Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2008)
Heft: 3

Artikel: De la vulnérabilité des sociétés modernes
Autor: Juilland, Dominique
DOI: https://doi.org/10.5169/seals-346854

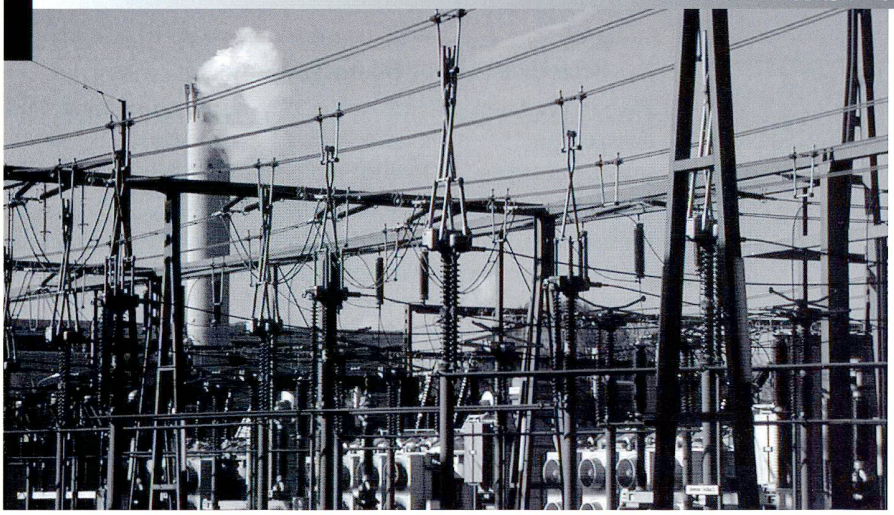
Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 17.11.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch



La mise en réseau (ici: électrique) implique une grande vulnérabilité. Elle nécesite de la redondance.

De la vulnérabilité des sociétés modernes

Div Dominique Juilland

Président, Association de la *Revue militaire suisse* (ARMS)

Introduction

Je propose quelques réflexions visant à mettre en lumière les aspects généraux de cette question, qui lorsqu'il s'agit de passer à la mise en œuvre des mesures concrètes de protection, s'avère très complexe.

Mon propos est articulé en trois parties, en s'inspirant de la méthode de raisonnement tactique militaire. D'abord tenter de répondre au fameux « dqs » de Foch : de quoi s'agit-il ? Ensuite analyser les « modes d'action ennemis », c'est à dire les menaces qui pèsent sur nos sociétés modernes. Comme il est impossible d'aborder tous les domaines, l'étude de l'impact de ces menaces est étudié à titre exemplaire dans le domaine de l'énergie et des biens de consommations. Eclairage sur les « modes d'actions amis », c'est à dire les parades permettant d'éliminer, ou pour le moins de réduire ces vulnérabilités.

De quoi s'agit-il ?

Il m'importe d'emblée de limiter l'objet de cette étude. Il n'y est pas question des vulnérabilités sociales, économiques et politiques de nos sociétés post-industrielles, quand bien même il y aurait beaucoup de matière à réflexion (par exemple les violences urbaines dans les banlieues françaises en 2005 ou les flux migratoires Sud-Nord). L'analyse porte uniquement sur les menaces qui pèsent sur les infrastructures techniques de nos sociétés modernes.

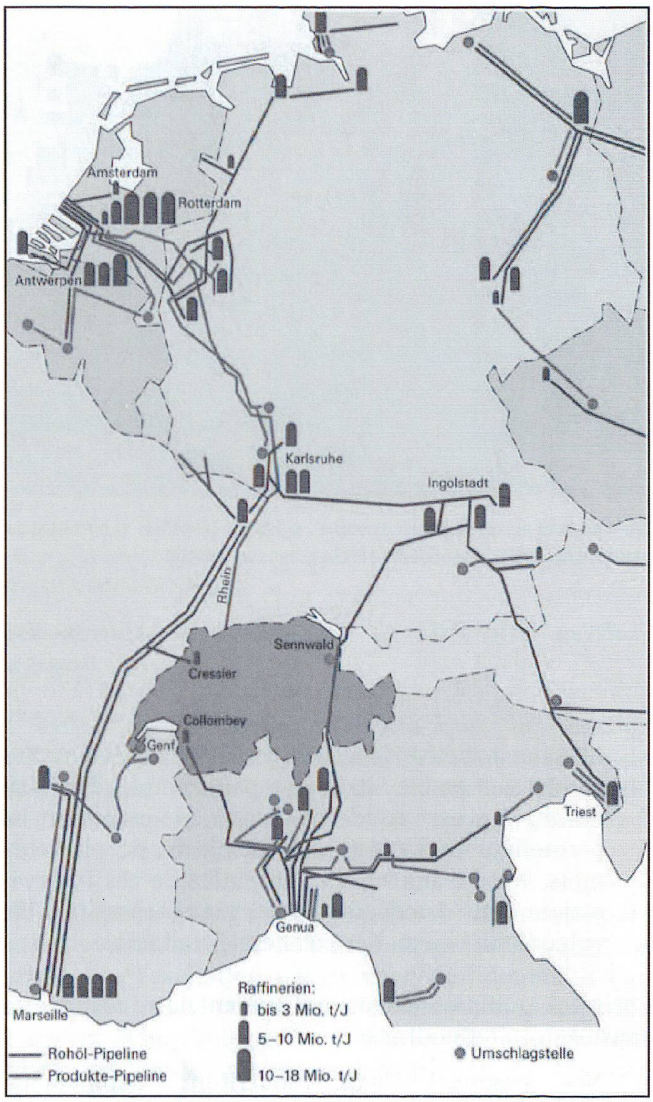
Qu'est-ce qui rend nos sociétés post-industrielles aussi vulnérables ? J'introduis la réponse par deux constats qui sont des lapalissades :

- Plus une société est archaïque, moins elle est vulnérable : une peuplade qui vit dans des zones forestières et qui tire son énergie du bois, ne souffrira pas des pannes d'électricité.
- Plus une société a de ressources et de réserves, moins elle est vulnérable : la Suisse, par exemple, disposait durant la guerre froide de réserves de carburant lui permettant de faire face à un blocus de plusieurs mois, voire d'années. Et l'ensemble de ces réserves étaient dans des dépôts souterrains ou sous roc. Sa vulnérabilité en matière d'énergie était faible.

Parmi les multiples facteurs qui rendent notre société très sensible, j'en retiendrai 4 :

- Nos besoins vitaux (nourriture, habillement, logement, énergie, communication) dépendent de plus en plus de technologies très sophistiquées, sensibles aux influences les plus diverses. Ex : nous dépendons pour l'énergie du pétrole, ou de l'électricité, avec tout ce que cela implique d'appareillages techniques d'un bout à l'autre de la chaîne allant de l'extraction de la matière première jusqu'à la consommation.
- Les petites collectivités locales (villages, clans, familles) ont perdu leur autonomie et sont incapables de subvenir aux besoins élémentaires de leur population. Ex : avant, chaque village avait son boulanger et sa laiterie. Aujourd'hui, le pain et les produits laitiers sont amenés de l'extérieur, parfois de fort loin.
- Nous sommes devenus une société à la fois concentrée (en zones urbaines) et mobile, ce qui nécessite de grosses infrastructures et des réseaux denses de transport et de communication, eux aussi vulnérables aux actions hostiles.
- Il résulte de ces facteurs une complexité et une interconnexion des différents secteurs de notre vie moderne, ce qui la rend si sensible.

Le sujet du forum est l'impact des problèmes de sécurité sur un pays de petites dimensions. Pour ma part, je ne pense pas que la dimension d'un pays soit très significative dans



Réseaux pétroliers en Europe

ce cas. Un petit pays peut mieux surveiller et entretenir ses infrastructures (comme l'illustre le récent exemple des grosses chutes de neige dans le centre de la France ayant provoquées de nombreuses coupures sur le réseau de distribution d'énergie électrique et la longue durée de remise en état compte tenu des grandes dimensions du secteur touché). D'un autre côté, un petit pays dépendra davantage de son environnement géopolitique.

La vulnérabilité d'un pays me semble dépendre davantage de son degré de développement technologique que de ses dimensions.

Les multiples menaces qui pèsent de l'extérieur sur les structures d'une société modernes peuvent être regroupées en trois grands domaines (je ne parle pas ici des causes endogènes du type pannes techniques pouvant paralyser un système, mais qui tendent à diminuer avec les progrès de la science) :

- Catastrophes naturelles (inondations, tremblements de terre, etc) ;
- Catastrophes technologiques (ex catastrophe nucléaire de Tchernobyl, catastrophes chimiques de Schweizerhalle et Bophal) ;
- Violences guerrière ou infra guerrière sous toutes les formes.

Cette brève étude n'aborde que le troisième type de menace et il faut d'emblée se poser la question : Quel est l'effet recherché par l'ennemi ou l'adversaire ?

En effet, sauf cas rarissimes (lorsque l'on a affaire à un fou par exemple), l'acte de violence de cette nature répond a une logique, a un objectif rationnel. Et suivant l'objectif recherché, la menace pesant sur les infrastructures ne sera pas la même. Voici quelques exemples de buts :

- Paralysie momentanée (p ex paralyser les transports et les communications le temps d'envahir un pays ou de prendre le pouvoir par une coup d'état).
- Destruction (empêcher définitivement l'adversaire d'utiliser certaines ressources, par exemple des puits de pétroles).
- Obtenir un effet médiatique, l'attention de l'opinion publique (c'était le cas du récent attentat à la bombe de l'ETA sur l'aéroport de Madrid). On peut d'ailleurs se poser la question si l'attentat du 9/11 n'est pas aussi de cette nature. Aucune infrastructure vitale américaine n'a été paralysée ou détruite.
- Dissuader (p ex les attentats en Corse qui vise essentiellement à dissuader les continentaux à s'établir dans l'Ile de Beauté).

En général, il y a adéquation entre effet recherché, mode d'action et moyens mis en œuvre. L'exemple contraire est en général fournit par les Etats-Unis d'Amérique : p ex la destruction des ponts sur le Danube durant la campagne du Kosovo en 1999 : l'objectif à court terme était de contenir les forces serbes au nord du Danube, l'objectif à long terme d'avoir une Serbie multiethnique pacifiée et de développer l'économie de l'ensemble des pays des Balkans. La stupide tactique à court terme appliquée par les Américains mettait à néant les objectifs à long terme puisque:

- il fallait reconstruire à grand frais (avec l'argent des Européens !) les ponts détruits ;
- l'économie des pays des Balkans, tributaire de la navigation fluviale sur le Danube, fut paralysée durant de long mois.

Un autre exemple récent d'inadéquation des méthodes et des fins sont les frappes israéliennes sur les infrastructures libanaises pour interrompre les opérations du Hezbollah (à moins qu'il y ait derrière ces frappes des intentions beaucoup moins avouables). Dans l'analyse des vulnérabilités de l'infrastructure d'un pays, il faut prendre en compte ce qui se passe dans la tête d'un adversaire ou ennemi potentiel. Que peut-il bien vouloir ?
Prenons l'exemple de l'énergie :

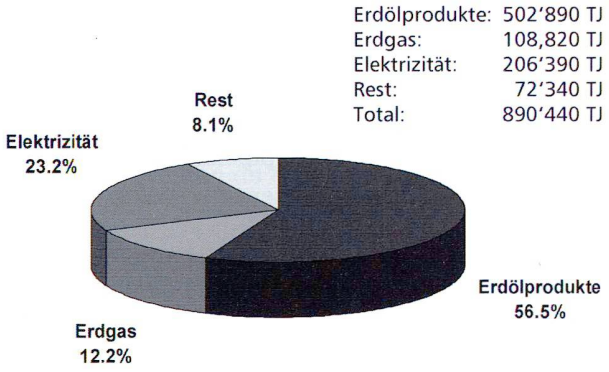
- Il est évident que si en Suisse on plastique une éolienne on n'obtient pas le même effet sur la production d'énergie électrique que si on fait exploser une centrale

nucléaire (sans compter les effets radioactifs).

- Si on veut priver le pays durablement d'énergie, on détruira une centrale nucléaire ou un barrage (ce qu'on fait les Anglais durant la Seconde Guerre mondiale dans la Ruhr).
- Si au contraire on ne veut qu' exercer une pression momentanée ou donner du poids à une revendication, on se limitera à faire exploser un pylone d'une ligne de haute tension ou un transformateur.

Les modes d'actions ennemis

Il n'est pas possible de brosser un tableau complet des menaces, et donc des vulnérabilités, pesant sur les sociétés modernes. Je me bornerai donc à apporter des touches ponctuelles en illustrant par deux exemples les points faibles de notre monde hypertechnisé.
La plus grande vulnérabilité de notre société est la vulnérabilité informatique. Ce n'est pas la génération qui a grandit avec un Ipod, un *laptop* et Internet qui contredira ce constat.
C'est un domaine dans lequel on obtient un maximum d'effet avec un minimum d'effort. Il est plus simple de perturber la distribution d'énergie électrique d'un pays en introduisant un virus dans le logiciel gérant les flux que de faire sauter un pylone de ligne de haute tension à l'explosif. La *Cyber War* est un sujet majeur qui doit être au centre des préoccupation de tout responsable

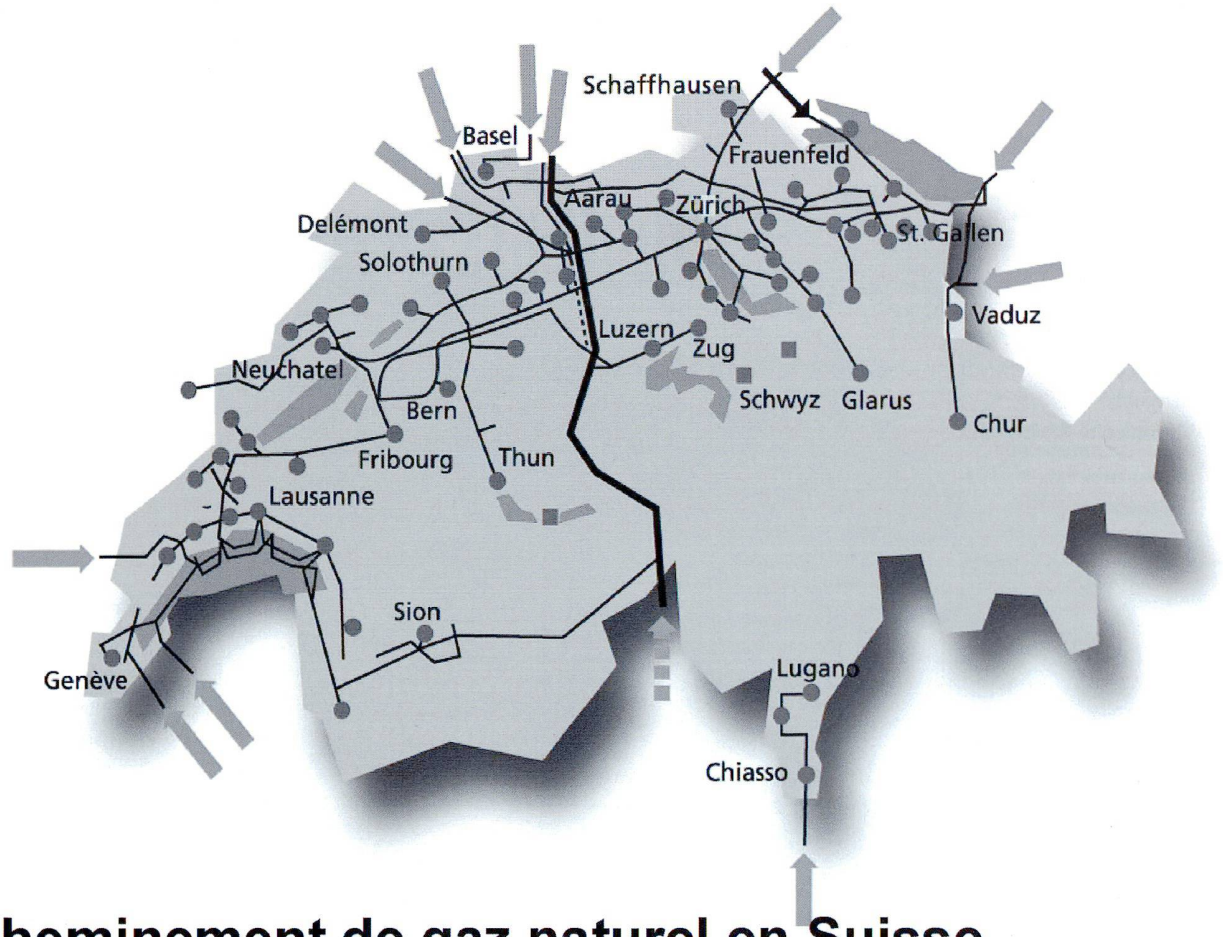


Besoins énergetiques en Suisse.

de sécurité, mais il faut une expertise spécifique pour l'aborder.
De même il ne sera pas question de la vulnérabilité du transport aérien. Tous ceux qui ont pris l'avion depuis le 9/11 ont subi sur leur propre personne les contraintes de la sécurité dans ce domaine.
Je vous propose deux exemples de vulnérabilité : l'énergie et les biens de consommation.

L'énergie

Quant on analyse les risques dans ce domaine, il faut distinguer:



Acheminement de gaz naturel en Suisse

- la production (centrales nucléaires, usines électriques) ;
- le stockage de l'énergie ou de la matière première (dépôts de carburants) ;
- le transport de l'énergie ou de la matière première (lignes de hautes tensions, pipeline, gazoduc) ;
- la distribution (stations essence, transformateurs).

Je laisse libre cours à la fantaisie du lecteur pour imaginer toutes les actions sournoises possibles dans ce domaine susceptibles d'empoisonner la vie des concitoyens. Mais toutes les actions n'ont pas le même impact et n'ont pas la même complexité et lourdeur dans la mise en oeuvre et l'exécution.
La centrale de Laufenburg en Suisse joue un rôle clé dans la régulation des flux d'énergie électrique en Suisse. Sa mise hors d'usage entraînerait un effondrement de toute la distribution en Suisse et sur le pourtour européen. Si on saisit le bon moment où tout le transfert de l'électricité produite au sud, mais utilisé au nord des Alpes passe par une seule ligne de haute tension, et que on arrive à rompre cette ligne, on paralyse presque instantanément l'ensemble du réseau ferroviaire suisse. C'est « l'exploit » qu'a réussi il y a quelques mois le conducteur d'une machine de chantier !
Faire sauter une centrale nucléaire ou un barrage comme la Grande Dixence aurait des conséquences désastreuses pour une grande partie du pays, mais c'est compliqué.
Il existe, en revanche, dans le système global « énergie » des sites dont la mise hors d'usage à peu de frais provoque des effets gigantesques. C'est comme toujours le maillon le plus faible de la chaîne qui en détermine la solidité. La mise hors service de certains points très sensibles du système (comme par exemple les vannes de contrôle des conduites forcées) exige moins de moyens, mais garantit une interruption de la production pour des années.
En Suisse, la configuration du réseau d'alimentation en gaz fait qu'il existe trois sites dont la mise hors d'usage provoque une pénurie quasi nationale.

Les biens consommation

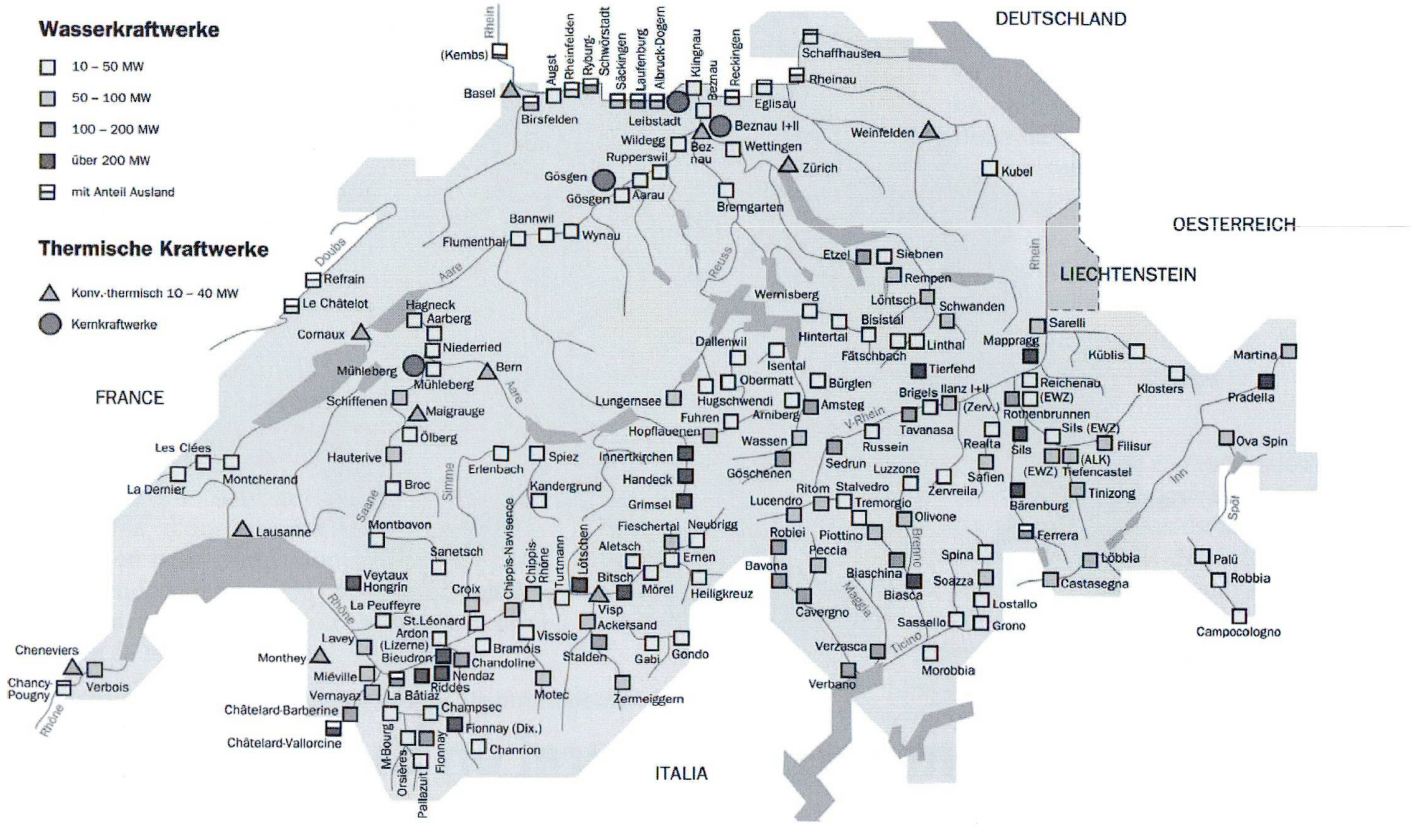
Là aussi, il convient de procéder à une analyse fine sur trois secteurs :

- la production ;
- le stockage ;
- la distribution.

Les vulnérabilités majeures tiennent aux aspects suivants :

- La globalisation : le marché des biens de consommation est désormais mondial.
- Il en résulte une segmentation géographique des cycles

Production d'électricité en Suisse



économiques : matières premières – production – conditionnement – consommation ne sont plus dans la même aire géographique.

- La production est souvent centralisée dans quelques sites majeurs.
- Pour des questions de coûts, les stocks sont réduits aux minimum. On vit aujourd'hui dans une logistique de flux tendus.
- Les réseaux de transport et de communication des personnes, des biens et des informations (pensez au réseaux de télécommunication) prennent dès lors une importance vitale.
- Mais ces réseaux sont eux aussi très vulnérables.

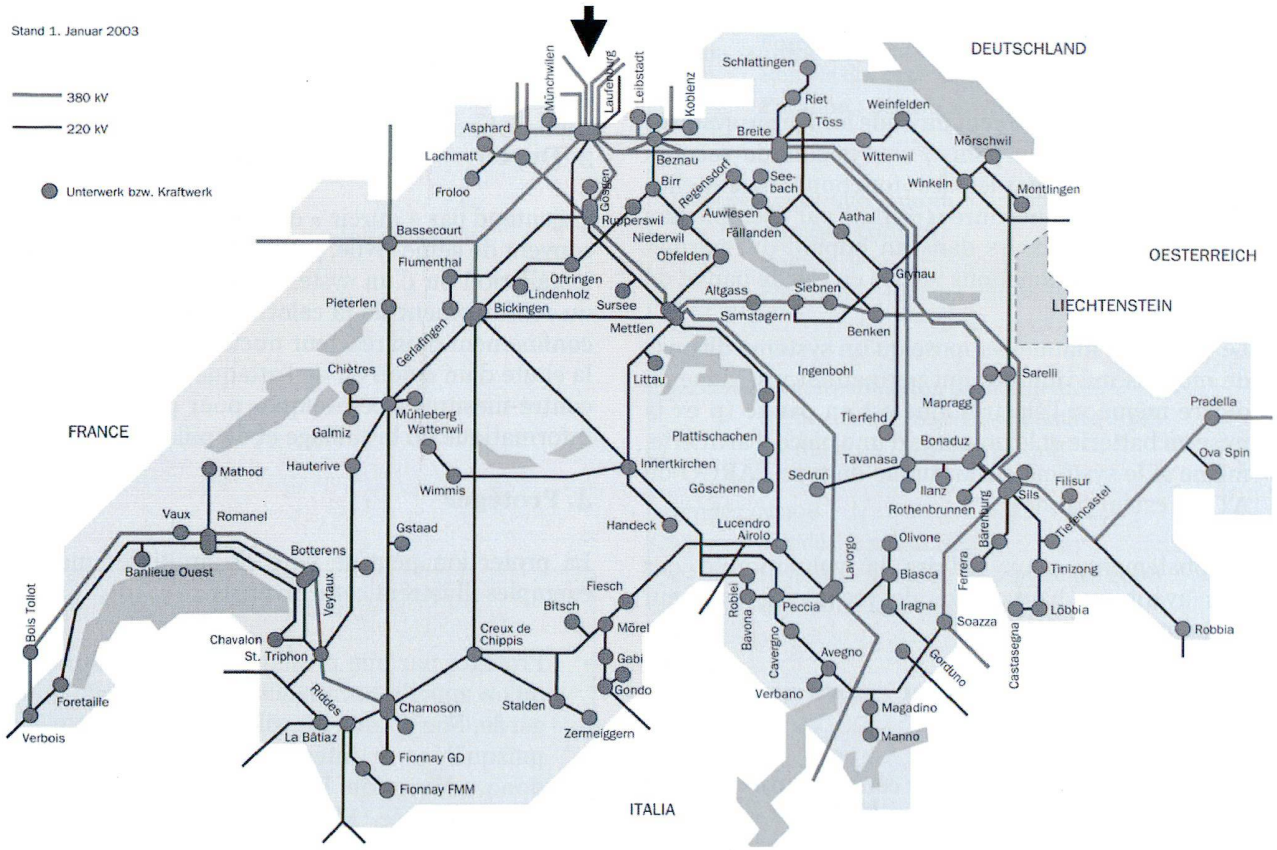
Quelques exemples suffisent à illustrer l'extrême vulnérabilité de nos sociétés dans ce domaine (mais sociétés qui – il faut le souligner - ont aussi une énorme flexibilité et beaucoup de ressources pour réagir vite et de façon adéquate pour contrer les menaces).

La grippe aviaire est un exemple significatif des menaces biologiques pesant sur notre société. Or, cette grippe n'a pas été déclenchée volontairement. Qu'en sera-t-il le jour où un groupe terroriste décide de contaminer le réseau d'eau d'une mégalopole comme Tokyo ou Mexico-City ? L'hystérie déclenchée par les attaques d'anthrax après le 9/11 donne un avant-goût de ce pourrait être le chaos. Le tremblement de terre de Kobé en 1995 a provoqué une pénurie mondiale de composante électronique vitales pour l'informatique, car ce site produisait l'essentiel des besoins du globe.

L'exemple du canton du Valais en hiver illustre à petite échelle ce qu'est la vulnérabilité d'une société moderne :

- Beaucoup de productions de bien de consommation de première nécessité (produits laitiers, produits carnés) se situent hors du canton.
- En hiver, il n'existe qu'une voie d'accès à haut débit (St.Maurice), plus deux accès ferroviaires (Lötschberg et Furka) depuis la Suisse. Ces accès sont vulnérables en cas de météo défavorable.
- Les stocks sur place sont réduits au minimum car le ravitaillement depuis le plateau suisse est quotidien.
- La population est localement multipliée par 6 à cause de l'afflux des touristes (à Crans-Montana on passe de 7 500 habitants à 45 000 résidents en haute saison, c'est-à-dire de 20 à 120 hab/hectare).
- Il existe donc des problèmes majeurs de ruptures de stock ou d'évacuation de populations.

Réseau de distribution électrique en Suisse



Nos modes d'actions

Premier constat, il est impossible de tout protéger :

- Par manque de ressources humaines (il n'y aura jamais assez de forces militaires et paramilitaires pour tout protéger) et techniques (on ne peut mettre une caméra TV à côté de chaque pylone électrique) ;
- Pour des questions de coûts : les mesures de protections sont onéreuses (exemple : le surcoût de la sécurité sur les billets d'avion).

Qui trop embrasse, mal étreint : il faut faire des choix et se limiter à la protection de l'essentiel. C'est un travail de longue haleine qui se fait par les responsables de la sécurité (par exemple les commandants des régions territoriales) et les experts techniques de la branche en question.

Dans une analyse très pointue, il s'agit de déterminer où sont les maillons faibles d'un système, où une intervention exogène peut provoquer le plus de dégâts, quelles sont les mesures techniques, sécuritaires, humaines qui seraient susceptibles de contrecarrer ces faiblesses.

Dans ce contexte, on ne peut faire que quelques réflexions générales, car encore une fois, chaque cas est un cas particulier qui nécessite une étude spécifique en tenant aussi compte de la situation géopolitique et sécuritaire du moment.

Les maîtres mots sont: redondance ; travail en dégradé ; travail en manuel.

- Redondance signifie doubler ou tripler les systèmes (comme par exemple les systèmes vitaux sur un avion).
- Travailler en dégradé veut dire que lorsque le système principale tombe en panne, un système de secours permet de sauvegarder les fonctions essentielles pendant une certaine durée (comme par exemple une génératrice de secours dans un hôpital qui permet de maintenir les fonctions vitales en cas de panne de courant).
- Le travail en manuel suppose qu'un système dispose de moyens mécaniques qui permettent une mise en œuvre même si l'électronique est en panne (p ex la mise en batterie et le pointage d'une pièce d'artillerie, même si le système électronique de type FARGO ou ATILA est en panne).

Plus globalement, pour réduire la vulnérabilité des sociétés ayant un haut degré de technicité, on peut envisager quatre mesures :

1. Diversifier ou/et créer des systèmes redondants

Voici trois exemples pour illustrer cette mesure :
Il faut chercher à diversifier les sources d'approvisionnement énergétiques, comme par exemple en Suisse en ayant des centrales nucléaires (plusieurs petites plutôt qu'une seule grande) et de l'électricité d'origine hydraulique.

Densifier le réseau de lignes électriques en éliminant les goulets. d'étranglement (c'est ce que cherche à faire l'Europe en augmentant les pipelines amenant gaz et pétrole russe).

Créer des rocades (routières, ferroviaires, aéroportuaires).

Ce dernier point appelle une remarque. Le relief d'un pays peut s'avérer un obstacle de taille qui peut engendrer des coûts et des difficultés de taille. C'est le cas notamment de la Suisse avec la barrière des Alpes. D'où l'importance de protéger, non pas seulement pour la Suisse, mais pour l'Europe entière, ce qu'on appelle les transversales alpines.

Une transversale alpine, ce n'est pas seulement un axe routier (avec un tunnel garantissant aussi le franchissement des Alpes en hiver), mais souvent aussi une voie de chemin de fer, un oléoduc, une ligne de haute tension, des câbles de fibre optique.

Un regard sur la carte montre que les rocades sont rares et souvent de faible capacité. D'où l'importance stratégique, de protéger et de garantir le libre usage de ces transversales.

2. Créer des stocks et des réserves

La Suisse a appliqué cette mesure avec beaucoup d'assiduité durant la période de la guerre froide. Cette mesure dépend essentiellement d'une volonté politique car elle est très onéreuse (immobilisation de capital, espace de stockage, entretien et protection).

3. Durcir

On entend par « durcir » des mesures techniques, le plus souvent de génie civile, pour réduire la vulnérabilité d'un installation ou d'un système. Il peut s'agir par exemple du renforcement de la calotte de béton de l'enceinte de confinement d'un réacteur nucléaire (pour le protéger de la chute d'un avion ou de l'attaque par un missile) ou de contre-mesures électroniques pour protéger un système informatique du brouillage et du pillage.

4. Protéger

La protection peut se faire de multiples manières. 4 exemples illustrent cette diversité :

- Protéger par une présence armée humaine ; c'est ce qu'on appelle communément en langage militaire la garde. Son avantage : elle est efficace et très souple puisqu'il y a intervention directe de l'homme, donc adéquation idéale entre menace et réaction proportionnée. Mais la garde a des inconvénients majeurs : elle est coûteuse car intensive en personnel ;

elle met en outre en danger la vie humaine.

- C'est pourquoi on s'achemine partout où faire se peut vers des solutions de surveillance technique et électronique : caméras de surveillance, senseurs de mouvement ou thermiques terrestres (ou aéroportés comme des drones).
- Une autre mesure de protection consiste à contrôler et autoriser l'accès à certaines installations ou zones sensibles de manière sélective comme par exemple dans les centrales nucléaires ou les aéroports (la zone de préparation des avions au vol ou l'accès aux aéronefs).
- Une autre technique consiste à créer une zone d'exclusion. Ce fut par exemple le cas lors du sommet du G8 à Evian où l'on créa une bulle aéro-terrestre, excluant tout accès par terre, air ou eau à la zone d'exclusion. Il en va de même aujourd'hui dans les environs de nombreux aéroports pour éviter des tirs de missiles sol-sol ou sol-air sur des avions en phase d'atterrissage ou de décollage.

Conclusion

La protection de nos sociétés modernes hypersensibles passe par une étroite coopération entre les responsables de la sécurité mandatés par le pouvoir politique – armée, gendarmerie, police – et les responsables techniques des installations et infrastructures à protéger. Ces derniers sont les seuls à pouvoir apporter l'expertise nécessaire permettant la meilleure protection au moindre coût. Mais militaires et forces de police sont les seuls à apporter la légitimité politique autorisant dans un état de droit l'usage de la force ou de la violence.

Cette protection de nos sociétés modernes passe aussi par la mise en place d'une solide organisation spécifique, bien dotée en personnel instruit et équipé de matériel performant que l'on nommera Protection de la Population en Suisse, Sécurité civile en France ou *Homeland Security* dans les pays anglo-saxons.

D.J.

ERRATA

Dans l'éditorial RMS N°2/2008, il faut lire que le cdt des Forces terrestres dispose désormais de 12 - et non de 11- subordonnés directs.

Réd.

Parution RMS+

Comme l'an dernier, la RMS+ produira en 2008 huit numéros selon le calendrier suivant : six numéros réguliers (bimestriel) et deux numéros thématiques. Les auteurs intéressés à soumettre des textes peuvent le faire selon l'échéancier suivant et sont encouragés à prendre dès que possible contact avec la rédaction.

≈

1/2008 Développement de l'armée, initiative avions militaires, armes et sécurité
Remise des textes : 7 janvier 2008
Parution : fin février.2008

≈

2/2008 Le feu, DEMOEX Défense, stratégie, terrorisme
Remise des textes : 28 février 2008
Parution : fin mars 2008

≈

3/2008 Humanitaire, opérations de maintien de la Paix, génie et sauvetage
Remise des textes : 17 mars 2008
Parution : début mai 2008

≈

4/2008 Sécurité, sécurité militaire, infanterie, sûreté sectorielle
Remise des textes : 12 mai 2008
Parution : début juillet 2008

≈

Aviation / 2008
Forces aériennes, Tiger-Ersatz
Remise des textes : 30 juin 2008
Parution : début août 2008

≈

5/2008 Logistique, aide au commandement, C4ISTAR, service territorial
Remise des textes : 30 juin 2008
Parution : début août 2008

≈

6/2008 Histoire militaire, infrastructure
Remise des textes : 22 septembre 2008
Parution : mi novembre 2008

≈

Blindés / 2008
Blindés et mécanisés
Remise des textes : 22 septembre 2008
Parution : mi novembre 2008

≈