Vulnérabilité et résilience des réseaux face aux risques naturels

Par Laurent WINTER *

Plusieurs grandes catastrophes naturelles survenues récemment en Europe et dans le monde ont mis en lumière la vulnérabilité des sociétés modernes aux phénomènes naturels de grande intensité, le développement technologique et l'interdépendance entre réseaux pouvant constituer à cet égard des facteurs aggravants. Les pouvoirs publics, qui ont jusqu'ici privilégié une approche par la limitation des droits à construire, et les opérateurs de réseaux ont pour mission d'assurer dans les situations de crise la satisfaction des besoins essentiels de la population et la reprise la plus rapide possible de l'activité économique, éventuellement en mode dégradé. Or, si certains risques « classiques » (comme les inondations et les séismes) sont maintenant bien pris en compte par les acteurs, des perturbations climatiques croissantes en fréquence et en intensité (tempêtes, précipitations abondantes, températures extrêmes) constituent autant de risques émergents face auxquels les stratégies de résilience restent à être affinées. En outre, l'évaluation socio-économique des programmes de résilience appelle des approfondissements.

Les grandes catastrophes récentes – séisme de Kobé (Japon, janvier 1995), ouragan Katrina (Louisiane, États-Unis, août 2005), tsunami et accident nucléaire de Fukushima (Japon, mars 2011), ouragan Sandy (New York et New Jersey, États-Unis, octobre 2012)... – ont mis en lumière la vulnérabilité des grandes agglomérations et des technologies modernes pourtant réputées les mieux sécurisées vis-à-vis des aléas naturels, et ont suscité un regain d'intérêt de la part du public pour les notions de « vulnérabilité » et de « résilience », au-delà des cercles étroits des seuls experts.

Aussi, est-il surprenant que les conséquences de ce type d'événements (ou d'événements de moindre gravité, comme les tempêtes de décembre 1999 en Europe occidentale) sur les réseaux de transport et de distribution d'énergie, d'eau, de transports de personnes et de marchandises... n'aient toujours pas donné lieu, à ce jour, à une revue d'ensemble, en France en tout cas.

Les quelques études réalisées jusqu'ici n'ayant porté que sur des réseaux particuliers (télécommunications, distribution électrique), il est apparu utile au Conseil général de l'Environnement et du Développement durable (CGEDD) de procéder à une revue plus large (sans prétendre à l'exhaustivité) portant sur un ensemble de réseaux « structurants », tant du point de vue de l'activité économique que de celui des services essentiels à apporter à la population et relevant du périmètre de compétence du ministère de l'Écologie, du Développement durable et de l'Énergie (MEDDE). En outre, une telle démarche plus globale doit permettre de faire apparaître des interactions croisées entre réseaux différents et des risques de défaillances en cascade. Bien que cette revue ne soit pas totalement finalisée au moment de la rédaction du présent article, il est toutefois possible d'en tirer d'ores et déjà quelques enseignements.

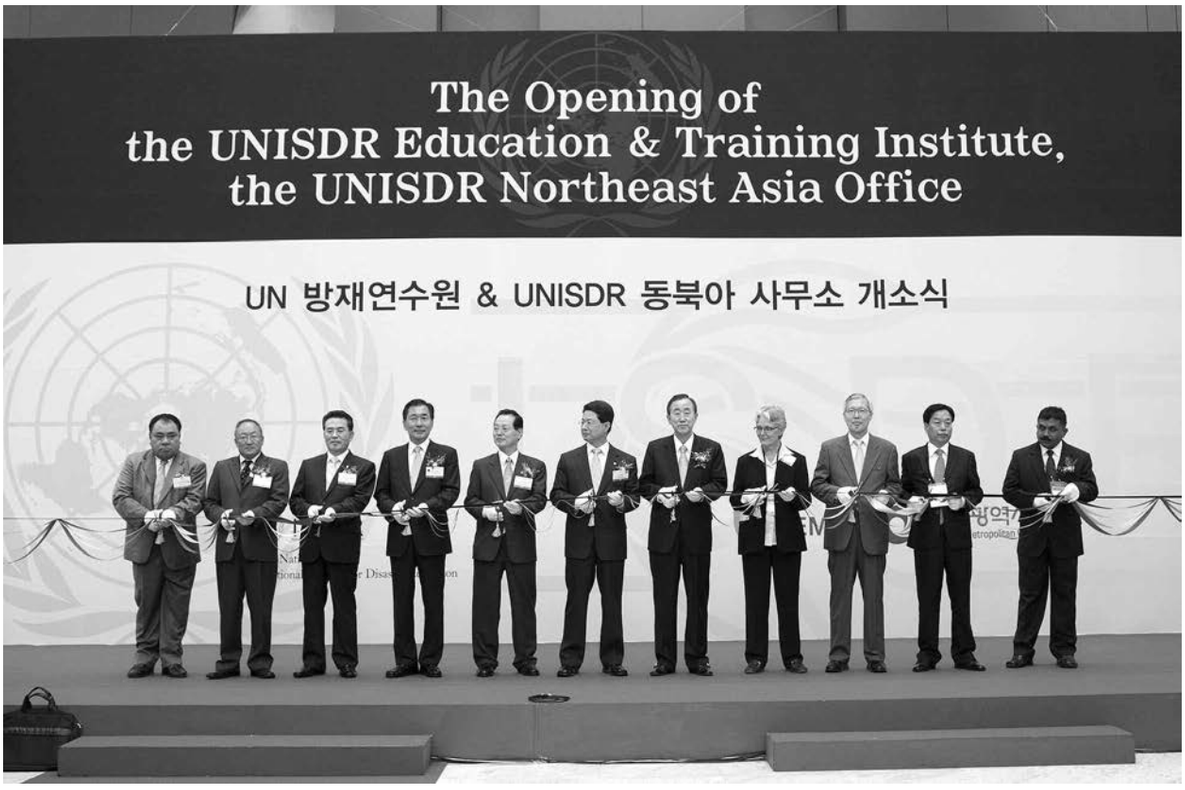
La variété des définitions des concepts de vulnérabilité et de résilience

En premier lieu, les concepts de vulnérabilité et de résilience ont reçu différentes définitions. Les définitions les plus fréquemment utilisées de ces concepts sont celles qu'en donne la norme ISO 73 :

« Vulnérabilité : propriété intrinsèque de quelque chose constituant une source de risque pouvant induire une conséquence ».

« Résilience : capacité d'adaptation d'un organisme dans un environnement complexe et changeant ».

Plus récemment (2009), l'UNISDR (1) a donné de nouvelles définitions de ces concepts.



© Eskinder Debebe / UN Photo

« Plus récemment (2009), l'UNISDR a donné d'autres définitions des concepts de vulnérabilité et de résilience ». Le Secrétaire général de l'ONU, Ban Ki-Moon, inaugurant l'Institut de formation de l'UNISDR pour l'Asie du Nord-Est, Incheon (Corée du Sud), août 2009.

Le droit applicable en la matière émane de sources juridiques nationales et communautaires

Alors que les catastrophes naturelles et leurs effets sur les territoires et sur les réseaux d'infrastructures ont longtemps été considérés comme des fatalités, les crues de très grande ampleur de l'Elbe et du Danube (en août 2002), qui ont affecté plusieurs pays d'Europe centrale ou orientale, ont fourni à la Commission européenne l'occasion de se saisir de la question et de proposer un nouveau paradigme face à un risque d'inondation dépassant les frontières nationales.

Selon ce paradigme énoncé dans la directive « inondations » 2007/60/CE du 23 octobre 2007, qui est, depuis mars 2011, entièrement transposée dans le droit français (Code de l'environnement et Code de l'urbanisme), il appartient à chaque État membre d'élaborer une stratégie nationale contre les inondations et de conduire une démarche préventive en trois étapes (évaluation préliminaire des risques d'inondation, établissement de cartes de risques et de plans de gestion des risques) qui conduit à un zonage des territoires à risque identifié. L'engagement de la solidarité de l'Union européenne envers un État membre touché par une inondation est conditionnée par la mise en œuvre progressive par celui-ci de cette stratégie de résilience.

Dans les zones à risques, qui doivent à terme être couvertes exhaustivement par des plans de gestion des risques d'inondation (PGRI), les autres documents d'urbanisme (ScoT (schéma de cohérence territoriale), PLU (plan local d'urbanisme)) doivent être mis en conformité avec ces PGRI. Toutefois, la transposition de la directive précitée dans le droit national français a porté prioritairement sur l'urbanisme et la construction, les réseaux d'infrastructures n'ayant pas fait l'objet de dispositions spécifiques.

De la même manière, le Code de l'environnement prescrit pour l'ensemble des risques naturels prévisibles (dont il donne une liste non exhaustive) l'établissement de plans de prévention des risques naturels prévisibles (PPR). Il s'agit là encore d'un zonage assorti de règles d'urbanisme restrictives en fonction des risques identifiés ; les réseaux et les ouvrages ne font pas davantage l'objet d'un traitement particulier. La liste des risques naturels (2) ne mentionne pas certains risques pourtant récurrents et à forte incidence sur le fonctionnement de certains réseaux, comme les chutes de neige ou les températures extrêmes.

Le Code de la sécurité intérieure, dans ses articles L. 732-1 et L. 732-2, fait une mention explicite des réseaux répondant aux besoins prioritaires de la population qu'il est impératif de satisfaire en temps de crise. La loi cite ainsi *« les exploitants d'un service, destiné au public, d'assainissement, de production d'eau pour la consommation humaine, d'électricité ou de gaz, ainsi que les opérateurs de*

réseaux de communications électroniques ouverts au public », auxquels elle enjoint de prendre les mesures nécessaires afin de faire face aux besoins prioritaires de la population dans des situations de crise. On relèvera que les réseaux de transport de personnes (routes, réseaux ferrés, voies d'eau, ports et aéroports) ne figurent pas dans cette liste.

L'organisation des pouvoirs publics en cas de crise répond au principe de subsidiarité

Chaque échelon territorial gère la crise à son niveau, ne faisant appel à l'échelon immédiatement supérieur que lorsque l'envergure de la crise excède les limites de son territoire. Cette organisation *bottom up* vise, en priorité, à protéger les populations et à satisfaire leurs besoins essentiels et, secondairement, à assurer la continuité des activités économiques. Elle part de la commune, dont le maire établit le plan communal de sauvegarde (PCS), et remonte dans les échelons territoriaux successifs :

- ✔ le préfet, à l'échelon départemental, qui s'appuie sur son directeur de cabinet et sur le Service interministériel des Affaires civiles et économiques de défense et de la Protection civile (SIACEDPC),
- ✔ le préfet de zone de défense et de sécurité (ZDS), qui s'appuie sur le délégué ministériel de zone (la Direction régionale de l'Environnement, de l'Aménagement et du Logement – DREAL),
- ✔ le niveau gouvernemental, avec le Secrétariat général de la Défense et de la Sécurité nationale (SGDNS), et avec, dans chaque ministère, le Haut fonctionnaire de défense et de sécurité (HFDS), qui est également le secrétaire général ministériel. Au MEDDE, le directeur général de la Prévention des risques (DGPR) définit la stratégie de résilience de l'État à l'égard de l'ensemble des risques naturels et technologiques, et en impulse la mise en œuvre sur le territoire en liaison avec les opérateurs de réseaux et leurs tutelles techniques.

Le réseau scientifique et technique (RST) du MEDDE apporte son concours aux pouvoirs publics et aux opérateurs de réseaux dans la prévention et dans la gestion des crises

Un ensemble d'organismes du RST (3) ministériel (qui seront regroupés à compter du 1er janvier 2014 au sein du Centre d'études et d'expertises sur les risques, l'environnement, la mobilité et l'aménagement – CEREMA), ainsi que le Bureau des recherches géologiques et minières (BRGM), l'Institut français des sciences et technologies des transports, de l'aménagement et des réseaux (IFSTTAR) et l'Institut national de l'environnement industriel et des risques (INERIS), ont développé, chacun dans un domaine qui lui est propre, une expertise sur l'évaluation des aléas, sur la vulnérabilité des réseaux et sur les solutions de réduction de cette vulnérabilité.

Ainsi, par exemple, le CETE (Centre d'Étude Technique de l'Équipement) Méditerranée (qui sera prochainement intégré dans le CEREMA – voir plus haut) est un pôle de compétence dans les domaines de la vulnérabilité des ouvrages et des réseaux aux risques sismiques et hydrauliques, et de la gestion des situations d'urgence. L'INERIS s'intéresse plus particulièrement aux installations industrielles, notamment aux installations classées pour la protection de l'environnement – ICPE (y compris les réseaux de canalisations enterrées ou aériennes), ainsi qu'aux interactions entre risques naturels et risques technologiques.

L'INERIS peut, en vertu d'une convention spécifique, apporter son appui aux DREAL dans la gestion de situations d'urgence sur simple demande de celles-ci. Il paraît souhaitable, dans un souci d'efficacité, qu'un tel dispositif soit étendu à l'ensemble du RST, ce qui n'est pas le cas actuellement.

Quelques enseignements de la mission du CGEDD sur la résilience

La mission a procédé à des auditions des administrations concernées, ainsi qu'à celles d'un certain nombre d'opérateurs de réseaux présents sur l'ensemble du territoire national (réseaux routier et autoroutier, réseau ferré national, voies navigables, aéroports, ports maritimes, transport et distribution d'électricité) ou à l'intérieur de l'agglomération parisienne (réseau métropolitain), en raison de l'importance économique et du poids démographique de cette dernière. Sans prétendre à l'exhaustivité, on trouvera ci-après quelques points importants qui sont ressortis de ces différents entretiens.

L'approche des risques naturels et technologiques par les pouvoirs publics (notamment par la direction de la Sécurité civile et par la DGPR) a légitimement privilégié la sécurisation des populations ; cela se traduit essentiellement par des restrictions de droits à construire dans les documents d'urbanisme. Un traitement adéquat des risques affectant l'intégrité des réseaux d'infrastructures et les services qu'ils assurent appelle l'apport de compléments à cette politique.

Ainsi, par exemple, le récent cadre d'actions pour la prévention du risque sismique (publié en début d'année 2013) ne mentionne que très ponctuellement les réseaux dans son Action 22b, qui s'intitule : « Poursuivre le recensement et le diagnostic des bâtiments, ponts et équipements nécessaires à la gestion de crise ».

La liste (non exhaustive) des risques identifiés par le portail Internet de la DGPR se rapproche de celle figurant en annexe de la loi prescrivant les plans de prévention des risques naturels prévisibles (PPR), sans complètement coïncider avec elle. Or, cette liste paraît mal adaptée à la problématique de la résilience des réseaux : ainsi, par exemple, le risque de tempête (non mentionné) est plus significatif que le risque des feux de forêts qui lui n'a jamais été cité, et le risque de tsunami en France métropolitaine y apparaît marginal et localisé. De même, les

températures extrêmes (notamment des périodes caniculaires prolongées) auxquels sont pourtant sensibles les équipements électroniques dont l'usage se généralise dans les réseaux, ne sont pas répertoriées comme risques dans la loi précitée relative aux PPR.

Le risque d'inondation est celui qui concerne la plus grande surface du territoire national, et c'est aussi celui qui est le mieux pris en compte dans les zonages et dans la planification de la mobilisation des opérateurs en cas de crise. Toutefois, les conséquences d'une crue centennale de la Seine sur l'agglomération parisienne seraient profondes et inévitables, et le retour à une situation normale prendrait plusieurs mois. Il en irait de même, mais avec des effets plus limités, d'une crue centennale du Rhône et de la Saône.

Les risques « classiques » bien cartographiés, notamment le risque d'inondation et le risque sismique, sont pris en compte par les pouvoirs publics (dans leur planification spatiale à travers les PPR) et par les opérateurs (dans leurs plans de mise en sécurité) d'une manière qui apparaît satisfaisante. Toutefois, la gestion d'une crue « centennale » de la Seine (*a fortiori*, d'une crue de type 1910) aurait des conséquences profondes pour la vie quotidienne des habitants et la continuité des activités économiques dans une partie importante de l'agglomération allant bien au-delà des seules zones submergées. Certes, la crue serait annoncée par avance à la population et la montée des eaux serait lente. Mais la décrue le serait également et les effets de l'inondation seraient longs à résorber.

La prise en compte de l'émergence de nouveaux risques liés au changement climatique et/ou à l'évolution technologique et celle de l'intensification de risques connus restent à approfondir.

À cet égard, on peut citer :

- ✔ le risque de submersions marines lié à l'élévation continue du niveau de la mer qui impose de reconsidérer le dimensionnement des ouvrages côtiers (notamment des digues de protection) ;
- ✔ des phénomènes de plus en plus récurrents, comme les températures extrêmes prolongées (fortes chaleurs, vagues de froid, gel), qui affectent plus particulièrement la fiabilité des composants électroniques, voire provoquent leur défaillance, alors même que les infrastructures (transmissions, *smart grids*, signalisation, équipements de sécurité...) et les matériels de transport recourent de plus en plus massivement à ces composants ;
- ✔ les tempêtes et les cyclones (ces derniers ne concernant pour l'instant que les DOM), dont l'incidence

*« La gestion d'une crue « centennale » de la Seine (*a fortiori, *d'une crue de type 1910 aurait des conséquences profondes pour la vie quotidienne des habitants et la continuité des activités économiques dans une partie importante de l'agglomération allant bien au-delà des seules zones submergées ».* Soldats sauveteurs lors de la crue de la Seine en 1910, Paris.

concerne toutes les infrastructures « hors sol » et dont la fréquence comme l'intensité semblent croître ;

- ✔ enfin, les chutes de neige importantes, notamment dans des régions mal pourvues en moyens matériels d'intervention, peuvent, même si elles n'altèrent pas les infrastructures proprement dites, paralyser pour une période plus ou moins longue le fonctionnement des réseaux, comme l'a démontré l'épisode neigeux de décembre 2010 en région parisienne.

Les réseaux de transport et de distribution d'énergie (électricité, gaz, hydrocarbures) comme ceux de communications électroniques (opérateurs de téléphonie fixe, de téléphonie mobile et Internet) apparaissent structurants pour la résilience de l'ensemble des autres réseaux, (notamment des réseaux de transport, d'eau et d'assainissement, de santé) et pour satisfaire les besoins essentiels de la population en conditions dégradées.

Ce point, qui fait l'objet d'un consensus de la plupart des acteurs rencontrés, a été mis en évidence tant à l'occasion d'exercices « sur table » (comme l'exercice « En Seine » organisé par la Préfecture de Police de Paris en 2010) que lors de crises réelles (comme l'ouragan Sandy, en 2012, dans l'agglomération new-yorkaise). Par ailleurs, ce même point fait actuellement l'objet de travaux menés sous l'égide du Secrétariat général de la Défense et de la Sécurité nationale (SGDSN). Pour un opérateur de réseau, le recours à un opérateur de téléphonie mobile unique risque de le fragiliser en cas de crise : la redondance en la matière doit donc être encouragée.

Si chaque opérateur a pris la mesure de la problématique risques (et notamment des risques naturels) pour ce qui le concerne et s'il améliore en permanence la sécurité de ses opérations, en revanche, la coopération entre opérateurs différents ne s'établit pas naturellement, comme en témoignent les simulations de crises et les crises réelles. Des exercices de simulation, mettant en jeu les pouvoirs publics ainsi que l'ensemble des opérateurs de réseaux, devraient être organisés plus systématiquement, et leurs retours d'expérience devraient être partagés entre les divers acteurs et être largement diffusés.

Les interdépendances entre les divers réseaux sont encore insuffisamment perçues et les pouvoirs publics seront amenés à affirmer leur rôle de coordination dans la gestion des crises. Par ailleurs, les retours d'expérience tant des exercices que des crises réelles ne semblent pas faire l'objet d'une diffusion ni d'une capitalisation suffisantes. Le CGEDD pourrait jouer un rôle plus affirmé dans cette double mission de diffusion et de capitalisation (entendue respectivement comme la mise en commun d'expériences et la constitution d'un corps de doctrine en constante évolution).

La réflexion sur les enjeux économiques de la résilience des réseaux reste à approfondir tant par les opérateurs eux-mêmes que par leurs tutelles respectives.

Cette problématique, étonnamment peu présente actuellement, repose tout autant sur les pouvoirs publics (l'étude d'impact d'une nouvelle réglementation en matière de sécurité devrait comporter un bilan prévisionnel de ses coûts et de ses bénéfices attendus) que sur les opérateurs de réseaux, qui se sentent pour l'instant assez peu concernés par cette réflexion, se considérant avant tout comme des exécutants d'une stratégie impulsée par l'État. En outre, ces derniers doivent élargir leurs évaluations prévisionnelles au-delà de leur périmètre propre, afin de permettre une prise en compte des coûts directs et indirects, pour la collectivité prise dans son ensemble, d'une défaillance (voire d'une rupture) de leur réseau entraînée par la concrétisation d'un aléa naturel.

Notes

* Ingénieur général des Ponts, des Eaux et des Forêts (IGPEF), Conseil général de l'Environnement et du Développement durable, ministère de l'Écologie, du Développement durable et de l'Énergie.

(1) *United Nations International Strategy for Disaster Reduction.*

(2) Inondations, mouvements de terrain, avalanches, incendies de forêts, séismes, éruptions volcaniques, tempêtes, cyclones.

(3) Le SETRA (Service d'Études techniques des Routes et Autoroutes), le CERTU (Centre d'Études sur les Réseaux, les Transports, l'Urbanisme et les Constructions publiques), le CETMEF (Centre d'Études Techniques Maritimes et Fluviales) et les huit CETE (Centres d'Études Techniques de l'Équipement).