance mutuelle. Des pannes à des points névralgiques peuvent avoir des effets en cascade dont il est très difficile de prévoir la dynamique.

Pour pouvoir organiser de manière optimale la collaboration entre différentes entreprises de services en cas de crise, les autorités doivent par conséquent savoir où se situent les interfaces entre les entreprises. La protection de la population exige une planification branchée qui n'est possible qu'avec l'aide de réseaux coopératifs. C'est pourquoi la mise sur pied de partenariats où les responsables des entreprises et des autorités compétentes se préparent à des cas de crise possibles fait partie des tâches centrales dans la protection de la population.

Exemples de coopération

La collaboration entre acteurs publics et privés est particulièrement importante dans la protection des infrastructures critiques. C'est ainsi que l'on appelle les entreprises garantissant la disponibilité de biens ou services centraux (p.ex. énergie,

transports ou télécommunications). Beaucoup de pays ont développé des vastes programmes pour organiser la coopération dans ce domaine. On trouve au centre de cette coopération l'échange d'informations se rapportant à la sécurité entre les exploitants des infrastructures critiques et les représentants des autorités.

La collaboration est généralement organisée par secteur, ce qui signifie que ce sont principalement des entreprises et des autorités du même secteur économique qui échangent des informations sur les risques, tendances et mesures de protection possibles. Un comité supérieur composé pour sa part de représentants publics et privés de tous les secteurs se charge souvent de coordonner les différents partenariats sectoriels. On peut décrire cette forme structurée de coopération publique-privée comme un «diagramme radial» (cf. graphique). Les programmes de protection des infrastructures critiques, par exemple en Grande-Bretagne, aux Pays-Bas, en Australie et aux Etats-Unis, suivent ce modèle ou un modèle similaire.

Les partenariats dans le domaine de la cyber-sécurité suivent une logique similaire. Dans ces PPP aussi, il s'agit en premier lieu d'échanger des informations. Les entreprises communiquent aux autorités quels incidents elles ont enregistré, où il y a d'éventuelles failles de sécurité et quelles mesures de protection elles ont prises, ce qui permet aux autorités de se faire une idée des menaces et risques dans le domaine de la cyber-sécurité. En contrepartie, les entreprises bénéficient de l'aide des autorités dans la prévention des incidents et la réaction à ces derniers. Parce que le cyberspace ne connaît pas de frontières nationales, les autorités jouent un rôle décisif, particulièrement dans la

coordination avec les autres pays. La forte dépendance mutuelle entre l'Etat et les entreprises pour ce qui est de la cyber-sécurité a contribué au succès retentissant des PPP dans ce domaine. Les PPP sont mentionnés dans presque tous les pays comme un instrument important dans les stratégies et initiatives sur le thème de la cyber-sécurité.

Les programmes de protection des infrastructures critiques et de promotion de la cyber-sécurité sont des exemples de partenariats nouvellement établis. L'intensification de la collaboration dans la sécurité intérieure découle cependant aussi d'un approfondissement de formes de coopération qui existaient déjà. Il y a par exemple une longue tradition dans le domaine de la politique d'approvisionnement. Garantir même en temps de crise la disponibilité de biens nécessaires comme les denrées alimentaires, les matières premières, l'énergie ou les médicaments fait partie des tâches centrales de l'Etat. Dans le cadre de la politique d'approvisionnement – qui remonte en Suisse aux expériences faites pendant les guerres mondiales – l'Etat a déjà recherché très tôt la collaboration des fabricants de ces biens. Les autorités sont souvent intervenues directement sur le marché, par exemple avec la consigne de créer des réserves obligatoires pour certains biens.

On essaie davantage, aujourd'hui, de ne plus garantir la sécurité d'approvisionnement par des consignes mais en intensifiant la coopération. Pour comprendre les ramifications nationales et internationales complexes de l'économie et en déduire une politique de prévoyance efficace, les autorités ont besoin de travailler avec le secteur privé. Inversement, les entreprises s'intéressent également à une réglementation efficace. Elles veulent d'une part éviter des interventions inutiles sur le marché et ont d'autre part elles aussi besoin des ressources d'autres entreprises et sont donc intéressées par une sécurité d'approvisionnement élevée.

L'exemple de l'approvisionnement économique du pays (AE) en Suisse illustre comment la politique de sécurité de l'approvisionnement – longtemps caractérisée par le contraste (prétendu) entre interventionnisme et liberté du marché – est devenue ces dernières années une collaboration partenariale. La structure actuelle de l'AE est fortement marquée par la coopération de personnel de milice des entre-

prises et des autorités. Plus de 300 cadres de l'industrie et de l'administration sont impliqués au total. L'Office fédéral pour l'approvisionnement économique du pays (OFAE) sert d'état-major coordonnant et structurant la collaboration. Les représentants des sociétés et des autorités essaient de prendre ensemble des mesures pour les situations de crise. L'idée selon laquelle ni le marché ni l'Etat ne peuvent garantir un approvisionnement de la population en biens importants sans se soutenir mutuellement s'est imposée.

La prolifération des PPP dans les domaines de la protection des infrastructures critiques, de la cyber-sécurité et de la politique d'approvisionnement montre combien la coopération publique-privée est devenue importante dans la politique de sécurité. Il est essentiel de comprendre que les partenariats publics-privés dans le domaine politique de la sécurité intérieure ne servent pas à privatiser des tâches de la politique de sécurité mais représentent un complément et une alternative aux interventions régulatrices de l'Etat. Dans un contexte fortement branché et dynamique, il n'est plus guère possible d'établir efficacement la sécurité en édictant des consignes. Se concentrer sur l'intérêt commun pour un contexte sûr et prévisible peut aider à surmonter la contradiction parfois totale entre sécurité et rentabilité.

Défis et limites

Il ne faut pas sous-estimer les difficultés rencontrées lors de la mise en place d'une approche partenariale dans la politique de sécurité. Deux grands défis se posent en pratique. Premièrement, la collaboration ne peut porter des fruits que si elle est bien coordonnée, ce qui comporte différentes tâches. Dans un premier temps, tous les acteurs importants doivent être convaincus de la valeur de la coopération. Il faut ensuite se mettre d'accord sur des objectifs et des méthodes communs et il faut encore, finalement, décider qui est responsable de l'implantation de quelles mesures. Toutes ces étapes recèlent un potentiel conflictuel et doivent être réglées dans le cadre de processus parfois fastidieux. Il faut donc des acteurs qui coordonnent, structurent et activent la coopération. Ces acteurs peuvent venir du secteur public ou privé. Il est important qu'ils disposent des ressources nécessaires pour gérer le partenariat et soient reconnus par les autres partenaires comme les organisateurs de la collaboration.

Les PPP: activités exemplaires dans le domaine de la cyber-sécurité

- Soutien en cas d'incidents:** le réseau de PPP est utilisé pour analyser un incident (virus, attaque de pirate, etc.) et définir des contre-mesures techniques. Les acteurs publics offrent – si nécessaire – leur aide pour entamer des démarches juridiques ou coordonner des actions avec des autorités étrangères.
- Alerte précoce:** les membres sont rapidement informés d'attaques contre d'autres membres par le biais de canaux de communication internes. Ils peuvent ainsi prendre d'emblée des contre-mesures si nécessaire.
- Workshops:** des experts expliquent aux membres les nouveaux dangers et possibilités de protection contre les cyber-attaques dans le cadre de rencontres régulières. Les workshops ne servent pas seulement à échanger des connaissances spécialisées mais aident aussi à renforcer la confiance mutuelle.
- Relations publiques:** les membres s'engagent conjointement lorsque les utilisateurs des services Internet sont avisés des dangers possibles. L'approche conjointe augmente la crédibilité des alertes.

Le second défi consiste à communiquer vers l'extérieur. Le grand potentiel attribué au concept de coopération publique-privée entraîne souvent des attentes trop élevées. Tant les représentants des autorités que les représentants des entreprises doivent rendre compte à leurs supérieurs. Il est parfois difficile de faire comprendre à ces derniers qu'il faudra attendre relativement longtemps avant de pouvoir présenter des résultats concrets. Parce que beaucoup d'entreprises ont des activités internationales il peut en outre s'avérer difficile de convaincre les directions des entreprises de l'importance de la coopération nationale ou même locale.

En plus de ces défis pratiques, il est aussi déterminant de tenir compte des principes démocratiques pour la coopération. Même s'il est légitime que les autorités coopèrent en premier lieu avec les entreprises immédiatement importantes pour la sécurité, cela ne peut pas entraîner de favoritisme susceptible de distordre la concurrence. Il faut en outre maintenir un minimum de transparence, même dans les partenariats où sont échangées des informations délicates. Les représentants des autorités doivent s'assurer que les PPP ne se meuvent pas en dehors des mécanismes de contrôle démocratiques et puissent donner à leur organe de surveillance démocratique respectif des renseignements quant aux activités.

Il est central, dans la mise en place d'une approche partenariale en politique de sécurité, de ne pas perdre la cohérence. Fixer des priorités sécuritaires et imposer la mise en œuvre de la politique définie reste la tâche du gouvernement. Les PPP peuvent être en l'occurrence un instrument prometteur parce qu'une coopération est souvent plus efficace qu'une réglementation. Mais la collaboration exige que le gouvernement préserve son

indépendance vis-à-vis des intérêts privés et dirige et coordonne les PPP de façon à ce qu'ils servent les objectifs de politique sécuritaire supérieurs. C'est la seule façon de garantir le succès d'une approche partenariale en politique de sécurité et son acceptation par la société.

Les PPP en Suisse

Il y a en Suisse plusieurs exemples réussis de collaboration entre l'Etat et les entreprises dans le domaine de la politique de sécurité. En plus de l'Office fédéral pour l'approvisionnement économique du pays, le programme de protection des infrastructures critiques de l'Office fédéral de la protection de la population (OFPP) repose lui aussi sur la coopération publique-privée. On citera également la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) qui se concentre sur la protection des structures informatiques.

Ces partenariats fonctionnels prouvent le potentiel de coopération dans le domaine de la politique de sécurité en Suisse. Comparée à d'autres pays, la Suisse dispose de conditions particulièrement favorables. Parce que le système de milice y est largement ancré, il n'y a pas de fossé profond entre l'administration et les entreprises. Il existe de nombreux réseaux supra-sectoriels pouvant être utilisés pour la collaboration. Alors que la relation entre l'Etat et l'économie est caractérisée par une grande méfiance mutuelle dans de nombreux autres pays, ce qui entrave souvent la coopération, ce problème est beaucoup moins important en Suisse grâce au système de milice et à l'exiguïté géographique.

Le plus grand défi rencontré lors de la mise en place de PPP en Suisse se situe au niveau du fédéralisme prononcé. Le partage des tâches entre la Confédération, les cantons et les communes peut avoir pour

corollaire une répartition peu claire des responsabilités du côté des autorités. La collaboration avec le secteur privé ne peut cependant fonctionner avec succès que si l'on définit clairement quel acteur de l'administration publique est l'interlocuteur des entreprises. L'implantation de PPP pré-suppose donc une coordination soigneuse entre les différents représentants des autorités. Il peut s'avérer utile à ce sujet de confier à un acteur un mandat clair pour coordonner les partenariats dans un domaine concret de la politique sécuritaire.

Il est souhaitable, à l'avenir, de tenir compte davantage et le plus tôt possible de l'approche coopérative dans la formulation de politiques dans le domaine de la sécurité intérieure. Cela exige des consignes claires aux différentes autorités quant aux responsabilités dans l'encouragement et la mise en œuvre de la coopération avec le secteur privé. Justement parce que l'instrument des PPP a encore beaucoup de potentiel dans la politique de sécurité, il est d'autant plus important de l'utiliser de manière prudente et responsable.

I Editeur responsable: Daniel Trachsler
analysen@sipo.gess.ethz.ch

I Expert ayant contribué à cette analyse:
Manuel Suter
suter@sipo.gess.ethz.ch

I Commande d'analyses et abonnement:
www.ssn.ethz.ch

Parus précédemment



- N° 110: L'OSCE en position difficile
- N° 109: Afghanistan: vague espoir de solution régionale
- N° 108: La puissance protectrice: la renaissance d'une tradition?
- N° 107: Armes atomiques au Moyen-Orient: aucune solution en vue
- N° 106: Politique étrangère suisse après Mme Calmy-Rey
- N° 105: Médiation dans les conflits religieux
- N° 104: Fukushima et les limites de l'analyse des risques
- N° 103: La cartographie de crise: le phénomène et son utilité
- N° 102: L'Afrique du Sud: une puissance régionale limitée
- N° 101: Les Frères musulmans en Egypte: obstacles sur la voie du pouvoir
- N° 100: La Libye après Kadhafi: transition politique et options occidentales
- N° 99: Une Europe fragmentée dans un Congo instable
- N° 98: Al-Qaïda après les bouleversements arabes et la mort de Ben Laden
- N° 97: Le Pakistan après Ben Laden: un constat
- N° 96: Politique extérieure de l'UE: nouvelles structures, anciennes faiblesses
- N° 95: Caucase du Nord: instabilité croissante dans le sud de la Russie
- N° 94: Conflit au Proche-Orient: nouveau contexte, nouvelle dynamique
- N° 93: Le Brésil: puissance économique à se profiler en politique étrangère
- N° 92: La lutte pour les avions de combat: gagnants et perdants
- N° 91: Opération militaire en Libye: l'OTAN prise dans un dilemme
- N° 90: Sécurité humaine: genèse, débats, tendances
- N° 89: Désarmement nucléaire: une voie semée d'embûches
- N° 88: Le progrès biotechnologique: un défi sécuritaire
- N° 87: Gestion civile des crises de l'UE: un bilan intermédiaire
- N° 86: L'OTAN et la défense antimissile: chances et questions en suspens
- N° 85: Le sommet de l'OTAN: résolutions ambitieuses, réalisations incertaines
- N° 84: La Force africaine en attente
- N° 83: Sanctions économiques: arme miracle ou échec?
- N° 82: Les services de renseignement contraints à la réforme
- N° 81: Politique européenne de la Suisse: où conduit la voie bilatérale?
- N° 80: Privatisation de la sécurité: limites de l'externalisation militaire
- N° 79: Démocratisation après les conflits: pièges de l'influence extérieure
- N° 78: Drones: applications militaires et débats politiques
- N° 77: Affaire libyenne: bilan de la gestion de la crise par la Suisse
- N° 76: Sécurité énergétique: les marchés du gaz naturel en mutation
- N° 75: Le service militaire obligatoire en comparaison européenne
- N° 74: Politique nucléaire américaine: un changement modéré
- N° 73: L'Inde: une puissance émergente placée devant de grands défis
- N° 72: Réforme du Conseil de sécurité: un noeud gordien?
- N° 71: Cyberguerre: concept, état d'avancement et limites
- N° 70: Le Yémen: lutte difficile contre le terrorisme
- N° 69: La politique énergétique de l'UE face à de grands défis
- N° 68: Finlande: gestion de crises et défense territoriale
- N° 67: Engagements de l'armée à l'étranger: bilan et options
- N° 66: L'Organisation de coopération de Shanghai: signification pour l'occident
- N° 65: La crise du TNP: avant la conférence d'examen de 2010
- N° 64: Politique de défense britannique: pression réformiste
- N° 63: Promotion civile de la paix: potentiel et limites
- N° 62: Communication du risque: utilité pour la politique de sécurité
- N° 61: Politique extérieure de la Suisse 2009: Etat des lieux
- N° 60: La résilience: un concept pour la gestion des catastrophes et crises
- N° 59: Iran: Crise interne et marge de manoeuvre des états occidentaux
- N° 58: Prix du pétrole et géopolitique: les gagnants et les perdants
- N° 57: Le nucléaire gagne du terrain: le risque de prolifération
- N° 56: Le voisinage oriental de l'Europe entre influence russe et ancrage à l'Ouest
- N° 55: Opération Atalante: piraterie et politique de sécurité de la Suisse
- N° 54: Alliance de contradictions: l'OTAN après le sommet anniversaire
- N° 53: Désarmement atomique: l'Amérique et la Russie reprennent les négociations