LA PROTECTION DES INFRASTRUCTURES CRITIQUES, L'ENJEU STRATÉGIQUE DU XXIe SIÈCLE

PAR

JEAN-FRANÇOIS DAGUZAN (*)

La protection des infrastructures critiques ne date pas du 12 septembre 2001. Dans les périodes de guerre ou de risque de guerre, cette question s'inscrivait dans la logique de la défense du territoire et, plus largement, de la défense civile. Il s'agissait alors de protéger les installations dites «sensibles» des risques de sabotage ou de destruction de la part de commandos spécialisés (les *spetnatz* soviétiques, commandos infiltrés, par exemple) ou de «cinquièmes colonnes» (membres de la population supposés ralliés à la partie adverse). Cette protection était assurée dans la plupart des pays à système de conscription par les forces armées, car la «main-d'œuvre» était abondante. En France, cette protection était assurée dans le cadre de la Défense opérationnelle du territoire (DOT). Des plans étaient prévus en période de montée de tension pour qu'une surveillance, le plus souvent statique, soit assurée par les armées. Ainsi, ouvrages d'arts, infrastructures de transports, établissements énergétiques (centrales, lignes à hautes tensions, dépôts de gaz ou de carburant), ministères, centraux téléphoniques, etc. étaient gardés par les troupes de réserves appuyées par des éléments professionnels de police et surtout de gendarmerie.

Avec la fin de la Guerre froide, la notion de défense du territoire perdit considérablement de sa vigueur. Les pouvoirs publics ne s'en désintéressèrent pas, mais l'effet psychologique lié à la disparition de la grande menace et l'émergence d'autres besoins furent déterminants. De plus, dans le même temps, les forces françaises furent amenées à intervenir de plus en plus souvent sur des théâtres d'opérations extérieures pour assurer le maintien ou le rétablissement de la paix. Pour de nombreux esprits, cette mission finit par devenir prédominante, voire exclusive. A bien des égards, en dépit de sa reconnaissance officielle, la défense du territoire fut ravalée au rang de mission subalterne. Bien évidemment, cette évolution n'a pas été spécifiquement française; elle fut commune à presque tous les pays européens. Aux Etats-Unis, le débat sur la *Homeland Defense* restait réservé à quelques

(*) Maître de recherche à la Fondation pour la recherche stratégique (FRS, France) et professeur associé à l'Université Panthéon-Assas (Paris II, France).

spécialistes, dont les plus engagés faisaient figure d'invétérés «*Cold Warriors*».

Cela ne veut pas dire que les pouvoirs publics soient restés les bras croisés après la fin de la Guerre froide, mais cette notion de «protection» qui, en France, a toujours été mise en avant dans les Livres blancs de la défense successifs définissant la doctrine officielle de la France a *de facto* occupé une position subalterne par rapport à de «nouvelles menaces» ou de nouvelles préoccupations, comme le maintien de la paix, les opérations extérieures, voire le soutien à l'action humanitaire.

L'electrochoc du 11 septembre 2001

Dès la seconde moitié des années 1990, la menace sérieuse d'Al Qaïda était connue. Cependant, personne ne pouvait imaginer *a priori* le niveau de destruction que ce groupe serait capable de mettre en œuvre.

Le président Clinton avait établi, en 1996, la Commission présidentielle pour la protection de l'infrastructure critique (President's Commission on Critical Infrastructure Protection ou PCCIP). Cette commission était chargée d'étudier les infrastructures essentielles qui constituent le soutien vital des Etats-Unis, de déterminer leur vulnérabilité et de proposer une stratégie pour les protéger. Dans son rapport de 1997, la commission soulignait que la protection de l'infrastructure vitale était une responsabilité qui incombait à la fois au secteur public et au secteur privé. En 1998, la Directive présidentielle sur la protection des infrastructures critiques (Presidential Decision Directive 63 on Critical Infrastructure Protection ou PDD 63), déclarait que les installations fédérales devraient être parmi les premières à adopter les meilleures pratiques, une gestion active des risques et l'amélioration de la planification de la sécurité.

La destruction des tours jumelles du World Trade Center et du Pentagone, puis les attaques à la maladie du charbon (Anthrax) en octobre et novembre 2001 aux Etats-Unis entraînèrent une prise de conscience brutale des faiblesses des sociétés technologiques et de leurs infrastructures. Les Etats revinrent donc à marche forcée vers la notion de «protection».

La National Strategy for Homeland Security publiée par la Maison-Blanche en juillet 2002 pose les infrastructures critiques au cœur des aires de mission critiques (Critical Mission Areas) à traiter en priorité (alerte et renseignement, sécurité des transports et des frontières, contre-terrorisme domestique, protection des infrastructures critiques et biens – clefs, défense contre des menaces catastrophiques et réponse et préparation à l'urgence) (1).

(1) White House, Office of Homeland Security, juil. 2002, 76 p.

En 2003, après la création du Department for Homeland Security, les Etats-Unis publiaient un texte majeur précisant la stratégie spécifique pour ce domaine : the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (désormais Key Resources). Ce texte met l'accent non seulement sur les destructions et pertes physiques potentielles, mais aussi sur les atteintes au prestige et au moral des Etats Unis par la destruction de cibles symboliques (comme la Statue de la liberté ou le monument du Mont Rushmore, par exemple).

En 2006, le Department of Homeland Security (DHS) a publié le nouveau National Infrastructure Protection Plan (NIPP) (2). Il définit les objectifs de préparation pour «prévenir, détecter et défaire les terroristes» mais aussi pour faire face aux désastres nationaux (naturels) – il s'agit d'une conséquence de la gestion désastreuse des effets de l'ouragan Katrina à La Nouvelle-Orléans et dans sa région.

La protection des infrastructures critiques en France

Deux critères majeurs sous-tendent la notion d'infrastructure critique en France : la notion de continuité de l'Etat et la sécurité du citoyen. Les deux sont indissociables mais elles ne s'exercent pas de la même façon.

Dans le cadre de la première, il s'agit de permettre à l'Etat de continuer de fonctionner en situation de crise majeure (pandémie grippale, par exemple) ou d'état de guerre. Les pouvoirs publics doivent donc être capables d'assurer un minimum acceptable de fonctionnement de communication, transports, énergie, moyens médicaux, sécurité de bâtiments publics, etc. afin de pouvoir faire porter son action sur la sécurité de la population. On part du principe que si l'Etat est défaillant, la première victime en est la population.

Dans le cadre de la seconde, il s'agit que le citoyen puisse en sécurité bénéficier des moyens de vie habituels : infrastructures de transport, de communication, de soins, d'énergie, etc.

De la notion d'infrastructures critiques à la notion d'infrastructures vitales

La notion d'infrastructure critique (*critical infrastructure*) est une notion américaine. La France parle d'«infrastructures vitales».

A partir de septembre 2001, la réflexion est conduite dans ce pays pour revoir la doctrine de protection des infrastructures et s'assurer de sa pertinence eu égard aux événements dramatiques survenus sur le territoire amé-

(2) *Cf.* le site Internet www.dhs.gov/xlibrary/assets/NIPP_Plan_ExecSumm.pdf.

ricain. Le fait qu'Al Qaïda menace globalement le monde occidental est pris très au sérieux. L'engagement de la France dans la campagne d'Afghanistan, ses liens traditionnels avec le Maghreb et le Proche-Orient en font une cible privilégiée des Islamistes radicaux qui n'avaient pas hésité à frapper sur son territoire ou à s'en prendre à ses ressortissants dès 1993 à l'occasion de la guerre civile algérienne. Par ailleurs, la catastrophe accidentelle de Toulouse du 12 octobre 2001, qui vit la dramatique explosion de l'usine de phosphates dans la banlieue toulousaine, obligea les pouvoirs publics à revoir encore plus précisément et de façon contraignante le statut des infrastructures et des établissements à caractères sensibles.

La circulaire du 14 février 2002 a précisé les responsabilités gouvernementales en la matière : «*En coordination avec le Secrétariat général de la défense nationale (SGDN) et en concertation avec les ministères de rattachement des opérateurs, le ministre chargé de l'Economie propose ou prend les mesures du niveau nécessaire – législatif, réglementaire, administratif ou contractuel – permettant d'assurer un fonctionnement adéquat des infrastructures vitales vis-à-vis de l'activité des entreprises, de la vie des populations, de la continuité de l'action gouvernementale et des services de sécurité des populations : lutte contre la malveillance et le terrorisme, sécurité informatique, fiabilité générale, résistance aux catastrophes naturelles ou technologiques. Ces opérateurs d'infrastructures vitales participent, à la demande des autorités administratives de tout niveau, aux instances de prévention, de préparation à la gestion de crise, voire à la gestion de la crise elle-même*» (3).

L'évolution significative des réformes de 2006

En 2006, l'Etat a remis à plat l'organisation de la protection des infrastructures vitales à partir de trois composantes : la définition de la notion d'infrastructure vitale et d'opérateur d'infrastructure vitale, la notion de zone d'importance vitale, la notion de responsabilité assortie de sanctions. La France, cette année-là, publiait pour la première fois de son histoire un Livre blanc du gouvernement sur la sécurité intérieure face au terrorisme (4). Ce livre faisait à la fois un état très lucide des menaces et précisait la doctrine française pour y répondre. La protection des infrastructures vitales y est particulièrement présente dans la section «Préserver l'intégrité du pays». Le gouvernement part du principe que les terroristes frappent plus là où ils le peuvent que là ou ils le veulent! Il s'agit donc de «durcir» les cibles pour les pousser à renoncer ou à réduire les effets de leurs actes.

«*Sont concernées au premier chef*», précise le document, «*les activités indispensables pour satisfaire les besoins essentiels de la population et au maintien*

(3) *Journal officiel*, n° 70, 23 mars 2002, p. 5 164, texte n° 10; circulaire du 14 février 2002 relative à la défense économique.

(4) *La France face au terrorisme*, La Documentation française, Paris, 2006, 141 p.

des capacités de sécurité et de défense du pays : l'alimentation, l'eau, l'énergie, les transports, les institutions financières, les systèmes d'information et de communication, les centres de décision et de commandement» (5).

La démarche française est décrite comme «*cohérente*» avec celle de l'Union européenne (6).

Le Secrétaire général de la défense nationale, Francis Delon, précisait cette nouvelle politique : «*la base de ce nouveau processus a été posée par le décret du 23 février 2006 relatif à la* sécurité des activités d'importance vitale*, qui réforme en profondeur le dispositif des points et des réseaux sensibles hérité de la Guerre froide. Dans chaque secteur d'activités essentielles à la vie nationale, une directive de sécurité analyse les risques à partir de scénarios fondés sur les analyses de renseignements; elle énonce des exigences de sécurité traduites en actions de réduction des vulnérabilités et en dispositions pratiques de protection, ventilées en une posture permanente de sécurité et en mesures graduées en fonction de l'intensité conjoncturelle de la menace. Une directive nationale de sécurité est un schéma directeur permettant à chaque opérateur du secteur de bénéficier des analyses nationales. L'opérateur complétera la démarche à son niveau en menant sa propre analyse de risque et en concevant un dispositif de sécurité à deux étages : un plan de sécurité pour l'ensemble de son activité dans le secteur traité et des plans de protection pour ses points névralgiques.*» (7)

Le contenu des dispositions de 2006

Que sont les «infrastructures vitales» ? :

L'article R. 1 332-1 du Code de la Défense précise que les opérateurs d'importance vitale sont désignés parmi : 1) les opérateurs publics ou privés mentionnés à l'article L. 1 332-1; 2) les gestionnaires d'établissements mentionnés à l'article L. 1 332-2.

Un opérateur d'importance vitale 1) exerce des activités mentionnées à l'article R. 1 332-2 et comprises dans un secteur d'activités d'importance vitale; 2) gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population

L'article R. 1 332-2 précise également qu'«*un secteur d'activités d'importance vitale, mentionné au 1° du II de l'article R. 1 332-1, est constitué d'acti-*

(5) *Id.*, p. 76.
(6) *Ibid.*, p. 77.
(7) *Défense*, n° 130, nov.-déc. 2007.

vités concourant à un même objectif, qui : 1 ont trait à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations; ou à l'exercice de l'autorité de l'Etat; ou au fonctionnement de l'économie; *ou au maintien du potentiel de défense*; *ou à la sécurité de la Nation, dès lors que ces activités sont difficilement substituables ou remplaçables*; 2 *ou peuvent présenter un danger grave pour la population*».

C'est le Premier ministre qui fixe, par arrêté pris après avis de la commission compétente, les secteurs d'activités d'importance vitale. Cet arrêté désigne pour chaque secteur d'activités d'importance vitale un ministre coordonnateur.

Responsabilités et sanctions : tout repose sur l'opérateur

L'article L. 1 332-1 précise que les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation sont tenus de coopérer à leurs frais, dans les conditions définies dans le chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.

La loi française ne se contente pas de fixer des obligations au propriétaire ou à l'opérateur d'infrastructures vitales. Elle assortit le non-respect de son exécution de sanctions très lourdes. L'article L. 1 332-7 précise ainsi que : «*est puni d'une amende de 150 000 euros le fait, pour les dirigeants des opérateurs mentionnés à l'article L. 1 332-4 et à l'expiration du délai défini par l'arrêté de mise en demeure, d'omettre d'établir un plan de protection ou de réaliser les travaux prévus. Est puni d'une amende de 150 000 euros le fait, pour les mêmes personnes, d'omettre, après une mise en demeure, d'entretenir en bon état les dispositifs de protection antérieurement établis*».

La notion de «zone d'importance vitale»

L'article R. 1 332-35 stipule que «*lorsque dans une zone géographique continue sont implantés plusieurs points d'importance vitale relevant d'opérateurs différents et interdépendants, le préfet du département dans le ressort duquel se situe cette zone peut la désigner zone d'importance vitale, par arrêté pris après avis de la commission mentionnée à l'article R. 1 332-13*».

Ces nouvelles dispositions permettent aux pouvoirs publics de globaliser la notion d'infrastructure vitale et d'envisager des plans communs et des obligations communes aux opérateurs.

L'organisation de la protection des infrastructures vitales

L'organisation de la protection des infrastructures vitales relève du Secrétariat général de la défense nationale (SGDN), qui dépend du Premier ministre. La mission du SGDN est de veiller à l'information du Premier ministre dans tous les domaines touchant à la défense et la sécurité nationale – y compris les risques et menaces économiques, industriels et technologiques. Il assure également le secrétariat des Conseils de défense – qui prépare pour le Président de la République les grandes orientations de la défense de la nation –, la coordination du renseignement, le secrétariat des organes de contrôle des exportations d'armement et de technologies sensibles. Son action la plus importante, pour ce qui nous occupe, est d'établir la doctrine de protection et de sécurité de l'Etat et des populations et d'en préparer les plans. Cette tâche relève, au sein du SGDN, de la Direction de la protection et de la sécurité de l'Etat (DPSE).

La DPSE veille à la protection et à la sécurité des populations sur le territoire. Ses trois missions principales sont : la préparation de l'Etat aux risques et aux menaces majeurs; la protection du secret de défense et des documents classifiés; la sécurité des réseaux et des transmissions gouvernementales.

Le SGDN assure alors l'analyse du risque et la planification des mesures de prévention et d'intervention face à la menace terroriste (plan Vigipirate et famille des plans Pirate Biotox, Piratox, Piratom (8)) et en suit l'application; il anime également la Commission interministérielle de défense et de sécurité des secteurs d'activités d'importance vitale.

Depuis la création du Comité interministériel aux crises nucléaires et radiologiques par décret du 8 septembre 2003, le SGDN, qui en assure le secrétariat, est également chargé de la mise en cohérence des mesures interministérielles planifiées en cas d'accident ou d'attentat dans le domaine nucléaire et radiologique. Il anime plus généralement de nombreux travaux interministériels relatifs à la protection contre les risques et les menaces nucléaires, radiologiques, biologiques et chimiques (NRBC) : traitement des plis et colis suspects, définition d'une doctrine de secours face à un attentat, renforcement de l'équipement spécialisé. Face à l'accroissement du risque sanitaire, il est également en charge de l'élaboration du plan «Pandémie grippale».

(8) Le plan Biotox concerne le risque d'attentats biologiques, le plan Piratox le risque d'attentat chimique et les accidents industriels, enfin, le plan Piratom concerne une attaque utilisant des moyens nucléaires ou visant une centrale nucléaire. Il existe aussi désormais un plan Piratmer qui prend en compte une menace venant de l'arraisonnement d'un navire portant des matières dangereuses par des terroristes. Le plan Vigipirate porte sur la protection des infrastructures (notamment de transport) et les points dits sensibles. Le niveau d'alerte, qui va du vert à l'écarlate, détermine le niveau de protection. Les forces armées sont associées à la surveillance des infrastructures.

Chaque ministère dans son domaine de compétence est chargé de l'application de ces plans et de leur menée à bonne fin. Le ministère de l'Intérieur a en particulier la responsabilité de la gestion opérationnelle des plans de crise.

Le nouveau Président de la République, Nicolas Sarkozy, a souhaité, dès son élection, la révision complète de la politique de défense et de sécurité de la France. Un nouveau Livre blanc sur la défense et la sécurité nationale a été mis en chantier (9). Il a été porté à la connaissance du public le 17 juin 2008 (10). Il met en évidence beaucoup plus que par le passé la notion de protection. Celle-là avait été un peu négligée dans le Livre blanc de 1994, à un moment où on trouvait les grandes menaces sur le territoire national révolues. Elle redevient une des fonctions majeures avec, au cœur, la notion de résilience; c'est-à-dire la capacité, pour une société, de faire face à des agressions très importantes et d'en ressortir plus forte.

La protection des infrastructures vitales dans le Livre blanc du 17 juin 2008

Ce sont de considérables évolutions – pour ne par dire révolutions – qui apparaissent dans la nouvelle version du Livre blanc pour la défense et la sécurité publié récemment. D'abord, il faut noter le continuum défense et sécurité, qui n'existait pas vraiment avant, et, pour ce qui nous occupe ici, la prise en compte, avec les menaces, des risques liés aux catastrophes naturelles (le tsunami ou la pandémie grippale par exemple) et industrielles (AZF) et des actes de terrorismes.

Ces évolutions se traduisent par des changements fonctionnels importants, touchant entre autres les organes chargés de la protection des infrastructures vitales : «*le Secrétariat général de la défense nationale évoluera en un Secrétariat général de la défense et de la sécurité nationale, placé auprès du Premier ministre et travaillant en étroite liaison avec la Présidence de la République. Chargé de la préparation et du suivi des décisions prises par le Conseil de défense et de sécurité nationale, ce secrétariat général garantira les conditions du dialogue interministériel et l'expression, comme la présentation au chef de l'Etat et au Premier ministre, des points de vue éventuellement contradictoires.* [...] *Celui-ci coordonnera la préparation et s'assurera de la mise en œuvre des mesures concourant à la stratégie de sécurité nationale, par exemple la préparation aux crises majeures.* [...] *Le ministre de l'Intérieur*

(9) Il ne doit pas être confondu avec le Livre blanc du gouvernement sur la sécurité intérieure face au terrorisme de 2006. Le Livre blanc sur la défense et la sécurité nationale succède aux deux Livres blanc de la défense parus respectivement en 1972 et en 1994. Il s'agit d'un ouvrage doctrinal majeur, qui engage en principe la France pour plusieurs dizaines d'années. La «révolution» pour ce dernier est l'adjonction du mot «sécurité» à côté du mot défense.

(10) *Livre blanc sur la défense et la sécurité nationale*, Odile Jacob, Paris, 2008.

coordonne en particulier la gestion des crises sur le territoire national ainsi que le renseignement intérieur. Son action s'appuie sur les préfets de département et de zone de défense et de sécurité, qui sont, aux termes de l'article 72 de la Constitution, les représentants de chacun des membres du gouvernement et ont la charge des intérêts nationaux, du contrôle administratif et du respect des lois» (11).

La protection des infrastructures vitales

Contrairement au Livre blanc de 1994, le Livre blanc 2008 prend en compte de façon explicite et détaillée la protection des infrastructures vitales : «*Protéger les infrastructures vitales. La politique de sécurité des activités d'importance vitale lancée en 2006 sera poursuivie énergiquement. Elle vise, pour douze secteurs d'activité définis, à évaluer et hiérarchiser les risques, puis à élaborer les mesures pour y faire face. L'un de ses objectifs essentiels est de déterminer les sites névralgiques, sur lesquels les efforts de protection les plus significatifs devront être faits dès les prochaines années, d'abord par les opérateurs, puis avec les moyens de l'Etat si nécessaire*».

Secteurs d'activité d'importance vitale

(arrêté du 2 juin 2006)

Activités civiles de l'Etat – Activités judiciaires – Activités militaires de l'Etat – Alimentation – Communications électroniques, audiovisuel et information – Energie – Espace et recherche – Finances – Gestion de l'eau – Industrie – Santé – Transports.

«*Nombre d'infrastructures majeures, en particulier celles de transport d'énergie, d'informations et de marchandises, sont transnationales. Leur sécurité doit être appréhendée de manière cohérente par les Etats et les opérateurs concernés. A cet effet, l'approche française des secteurs d'activité d'importance vitale sera présentée à nos partenaires européens afin de faire déboucher les initiatives lancées par l'Union européenne sur l'établissement de principes communs pour l'organisation de la protection des infrastructures vitales et sur un partage des meilleures pratiques*» (12).

La protection des infrastructures vitales énergétiques

Il n'y a pas, en France, de doctrine spéciale concernant la protection des infrastructures vitales énergétiques. Celles-là sont considérées comme faisant partie d'un «tout» doctrinal et l'Etat est censé répondre aux agressions qui les menacent comme il répondrait à celles visant d'autres secteurs «vitaux». On se souvient dans ce pays que, lors de la guerre d'Algérie, entre 1954 et 1962, presque tous les dépôts de carburants et de gaz furent atta-

(11) *Ibid.*, pp. 253-254 et 258.
(12) *Ibid.*, pp. 187-188.

qués à un moment ou un autre. De plus, les guerres du Caucase et d'Iraq ont montré que les oléoducs et gazoducs étaient des cibles accessibles. Cela étant, il y a évidemment, dans le cas français, une prise de conscience aiguë de la spécificité nucléaire française.

Il existe donc des procédures spéciales visant à la sécurité des centrales au sens général. En cas d'incident, des plans départementaux d'urgence existent et sont rodés par de nombreux exercices. En matière terroriste, le plan Piratom cité précédemment est mis en œuvre en cas d'incident nucléaire volontaire (bombe radiologique, par exemple) et implique des unités spécialisées dans le désamorçage d'engins comme le Raid/DCI (13), dépendant du ministère de l'Intérieur, ainsi qu'une gendarmerie «nucléaire» chargée de la sécurité des armes et des centrales.

Les infrastructures énergétiques autres que nucléaires voient leur sécurité assurée dans le cadre des plans évoqués plus haut. La responsabilité de l'opérateur est partagée – moyens humains, moyens physiques et informatiques –, selon les missions, avec celle du préfet du département qui représente l'Etat.

Aujourd'hui, parmi les évolutions notables sur lesquelles l'effort portera prioritairement figure la cyber-sécurité. Il s'agit de se prévenir la menace d'attaques informatiques contre les systèmes centraux de management des infrastructures vitales. Le Livre blanc met l'accent là-dessus. On peut imaginer ce qui se passerait en cas de dysfonctionnement d'une tour de contrôle d'un grand aéroport par exemple.

La protection des infrastructures vitales au niveau de l'Union européenne : ambitions communautaires et réserves nationales

Les propositions de la Commission de décembre 2006 s'attachent à promouvoir un programme européen de protection des infrastructures vitales (EPCIP ou PEPIC), comme par exemple l'approvisionnement en énergie. Cela a permis l'adoption de conclusions par le Conseil Justice et Affaires intérieures, les 19 et 20 avril 2007, qui soulignent l'importance de la protection des infrastructures vitales et constituent une première prise de position du Conseil vis-à-vis des propositions de la Commission.

Le but de la démarche de la Commission est d'établir des procédures communes en matière de recensement et de classement par les Etats membres des infrastructures critiques situées sur leur territoire, ainsi qu'un

(13) Rattaché au groupe d'intervention de la Police nationale (RAID), le détachement central d'intervention est chargé de la localisation, de l'identification, du diagnostic et de la neutralisation d'engins nucléaires, radiologiques, biologiques ou chimiques improvisés; il regroupe les unités spécialisées de divers ministères. *Cf. La France face au terrorisme*, *op. cit.*, p. 84.

cadre commun permettant d'évaluer la nécessité de renforcer leur protection. Les ICE sont «*les infrastructures critiques dont l'arrêt ou la destruction pourrait avoir une incidence grave sur deux ou plusieurs Etats membres ou un seul, s'il s'agit d'un Etat membre autre que celui dans lequel l'infrastructure critique est située*». La directive présente une liste provisoire de onze secteurs d'infrastructures critiques – dont l'énergie – divisés en 29 sous-secteurs.

Le programme européen de protection des infrastructures critiques identifie les secteurs d'infrastructures critiques européennes de la manière suivante : Energie; Installations nucléaires; Technologies de l'information et de la communication; Eau; Alimentation; Santé; Finances; Transports; Industrie chimique; Espace; Laboratoires de recherche.

Partant de ce document, une autre Communication, de février 2007, sur la protection des infrastructures critiques européennes dans les secteurs de l'énergie et du transport proposait des critères pour recenser les infrastructures critiques dans ces deux secteurs. En outre, le Livre vert sur l'énergie de la Commission européenne de mars 2006 désigne également la sécurité de l'approvisionnement comme l'un des objectifs d'une stratégie européenne en matière d'énergie. La Commission propose notamment d'établir un Observatoire européen de l'approvisionnement énergétique pour définir les vulnérabilités des infrastructures et un Centre européen pour les réseaux énergétiques pour favoriser l'échange des informations et la création de normes communes pour les infrastructures énergétiques.

Dans le Livre vert sur les infrastructures critiques publié le 24 novembre 2005, la Commission aborde des questions essentielles comme la protection que devrait offrir le Programme européen de protection des infrastructures critiques (PEPIC), la définition des notions d'«infrastructure critique européenne» et d'«infrastructure critique nationale», ainsi que le rôle des propriétaires et des opérateurs d'infrastructures.

Le PEPIC inclurait alors une directive du Conseil portant sur l'identification et la désignation des infrastructures critiques, ainsi qu'un recensement des besoins pour améliorer leur protection. La directive met en place une procédure pour identifier et désigner ces infrastructures, ainsi qu'une approche commune pour en améliorer la protection selon les besoins recensés. Le PEPIC comporterait aussi des mesures destinées à faciliter sa mise en place, incluant un plan d'action sur le PEPIC, un réseau d'alerte concernant les infrastructures critiques, des groupes d'experts identifiant et étudiant les interdépendances. Il prévoirait également un soutien communautaire aux infrastructures critiques nationales des Etats membres. Sont en outre intégrées dans le PEPIC des mesures financières d'accompagnement, notamment à travers le programme européen proposé pour la période 2007-2013 – «La lutte contre le terrorisme : préparation et gestion des conséquences et autres risques liés à la sécurité» –, qui permettront d'accorder un

financement communautaire aux projets portant sur les infrastructures critiques et potentiellement utiles au niveau européen

Ces propositions, en apparence neutres, posent un certain nombre de problèmes politiques et rencontrent de ce fait les réticences, voire l'hostilité, de certains Etats membres. En effet, la notion d'infrastructure critique ou vitale européenne pose le problème du contrôle de sa sécurité. Or, des Etats membres n'envisagent pas de partager la sécurité d'infrastructures considérées comme stratégiques – on peut penser au nucléaire, mais cela va beaucoup plus loin; les centraux de communication et d'information également.

L'ECHELON INTERNATIONAL : UN CONSENSUS POUR DES ACTIONS SIGNIFICATIVES

Le G8 : un précurseur dans la prise de conscience

Depuis 2003, les dirigeants du G8 attachent un intérêt tout particulier à la protection des infrastructures vitales, notamment des infrastructures énergétiques.

La réunion des chefs d'Etat et de gouvernement du G8 d'Evian, les 2-3 juin 2003, a permis de mettre l'accent sur la protection des infrastructures vitales, en insistant sur celles d'information et de communication et en édictant un ensemble de «principes». Le texte adopté met solennellement en évidence une obligation à la fois individuelle et collective d'action et de coopération : «*les infrastructures d'information et de communication constituent une part essentielle des infrastructures vitales. En conséquence, afin de protéger efficacement leurs infrastructures vitales, les Etats doivent protéger leurs infrastructures vitales d'information et de communication d'éventuels dégâts et les sécuriser face aux risques d'agression. Une protection efficace des infrastructures vitales comprend l'identification des menaces contre ces infrastructures, la réduction de leurs vulnérabilités aux dommages et aux attaques, la minimisation des dégâts et de temps de restauration en cas de dommages ou d'attaque, et l'identification de l'origine des dégâts ou de la source de l'attaque en vue de leur analyse par des experts et/ou de leur investigation par les services judiciaires. Une protection efficace exige aussi communication, coordination et coopération, nationales et internationales, entre toutes les parties prenantes – industriels, universitaires, secteur privé et structures administratives, mais aussi services de protection des infrastructures et services de police. De tels efforts doivent être entrepris avec un respect évident de la sécurité des informations et de la législation relative à l'assistance mutuelle et à la protection de la confidentialité*».

A Heiligendamm, en Allemagne, le 6 juillet 2007, les chefs d'Etat et de gouvernement sont revenus sur la nécessité de protéger les infrastructures énergétiques : «*étant donné la nature transnationale des infrastructures éner-*

gétiques, aucun pays ne peut s'isoler d'un risque de dangereuse rupture d'approvisionnement. Nous sommes résolus à poursuivre nos efforts pour protéger les infrastructures énergétiques vitales contre des attaques terroristes. Au Sommet de Saint-Pétersbourg (15-17 juillet 2007), nous avions pris l'engagement d'assurer la sécurité du réseau énergétique dans le monde, de mieux comprendre les faiblesses de ce réseau et de définir la manière dont nous pouvons agir pour prévenir les ruptures d'approvisionnement qui résulteraient d'attaques délibérées contre lui. Nous avons chargé des experts nationaux d'élaborer des recommandations afin de lever les obstacles à la sécurité des infrastructures énergétiques vitales. Nous annonçons aujourd'hui les initiatives que nous prenons à ce sujet : évaluer les faiblesses des infrastructures énergétiques vitales et les risques potentiels auxquels elles sont exposées; échanger les bonnes pratiques pour des réponses efficaces en matière de sécurité; évaluer les menaces potentielles pesant sur les infrastructures énergétiques vitales».

Les autres organisations

Presque toutes les organisations internationales s'intéressent désormais, de près ou de loin, à la protection des infrastructures critiques (ONU, OCDE, Banque mondiale, etc.). Plus près de nous, certaines essaient de développer des stratégies plus particulièrement tournées vers les infrastructures critiques énergétiques.

L'Otan

Au Sommet de Riga en 2006, les chefs d'Etat et de gouvernement ont plaidé en faveur d'un «*effort international concerté afin d'évaluer les risques auxquels sont confrontées les infrastructures et de promouvoir la sécurité de ces infrastructures*» et ont chargé le Conseil de l'Atlantique-Nord (CAN) de définir «*les domaines dans lesquels l'OTAN peut apporter une valeur ajoutée s'agissant de préserver les intérêts des Alliés en matière de sécurité*». Ce regain d'intérêt pour la sécurité énergétique a également été intégré dans la Directive politique globale adoptée à Riga, qui mentionne «*l'instabilité due* [...] *à la perturbation des approvisionnements en ressources vitales*» comme l'un des principaux risques et défis auxquels l'Alliance sera confrontée dans les dix ou quinze prochaines années.

Suite à cette demande, le Conseil a préparé un rapport sur «Le rôle de l'OTAN en matière de sécurité énergétique», recommandant des principes et des domaines d'intervention de l'OTAN. Les chefs d'Etat et de gouvernement ont pris note de ce rapport lors du Sommet de Bucarest en avril 2008 et ont adopté une liste de domaines dans lesquels l'OTAN devrait s'investir, notamment «*la fusion et le partage des informations et du renseignement, la projection de la stabilité, la promotion de la coopération internationale et*

régionale, le soutien à la gestion des conséquences et le soutien à la protection des infrastructures énergétiques essentielles». Ils ont par ailleurs chargé le Conseil de préparer un rapport de synthèse sur les progrès accomplis dans le domaine de la sécurité énergétique, lequel sera soumis en 2009 au Sommet du soixantième anniversaire de l'OTAN.

L'OSCE

L'OSCE s'est très tôt sentie concerné par la protection des infrastructures énergétiques. De fait, son engagement dans la sécurité des Balkans et du Caucase lui a donné une sensibilité particulière dans ce domaine. La décision n° 6/072007 du Conseil ministériel précise que les Etats membres de l'organisation sont «*conscients que les infrastructures énergétiques vitales, notamment les centrales nucléaires, les barrages des centrales hydroélectriques, les installations de production de pétrole et de gaz, les raffineries, les installations de transmission, les voies et les installations d'approvisionnement, les installations de stockage d'énergie ainsi que les installations de stockage de déchets dangereux, peuvent être vulnérables à une attaque terroriste; Désireux d'appuyer la mise en œuvre du Plan d'action du G8 sur la sécurité énergétique mondiale adopté à Saint-Pétersbourg en 2006, qui promeut la coopération internationale pour remédier aux menaces et aux vulnérabilités qui pèsent sur les infrastructures énergétiques vitales*».

Dans ce cas particulier, tout est une question de moyens. Pour des Etats fragiles ou en reconstruction, la coopération internationale est indispensable tant en termes de moyens financiers que de soutien en formation et, évidemment, en renseignement. La route est encore très longue pour parvenir à une véritable efficacité.

* *
*

Derrière les progrès, un long chemin a parcourir

En 2003, le forum sur les infrastructures critiques du Centre de politique de sécurité de Genève donnait les conclusions suivantes : «*la protection des infrastructures critiques nécessitera un changement de perception et la création d'une 'culture du risque'. Les systèmes de protection civile devraient être placés au niveau des systèmes de défense traditionnels. Les autorités devraient adopter une attitude dynamique, être capables de 'penser de façon différente' et de penser même 'l'impensable'. Cette culture de sécurité devrait prendre en compte non seulement les plus grands réseaux mais aussi les petites et moyennes entreprises*» (14).

(14) *Forum on critical infrastructure*, Genève, 28-29 oct. 2003, p. 41.

Désormais, les infrastructures critiques ou vitales ont été globalement cernées. On considère que les infrastructures se retrouvant sur toutes les listes sont : la banque et la finance; les centres gouvernementaux et les ministères; les centres d'information et de télécommunication; les services d'urgence; les infrastructures énergétiques et d'électricité; les services de santé, les services de transport, logistique et de distribution, ainsi que les services hydrauliques (15). Les Américains y rajoutent les grands monuments (infrastructures symboliques). En revanche, la façon de protéger n'est pas la même pour tous. Cela étant, là aussi, la tendance à renvoyer la responsabilité vers les opérateurs se généralise. Cette tendance est liée aussi à la réduction des moyens financiers des Etats. Enfin, une approche supranationale de protection des infrastructures vitales est loin de faire l'unanimité. Les réticences aux efforts de la Commission pour une approche communautaire de cette notion le montrent aisément. Pour dépasser les réserves nationales, il faudra être capable de démontrer la réalité d'une véritable subsidiarité en la matière.

Beaucoup a été fait depuis, en France tout du moins, avec le nouveau Livre blanc, le niveau de préoccupation de sécurité des infrastructures vitales a rejoint celui des autres systèmes. En revanche une «culture de sécurité» généralisée est loin d'être atteinte. On est encore beaucoup trop dans l'application de plans que dans l'appropriation par les opérateurs.

Une tendance apparaît par ailleurs problématique. L'Etat tend de plus en plus à faire peser la responsabilité de la sécurité aux opérateurs. L'Etat édicte des règles et l'opérateur est censé les appliquer sous peine de sanctions. Le risque est que, d'un côté, l'Etat se satisfasse d'empiler des réglementations de plus en plus contraignantes en ayant le sentiment du devoir accompli et que, de l'autre, l'opérateur mette en place – au prix fort puisqu'il n'a pas le choix – des pratiques plus formelles qu'opérationnelles ou réellement efficaces. Au bout de la chaîne, l'usager en paie le prix financier et en contraintes de tous ordres.

Il faudra à un moment rééquilibrer la relation public-privé. Il faudra aussi trouver l'équilibre de subsidiarité entre l'Union européenne et les Etats membres.

(15) Isabelle Abele-Wigert & Myriam Dunn An inventory fo 20 national and 6 international critical information infrastructure protection policy, *International CIIP Handbook 2006,* Center for Security Studies, ETH Zurich.