Politique de sécurité: **analyses du CSS**

CSS ETH Zurich

N° 16 • juin 2007 • 2ème année

# INFRASTRUCTURES CRITIQUES: VULNERABILITES ET PROTECTION

La vulnérabilité des sociétés modernes constitue un défi croissant pour la politique de sécurité. Depuis les attentats du 11 septembre 2001, la protection des infrastructures critiques jouit d'une nouvelle priorité. L'élaboration de concepts de protection efficaces s'avère néanmoins laborieuse. Ceci exige des analyses de situation différenciées, une meilleure compréhension des vulnérabilités et un consensus politique sur les mesures de protection prioritaires. Une coopération nationale et internationale ainsi que des partenariats efficaces entre le secteur privé et le secteur public sont également indispensables.

*Infrastructures d'information – les centres nerveux de la société moderne* *www.istockphoto.com*

Dans la politique de sécurité, la protection des infrastructures a pris de l'importance. Ceci est essentiellement la conséquence des attentats traumatiques de New York et Washington (2001), de Madrid (2004) ainsi que de Londres (2005). Dans tous ces cas, les terroristes ont instrumentalisé des éléments d'infrastructure civile dans le but de tuer au hasard. Pour les attentats du 11 septembre 2001 aux Etats-Unis, ils se sont servis de l'infrastructure de transport en prenant comme armes des avions. En Europe, ce sont des trains, des métros, des gares et la foule de gens qui s'y trouvait qui étaient visés. Ce procédé a non seulement mis en évidence l'effroyable brutalité du «nouveau» terrorisme, elle a également renforcé le point de vue selon lequel les concepts traditionnels de sécurité intérieure ne satisfaisaient plus aux exigences de notre temps et devaient être réadaptés.

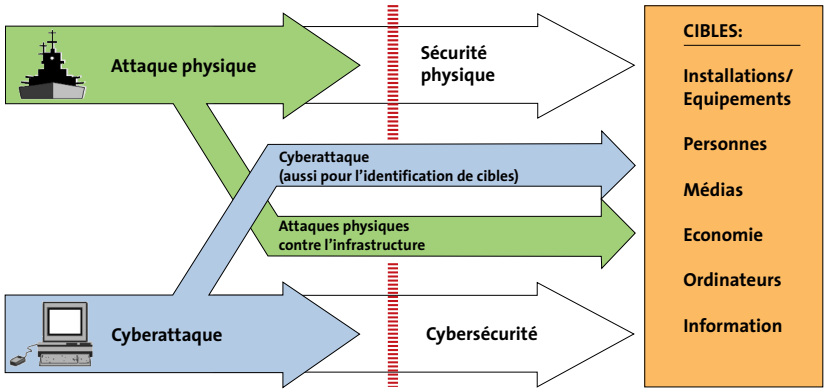
La protection d'installations stratégiquement importantes dans le propre espace socio-économique constituait déjà avant – sous le nom de «protection d'objet» – un élément important des concepts de défense nationaux. Mais la protection des infrastructures critiques, pour laquelle il est généralement repris le terme anglais de *Critical Infrastructure Protection* (CIP), couvre un concept plus large. D'une part, il ne s'agit plus seulement de se défendre concrètement ou d'engager des poursuites pénales après que l'acte a été commis, mais de plus en plus aussi de prévenir les dangers, voire de «prévoir la sécurité». D'autre part, la société moderne est aujourd'hui beaucoup plus vulnérable et le spectre des sources possibles de troubles et de crises est plus vaste et plus diffus. C'est pourquoi la protection des infrastructures critiques est devenue un point de cristallisation du débat actuel sur la sécurité.

## Des menaces aux risques

Deux facteurs ont conduit à la naissance et à l'établissement du concept de protection des infrastructures critiques. Premièrement, le changement de situation en matière de sécurité après la fin de la guerre froide a renforcé la nécessité de protéger les infrastructures. Durant le conflit Est-Ouest, les dangers touchant à la politique de sécurité étaient essentiellement des «menaces» militaires et liées à des acteurs. On procédait à l'identification et à l'évaluation de ces menaces en analysant ce qui était dénommé le triangle de menace, à savoir l'adversaire, ses intentions hostiles et les moyens à sa disposition. Alors que la menace découlant d'une telle analyse était relativement claire pendant la guerre froide, les formes et évolutions des défis posés à la politique de sécurité sont maintenant nettement plus diffuses. Le nombre limité de «menaces» a fait place à une multitude de «risques». Les risques sont caractérisés par l'incertitude et la complexité, il n'est plus guère possible de répondre à la question «qui-comment-où-quoi-pourquoi-quand». Depuis le tournant 1989/91, la politique de sécurité s'est adaptée à cette image diffuse en se concentrant moins sur les acteurs (difficilement identifiables) que sur les vulnérabilités de la société dans son ensemble. Le militaire américaine a fortement influencé ce débat en commençant, au début des années 90, à se pencher plus intensivement sur les menaces asymétriques.

Le deuxième moteur du concept de protection des infrastructures critiques a été la globalisation et notamment la révolution

**Interdépendances des risques et vulnérabilités**




*Source: Etude PCCIP 1997, p. 6*

de l'information qui a fortement marqué et accéléré ce processus. Dans les années 90, les nouvelles technologies d'information et de communication ont entraîné une transformation de la société, profonde et dynamique, qui n'est toujours pas achevée et dont les conséquences ne sont que partiellement perceptibles. Outre un grand nombre de facteurs positifs, cette évolution fait surtout ressortir un aspect négatif: la vulnérabilité des sociétés industrialisées modernes du fait de leur dépendance d'une multitude d'infrastructures d'information nationales et internationales. Celles-ci sont le lien fondamental entre d'autres domaines élémentaires et donc la condition de base pour le fonctionnement de toutes les autres infrastructures. Elles constituent aujourd'hui un élément central de la création de valeurs économiques. Et elles ne sont pas seulement incertaines par inhérence, mais aussi particulièrement sensibles aux mesures asymétriques.

## Des hackers aux terroristes

L'élément déterminant pour la diffusion mondiale du concept de protection des infrastructures critiques a été l'étude «Critical Foundations: Protecting America's Infrastructures» présentée aux Etats-Unis en 1997 par la *President's Commission on Critical Infrastructure Protection* (PCCIP). Le groupe d'étude a examiné les points faibles de la sécurité dans huit secteurs: télécommunications, approvisionnement en électricité, transport et stockage du gaz et du pétrole, banques et finances, transports, systèmes d'approvisionnement en eau, services de secours et administrations publiques. Il a constaté que les Etats-Unis sont si dépendants de ces infrastructures que le gouvernement devrait les examiner avec une «loupe de sécurité nationale», car une panne de longue durée pourrait avoir de graves conséquences pour toute la nation.

Conformément à cette approche, on entend par infrastructures critiques les installations, réseaux, services et biens d'équipement matériels et informatiques dont la panne ou la destruction aurait de graves conséquences sur la santé, la sécurité ou le bien-être économique des citoyens ainsi que sur le fonctionnement efficace du gouvernement d'un pays. Ces infrastructures peuvent être endommagées tant par des dangers structurels que par des attaques ciblées. Dans la première catégorie de risques figurent par exemple les catastrophes naturelles, les catastrophes anthropiques (par ex. ruptures de barrages, accidents nucléaires), la pénurie de personnel due à des grèves ou des épidémies, les problèmes d'organisation d'origine technique ou personnelle, les erreurs humaines, les pannes techniques ainsi que les dépendances et pénuries dans le domaine de l'énergie et de l'eau. Le spectre des auteurs possibles d'attaques, c'est-à-dire la deuxième catégorie, est très vaste et va de l'adolescent qui s'ennuie au collaborateur mécontent, à l'espion industriel, à la criminalité organisée, aux fanatiques et aux unités de terroristes et même jusqu'aux Etats hostiles.

Tout aussi variées, les options d'attaque peuvent inclure les attaques par des hackers aussi bien que la destruction physique d'équipements civils ou militaires. L'attention des premiers efforts américains en matière de protection des infrastructures critiques a de toute évidence essentiellement porté sur les risques encore largement inconnus du cyberspace: l'infrastructure mondiale de l'information semblait rendre possible de commettre des attaques anonymes de n'importe quel endroit du monde et rendait simultanément les outils des hackers accessibles à n'importe qui. En raison de cette perception de menace, la politique de protection des infrastructures critiques conçue sous le président américain Bill Clinton était principalement orientée sur la sécurité de l'information.

Depuis les attentats terroristes du 11 septembre 2001, on constate néanmoins un retour du concept classique de menace dans le débat sur la protection des infrastructures critiques. Notamment du point de vue des Etats-Unis, toute une série de dangers structurels sont dès lors de plus en plus fréquemment abordés dans le cadre d'une stratégie de lutte contre le terrorisme orientée sur les acteurs. Aux Etats-Unis, la protection des infrastructures critiques devint partie intégrante de la *Homeland Security* et intervient aujourd'hui essentiellement dans le contexte des stratégies de lutte contre le terrorisme islamiste. Les aspects physiques de la protection des infrastructures critiques sont passés au premier plan tandis que les aspects concernant l'information ont perdu de l'importance. Une telle orientation sur la défense contre le terrorisme se retrouve aujourd'hui aussi dans les débats de l'UE qui vient de commencer à développer un programme de protection des infrastructures critiques consistant essentiellement à coordonner les mesures des Etats membres.

## Défis à relever pour une politique efficace de CIP

L'exemple américain et les expériences d'autres pays conduisent à sélectionner quatre défis pour assurer une politique efficace de protection des infrastructures critiques. Premièrement, il est nécessaire de procéder à une évaluation solide du type et de l'ampleur des principaux risques et menaces. Au lieu de se concentrer exclusivement sur le terrorisme, comme c'est le cas actuellement, la protection des infrastructures critiques devrait suivre une approche plus vaste et se pencher de manière générale sur la vulnérabilité des systèmes hautement complexes. Dans le cadre d'une analyse de situation différenciée, les services de renseignements jouent un rôle important. Une telle analyse est d'autant plus importante que, selon le danger, les responsabilités varient et les protections doivent être différentes. C'est l'opérateur d'une infrastructure qui doit veiller à la protection contre les dangers et les risques dans un cadre «normal» – comme par exemple les attaques de hackers et les petites catastrophes naturelles. Par contre, on attend de l'Etat qu'il assure une protection contre les dangers d'un niveau supérieur, comme par exemple les attentats terroristes ou les attaques par d'autres pays.

La deuxième nécessité est une bonne compréhension des vulnérabilités, y compris une analyse des interdépendances entre les infrastructures. Il s'est avéré qu'en raison des systèmes très complexes la méthodique actuelle ne suffit pas pour saisir toute l'étendue du problème. Au plan stratégique, contrairement à l'approche technique dominante, il s'agit souvent moins de quantifier et mesurer «objectivement» les risques que de les comprendre dans leur contexte social, politico-institutionnel, culturel ou économique.

Troisièmement, il s'agit de savoir ce qui rend une infrastructure «critique». Après le 11 septembre, la liste des infrastructures critiques aux Etats-Unis a été fortement étendue: il est désormais également critique ce qui pourrait avoir des répercussions sur la psyché et la morale nationale. Ceci entraîne des problèmes quasiment insurmontables pour la conception de mesures de protection: comment assurer la sécurité quand presque tout est potentiellement critique et donc à protéger? Les seuils entre «normal» et «critique» ne doivent pas être trop bas. Des priorités judicieuses sont un aspect central. Mais ceci n'est possible que sur la base d'analyses de risques approfondies. La vulnérabilité hypothétique d'une cible n'est pas un indicateur suffisant pour juger si cette cible doit être protégée. Pour procéder à une évaluation judicieuse, il faut aussi disposer d'informations sur des menaces concrètes ainsi que sur la portée et l'ampleur d'un éventuel dommage.

Quatrièmement, la protection des infrastructures critiques exige une vaste coopération. Un partenariat efficace entre l'Etat et les milieux économiques est indispensable. Suite à la libéralisation de nombreux domaines du secteur public depuis les années 80, de nombreuses infrastructures critiques appartiennent aujourd'hui au secteur privé. C'est pourquoi les milieux économiques assument un rôle primordial tant pour la définition que pour la mise en œuvre d'une politique de protection. Mais une politique efficace de CIP exige aussi une cohérence entre les divers organes publics ainsi qu'une coopération internationale. Les actes terroristes et autres délits, tout comme les catastrophes naturelles ou autres, ne s'arrêtent pas aux frontières. Il est donc nécessaire de coordonner les contre-mesures au plan international.

## Conséquences pour la Suisse

En Suisse aussi, plusieurs organes s'occupent déjà, à l'échelle nationale, de la protection des infrastructures critiques, mais sous des angles très différents et pour ainsi dire sans coordination. En conséquence, l'Office fédéral de la protection de la population (OFPP) a été chargé par le Conseil fédéral à la mi-2005 de définir les besoins et d'élaborer les mesures correspondantes en collaboration avec tous les départements concernés.

Si l'on analyse l'état actuel des efforts suisses en matière de CIP sur la base des quatre exigences ci-dessus, on obtient un tableau différencié: sur le plan de l'évaluation de la situation, la Suisse peut, dans le domaine de la sécurité de l'information, faire valoir une approche performante, même en comparaison internationale. En bonne part en raison de ses liens étroits avec le service de renseignement intérieur (SAP), la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) s'est avérée être un instrument efficace. Ceci devrait servir de base à une stratégie de protection des infrastructures critiques. Par ailleurs, il faudrait prévoir un vaste réseau d'experts pour assurer une évaluation continuelle de la menace.

La Suisse devrait vérifier systématiquement l'utilité des approches de saisie des vulnérabilités qui dépassent la classique analyse de risque. Une meilleure et plus vaste compréhension des vulnérabilités n'est en outre possible que par la recherche interdisciplinaire et surtout internationale, comme l'UE l'encourage en priorité dans son 7e programme dès 2008. La Suisse doit veiller à ne pas se faire dépasser et devrait chercher à participer activement à l'élaboration des programmes de recherche correspondants.

La définition de seuils pour juger du caractère critique des infrastructures exige un débat politique qui n'a pas encore eu lieu en Suisse. Un concept fédéral d'information est également nécessaire dans ce domaine. La saisie du caractère critique et de la vulnérabilité des infrastructures doit en outre reposer sur une approche unique pour tous les départements, avec une méthodique homogène qui intègre également des acteurs non publics.

Enfin, concernant la nécessité d'une vaste coopération, on constate pour la Suisse tant des points forts que des déficits importants. Le système suisse de milice, c'est-à-dire une étroite liaison entre l'Etat et les milieux économiques, offre un gros avantage pour intégrer le secteur privé dans l'analyse de risque. Ici, l'objectif sera d'exploiter les partenariats déjà formés entre le public et le privé au niveau des offices fédéraux pour élaborer une stratégie suisse globale de protection des infrastructures critiques et il s'agira d'étendre les structures de confiance existantes. Par contre, la Suisse doit mettre les bouchées doubles au niveau de la coopération internationale: des conventions sectorielles sur le développement de standards homogènes, des examens communs sur la protection des infrastructures critiques, la recherche des types de menace courants et l'échange de méthodes de protection éprouvées doivent être les éléments de base d'une future stratégie de coopération suisse. Justement parce que la Suisse jouit de conditions favorables en matière de partenariats entre le secteur public et le secteur privé, elle devrait apporter plus fortement ses propres solutions dans le débat international sur la protection des infrastructures critiques.

### Chronologie de la protection des infrastructures critiques en Suisse

- **Novembre 1997:** Exercice de conduite stratégique 1997 (ECS 97), scénario d'attaques électroniques perturbant l'infrastructure d'information suisse. Résultat: proposition urgente de créer un état-major spécial de sécurité de l'information pour la gestion des crises à l'échelle nationale.
- **Juin 2001:** Exercice INFORMO, «Crises déclenchées par des perturbations dans l'infrastructure de l'information», test de l'état-major spécial sûreté de l'information (SONIA).
- **2001:** La fondation InfoSurance organise dans divers secteurs des tables rondes sur le thème «Risques et dépendances dans la société de l'information» qui seront reprises dès 2004 par l'Office fédéral pour l'approvisionnement économique (OFAE).
- **Octobre 2003:** Création de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI).
- **Juin 2006:** Le Conseil fédéral décide qu'à titre de base pour une stratégie future l'OFPP doit concrétiser les besoins et élaborer les mesures correspondantes. Point de départ: définitions communes et homogènes; identification des infrastructures critiques importantes pour la Suisse; éventail de base de scénarios de dangers.

- Editeur responsable: Daniel Möckli
analysen@sipo.gess.ethz.ch
- Commande d'analyses et abonnement gratuit: www.ssn.ethz.ch