Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Intervention de M. Jean-Philippe GRELOT
Conseiller du Secrétaire Général de la Défense Nationale
Protection des infrastructures critiques
Plénière de la Conférence du Désarmement
Genève, le 22 juin 2006

Vérifier au prononcé

C'est au milieu des années 1990, voilà donc dix ans, que plusieurs pays ont engagé des réflexions sur les infrastructures critiques. A cette époque, le spectre de la Guerre froide et de ses menaces proprement militaires s'éloignait du ciel européen. La demande de sécurité de la population se portait vers d'autres risques : catastrophes naturelles, accidents technologiques, perturbations générées par de grands mouvements sociaux. On avait connu, en divers lieux du globe, de gigantesques pannes d'électricité provoquées par le gel, des inondations exceptionnelles, l'explosion d'usines chimiques ou encore un accident majeur sur une centrale nucléaire.

On a alors identifié que le fonctionnement de la société était tributaire de quelques grandes infrastructures. On a constaté que ces infrastructures étaient interdépendantes et qu'elles offraient en général une faible capacité de substitution en cas de défaillance. La préparation du passage informatique à l'an 2000 a révélé la place cruciale des systèmes d'information au cœur de leur fonctionnement.

Les attentats du 11 septembre 2001 à New York et à Washington, ceux du 11 mars 2004 à Madrid, ceux du 7 juillet 2005 à Londres ont frappé d'abord la population civile. Ils ont également touché des centres économiques et politiques pour les premiers, des réseaux de transport public pour les seconds, montrant les perturbations que des actes de terrorisme pouvaient provoquer sur les infrastructures. On a imaginé les conséquences de telles attaques si elles étaient commises avec des engins de destruction massive.

On l'a encore vu tout au long de ces trente derniers mois, chaque tremblement de terre, chaque cyclone, chaque tsunami détruit les infrastructures de télécommunications, de distribution d'énergie, de transport et de soins. Les capacités d'évaluation de la situation, d'acheminement des secours et de prise en charge des victimes en sont réduites d'autant.

Enfin, tous les pays qui, à l'invitation de l'Organisation mondiale de la santé, ont élaboré depuis deux ans des plans de lutte contre une pandémie grippale d'origine aviaire, ont traité de deux sujets principaux : d'une part la protection de la population ; d'autre part, pendant les semaines ou les mois de présence de l'épidémie, la continuité des activités essentielles, souvent tributaires d'infrastructures critiques.

Nous ne pouvons plus nous considérer dans un monde de menaces théoriques contenues par l'équilibre de la Guerre froide. Nous sommes confrontés à des menaces permanentes, terroristes, informatiques, économiques, sanitaires ou météorologiques, d'intensité variable dans le temps et dans l'étendue géographique. Elles peuvent nous affecter à chaque instant. Elles peuvent frapper chaque pays sur son territoire même ou, mondialisation aidant, à travers ses ressortissants et ses intérêts à l'étranger. Souvent pernicieuses, elles ne sont pas principalement dirigées contre l'État ni contre ses institutions et ses structures administratives : elles visent en premier lieu la population et ses conditions de vie.

Les enjeux sont alors de répondre à la demande de sécurité et de protection de la population non pas seulement au moment où une crise survient, mais en profondeur et dans la durée. Dans ce mouvement, les infrastructures critiques se sont ainsi imposées dans les problématiques de prévention et de gestion des crises, que leur origine soit une catastrophe naturelle, un accident, un acte de malveillance ou un attentat.

Dimension internationale

Le sujet ne concerne pas seulement chaque État individuellement, légitimement soucieux du bien-être de sa population et du bon fonctionnement de son économie. Il concerne la communauté internationale.

Une première raison en est que, dans des États dont l'économie ou l'administration est fragile, une atteinte grave aux infrastructures critiques n'aura pas seulement un bilan éventuellement humain et toujours financier. Elle pourra fragiliser les institutions politiques et générer une instabilité voire des troubles plus ou moins durables, plus ou moins profonds.

Une seconde raison tient à la mixité des acteurs : des administrations d'un côté, des entreprises de l'autre. Un État avec ses frontières, qui limitent le champ de compétence de ses services ; des entreprises souvent multinationales, dont les logiques d'action ne reconnaissent pas nécessairement un concept de devoir national.

Une troisième raison découle de l'extension géographique de certaines infrastructures et de leur zone d'influence : infrastructures transfrontalières comme les ponts ou les tunnels, infrastructures régionales comme les réseaux de transport d'électricité ou d'hydrocarbures, infrastructures mondiales comme le transport aérien et plus encore l'Internet.

Une quatrième raison est que les crises, comme la mondialisation, ont dissipé les frontières. Les médias internationaux portent immédiatement le moindre accident, la moindre décision d'un gouvernement à la connaissance du monde entier. Toute réaction à une menace ou à une crise importante amène un État à assurer une coordination avec ses voisins, avec ses alliés et ses partenaires, avec les grandes organisations internationales. Chacun en tire des conclusions pour sa propre situation.

Une cinquième raison, dans le cas des actes intentionnels, réside dans les instruments que le droit international a construits pour dissuader les agressions, pour protéger certaines infrastructures et pour poursuivre les agresseurs.

Une sixième raison pourrait être la définition internationale d'une liste d'infrastructures critiques. Elle n'existe pas, bien que les approches convergent sur les principaux domaines à couvrir. A titre d'exemple, la Commission européenne, dans son récent *Livre vert relatif au programme européen de protection des infrastructures critiques*[1], a arrêté une liste de 37 infrastructures regroupées en onze secteurs :

[1] Livre vert relatif au programme européen de protection des infrastructures critiques du 17 novembre 2005.

I. énergie : (1) production, raffinage, traitement et stockage, y compris les canalisations, de pétrole et de gaz ; (2) production d'électricité ; (3) transmission d'électricité, de gaz et de pétrole ; (4) distribution d'électricité, de gaz et de pétrole ;

II. information, technologies de communication : (5) protection des systèmes d'information et des réseaux ; (6) automatisation des instruments et des systèmes de contrôle ; (7) Internet ; (8) fourniture de télécommunications fixes ; (9) fourniture de télécommunications mobiles ; (10) communication radio et radionavigation ; (11) communication par satellite ; (12) radiodiffusion ;

III. eau : (13) fourniture d'eau potable ; (14) contrôle de la qualité de l'eau ; (15) digues et contrôle de la quantité d'eau ;

IV. alimentation : (16) fourniture de nourriture - maintien de sa sécurité et de sa sûreté ;

V. santé : (17) soins médicaux et hospitaliers ; (18) médicaments, sérums, vaccins et produits pharmaceutiques ; (19) laboratoires et agents biologiques ;

VI. finances : (20) services et structures privés de paiement ; (21) finances publiques ;

VII. ordre public et sécurité : (22) maintien de l'ordre public, de la sécurité et de la sûreté ; (23) justice et administration pénitentiaire ;

VIII. administration civile : (24) fonctions gouvernementales ; (25) forces armées ; (26) services de l'administration civile ; (27) services d'urgence ; (28) services postaux et courrier ;

IX. transports : (29) transports routiers ; (30) transports ferroviaires ; (31) trafic aérien ; (32) transports fluviaux ; (33) transport maritime et cabotage ;

X. industrie chimique et nucléaire : (34) production et stockage / traitement de substances chimiques et nucléaires ; (35) canalisations de matières dangereuses (substances chimiques) ;

XI. espace et recherche : (36) espace ; (37) recherche.

Approche méthodologique : le cas français

En France, un texte législatif visait, dès 1958, la protection des installations d'importance vitale[2]. Étaient concernés les établissements, installations et ouvrages dont l'indisponibilité risquait de diminuer de façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation. Étaient également concernées les installations classées pour la protection de l'environnement dont la destruction ou une avarie présenterait un danger grave pour la population.

Reprenant ces deux dimensions d'activités d'une part, de protection de la population d'autre part, mais en adaptant leur champ aux attentes actuelles de la population en matière de sécurité globale, un nouveau texte réglementaire de février 2006 a défini le concept de « secteurs d'activités d'importance vitale »[3], dénomination préférée à celle d'infrastructures critiques ou d'infrastructures vitales.

[2] ordonnance n° 58-1371 du 29 décembre 1958 tendant à renforcer la protection des installations d'importance vitale, codifiée aux articles L. 1332-1 à L. 1332-7 du code de la défense, modifiés par la loi n° 2005-1550 du 12 décembre 2005 modifiant diverses dispositions relatives à la défense.

[3] décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.

Un secteur d'activités d'importance vitale est constitué d'activités concourant à un même objectif : activités ayant trait à la production et à la distribution de biens ou de services indispensables dès lors que ces activités sont difficilement substituables ou remplaçables, ou activités qui peuvent présenter un danger grave pour la population.

Le caractère indispensable est apprécié au regard de la satisfaction des besoins essentiels pour la vie de la population, de l'exercice de l'autorité de l'État, du fonctionnement de l'économie, du maintien du potentiel de défense ou de la sécurité de la nation.

Les conclusions du forum d'octobre 2003 sur les infrastructures critiques organisé par le Centre de politique de sécurité de Genève avait retenu la définition suivante : *« Les infrastructures critiques constituent des systèmes vitaux et des réseaux dont la dégradation porterait sérieusement atteinte au bon fonctionnement de la société »*. Le concept des secteurs d'activités que nous avons retenu en France est plus large et apparaît plus fécond : il part des finalités, c'est-à-dire de ce à quoi servent les infrastructures, pour dresser un inventaire aussi complet que possible des infrastructures qui y contribuent, en essayant de hiérarchiser leur contribution et donc les atteintes possibles en cas de dégradation.

Une liste de douze secteurs d'activités vient d'être arrêtée[4] : activités civiles de l'État ; activités judiciaires ; activités militaires de l'État ; alimentation ; communications électroniques, audiovisuel et information ; énergie ; espace et recherche ; finances ; gestion de l'eau ; industrie ; santé ; transports. A l'intérieur d'un secteur sont déterminés des sous-secteurs et des missions ou des enjeux de sécurité. Le secteur de l'alimentation regroupe ainsi les filières alimentaires essentielles (production des aliments de première nécessité), la distribution des produits alimentaires et la surveillance sanitaire des aliments ; le principal enjeu de sécurité en est la qualité sanitaire des produits alimentaires distribués. Le secteur de la santé recouvre la veille et la vigilance sanitaires, l'analyse et le diagnostic, l'organisation des soins et l'accueil des malades, les produits de santé ; les missions de ces sous-secteurs sont d'anticiper, de surveiller, d'alerter et d'évaluer les menaces sanitaires, d'assurer l'aide médicale urgente et d'organiser l'accueil des victimes et les soins, de produire, d'évaluer, de stocker et de distribuer les produits de santé. Sur ces critères sont ensuite analysés les systèmes de production des biens et des services, ce qui permet d'identifier les opérateurs et leurs moyens de production ; on aboutit alors aux infrastructures vitales, en ayant explicité les motivations de leur choix.

Le pilotage de chaque secteur d'activités est placé sous la responsabilité d'un ministre, qui bénéficie du concours des autres ministres concernés.

Pour chaque secteur d'activités sont définis des scénarios de menace pris en compte pour une analyse des risques. Sur la base de cette analyse, une directive nationale de sécurité définit des mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre toute menace, notamment à caractère terroriste.

En cohérence avec la directive du secteur concerné, chaque opérateur d'importance vitale élabore un plan de sécurité dont l'objet est de définir sa politique générale de protection pour ses établissements, installations et ouvrages, notamment pour ceux organisés en réseaux. Le plan comporte des mesures permanentes (le socle de protection, ou posture permanente de sécurité) et des mesures graduées activées en cas d'alerte transmise par l'autorité publique. L'opérateur détermine les points névralgiques de son système et les propose à l'administration pour classement en tant que points d'importance vitale. Pour chacun de ces points, il établit un plan de protection interne, découlant de son plan d'opérateur et donc cohérent avec la directive nationale de sécurité du secteur d'activités considéré ; ce plan comporte des mesures permanentes de

[4] arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs.

protection et des mesures graduées d'application temporaire, qui constituent la mise en oeuvre locale des mesures correspondantes du plan de sécurité de l'opérateur.

Ce dispositif associe l'État et les opérateurs : l'État détermine les secteurs d'activités, élabore les directives nationales de sécurité, et établit les plans de protection externe des points d'importance vitale. Chaque opérateur définit son plan de sécurité, sélectionne ses points d'importance vitale et établit leur plan de protection interne.

Du fait de la base juridique utilisée, l'ensemble des directives et des plans sont centrés sur la protection, c'est-à-dire fondamentalement sur la limitation des conséquences d'une menace, d'une agression malveillante ou d'un accident. Ce n'est qu'indirectement qu'ils traitent de la continuité des activités, dans la mesure où la continuité aura été considérée comme un critère d'organisation permettant de réduire les vulnérabilités.

En revanche, le thème de la continuité a trouvé toute sa place dans la préparation d'un plan gouvernemental de prévention et de lutte contre la pandémie grippale, entré en vigueur en janvier 2006. Il a été abordé de manière coopérative entre l'État et les opérateurs des secteurs d'activité d'importance vitale, les deux parties ayant un intérêt commun pour maintenir autant que possible l'ensemble des activités sociales et économiques tout au long de la phase pandémique si celle-ci se déclarait.

Approche fonctionnelle

Complétons cette approche méthodologique du cas français par une approche fonctionnelle.

La structuration du domaine revient à l'État, ce qui ne doit pas l'empêcher d'en discuter avec les opérateurs. Garant de l'intérêt général, l'État est légitime pour déterminer les secteurs d'activités d'importance vitale ou les infrastructures critiques fournissant les services essentiels à la vie de la population dans toutes ses composantes. D'un pays à l'autre, d'une région du monde à une autre, leur périmètre sera aménagé en fonction des traditions sociales, de l'organisation de l'État, de l'étendue du territoire, de choix politiques.

Nous avons vu à travers l'approche méthodologique française comment se construisait la planification. Évoquons maintenant cinq fonctions clés de la gestion de crise : la dissuasion, la prévention, la veille, la protection et la réaction.

La dissuasion, qui ne s'applique qu'aux actions malveillantes mais non aux risques naturels ou accidentels, a pour objectifs d'accroître le risque pour l'agresseur et de diminuer le profit qu'il pourrait tirer de son action. Cela passe par un régime de sanctions, reconnu internationalement dès lors que la zone d'intérêt d'une infrastructure dépasse les frontières d'un pays ou que les attaques peuvent être préparées et menées depuis l'étranger. A ce titre, on soulignera l'importance des conventions antiterroristes des Nations Unies : six de ces treize conventions (les quatre traitant du transport aérien[5], les deux traitant de la navigation maritime et des plateformes en mer[6]) visent directement la répression des actes terroristes commis contre des éléments d'infrastructures vitales. Citons également, dans le même ordre d'idée, la convention du Conseil de l'Europe sur la cybercriminalité (2001).

[5] convention relative aux infractions et à certains autres actes survenant à bord des aéronefs (1963) ; convention pour la répression de la capture illicite d'aéronefs (1970) ; convention pour la répression d'actes illicites dirigés contre la sécurité de l'aviation civile (1971) ; protocole pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale (1988).

[6] convention pour la répression d'actes illicites contre la sécurité de la navigation maritime (1988) ; protocole à la convention susmentionnée pour la répression d'actes illicites contre la sécurité des plateformes fixes situées sur le plateau continental (1988).

Deuxième fonction clé, la prévention vise à réduire les vulnérabilités de manière structurelle ou occasionnelle face à l'ensemble des risques. Elle se traduit par une organisation (par exemple, répartition d'installations plutôt que concentration, mise en place de redondances) ainsi que par des dispositions techniques réduisant l'exposition aux risques. Face aux agressions malveillantes, on peut y ajouter le renseignement qui cherchera à identifier l'agresseur potentiel pour le neutraliser avant qu'il commette une action. D'une certaine manière, des traités internationaux réglementant le droit de la guerre concourent à la prévention des actions contre les infrastructures vitales : traité de la Haye sur les règles de la guerre (1907), traité de la propriété culturelle (1954), protocoles additionnels à la convention de Genève (1977) sur la légalité d'emploi des armements et la protection des sites et des installations.

Troisième facteur clé, la veille a pour objet de détecter, de qualifier et d'alerter au plus tôt en cas d'incident ou d'événement perturbateur. Dans les grands organismes, elle est assurée par une cellule permanente où se retrouvent, à côté des divisions opérationnelles, les chaînes fonctionnelles de sécurité, de ressources humaines et de communication. La cellule de veille constitue le noyau du centre de crise activé dès que l'événement atteint un seuil d'alerte. Les cellules de veille travaillent fréquemment en réseaux géographiques ou thématiques, avec des moyens de liaison redondants aptes à résister aux dysfonctionnements qui affectent immédiatement les réseaux publics de télécommunication en cas de crise. Leur réactivité est particulièrement déterminante en cas d'agression sur les réseaux informatiques, qui ont la capacité de se propager quasiment instantanément sur toute la planète : en 2001, le virus informatique *Code Red* avait défrayé la chronique en infectant plus de 300 000 ordinateurs en 19 heures ; en 2003, *SQL Slammer* en avait infecté 75 000 en une demi-heure ; les méthodes d'attaque actuelles sont encore plus rapides et parviennent à ces scores en quelques minutes. Là encore, des instruments juridiques internationaux apportent des aides majeures : parmi les conventions antiterroristes des Nations Unies, retenons ici la convention sur le marquage des explosifs plastiques aux fins de détection (1991), tant les explosifs sont désormais utilisés pour détruire des installations critiques ; la convention ne couvre malheureusement pas les explosifs artisanaux, d'emploi désormais fréquent, dont les tentatives de fabrication pourraient être décelées à travers des produits chimiques précurseurs.

Quatrième fonction clé de la gestion de crise, la protection mobilise des dispositifs et des moyens visant à contenir une agression et à en limiter les effets. Elle comporte des mesures permanentes et des mesures temporaires, graduées en fonction du risque ou de la menace qui surgit.

Dernière fonction clé, la réaction comporte plusieurs volets : la neutralisation de l'agression, les secours aux victimes, la réduction de l'activité (résilience par passage du système en mode dégradé, ou reconfiguration par appel à des moyens de substitution), enfin la réparation et la restauration du système antérieur.

Les dispositions ne sont pas figées. Elles se nourrissent d'études renouvelées, d'enseignements tirés d'événements réels et d'exercices, de définition et d'échanges de bonnes pratiques. Les forums internationaux sont un moyen essentiel de progrès sur ces sujets complexes qui, délibérément ou non, lient les États entre eux. C'est dans de tels forums que se développent en particulier les coopérations techniques mais aussi les normes juridiques nécessaires à la prise en compte de la dimension nouvelle qu'apportent les infrastructures critiques, dont il est bon de rappeler l'objet fondamental : apporter les biens et les services essentiels à la vie de la population et de la société.