NATO OTAN

Bulletin d'information PCU

Civil Emergency Planning

Plans civils d'urgence

N°8 • Septembre 2009

Soutenir les opérations de l'OTAN - Protéger les populations civiles

PAGES 3-4
Sécurité énergétique :
- Jurgita Bilvaisiene – Lituanie
- Diether Urban – président du Comité de planification industrielle

PAGES 5-6
Cybersécurité :
- Ligia Ferreira – président du Comité de planification industrielle,
- Suleyman Anil – chef du Centre de coordination et de soutien pour la cyberdéfense de l'OTAN – siège de l'OTAN

PAGE 8
- Piraterie : Jim Caponiti – président du Bureau d'étude des transports océaniques de l'OTAN

PAGE 9
- Pandémie mondiale : Eric Lecarpentier – président du Comité médical mixte de l'OTAN

PAGE 12
- Le programme scientifique de l'OTAN contribue à la cybersécurité dans les pays partenaires – Jayne Clinton

PAGE 13
- Développements interve-nus au sein du SCEPC

PAGES 14-15
- Exposé d'actualisation de l'EADRCC – AidMatrix - Günter Bretschneider, chef de l'EADRCC

Avertissement : Publiés sous l'autorité du SGA pour les opérations, les avis exprimés dans ce Bulletin ne reflètent pas nécessairement l'opinion ou la politique officielle des gouvernements des pays membres ni celle de l'OTAN.

Éditorial

Martin Howard, secrétaire général adjoint de l'OTAN pour les opérations

Plans civils d'urgence de l'OTAN - Menaces et défis nouveaux

Contrairement à ce qui était le cas auparavant, les défis sécuritaires d'aujourd'hui concernent presque exclusivement la protection des populations plutôt que celle des territoires. Les mena-ces et les défis nouveaux qui sont le thème de ce numéro n'illustrent que trop clairement cette évolution. Sécurité énergétique, cyberdéfense, lutte contre la piraterie et gestion des pandémies : toutes ces problématiques touchent directement les populations, par-delà les frontières nationales

Dans notre numéro de septembre, nous avons voulu poser un certain nombre de questions. Les PCU en font-ils assez ? Pourraient-ils s'impliquer davantage et apporter une contribution dans d'autres domaines ? Leur réseau d'experts civils offre-t-il la palette de compétences appropriée pour relever ces défis ? Un autre thème, dont nous ne traitons pas dans ce numéro, devra également être abordé : il s'agit du changement climatique et de sa capacité à aggraver les risques, déjà présents, de déstabilisation des pays. Faudrait-il que les PCU envisagent d'élargir le champ de leur expertise et qu'ils contribuent davantage aux efforts visant à limiter les conséquences du changement climatique, par exemple en recourant plus largement à l'EADRCC, le Centre euro atlantique de coordination des réactions en cas de catastrophe ?

Récemment, dans une allocution qu'il a prononcée à l'occasion du lancement du nouveau concept stratégique, le secrétaire général de l'OTAN a déclaré que le fond du débat ne devrait pas être ce que l'OTAN peut faire, mais bien ce que l'OTAN doit faire, et que la question n'est pas tant d'adapter les missions aux capacités disponibles que d'adapter les capacités aux défis auxquels nous sommes confrontés. Cela vaut également pour les PCU. Trop souvent, notre préoccupation est de « vendre » des produits existants, comme par exemple une expertise déjà disponible. Peut-être devrions-nous plutôt nous attacher à trouver les moyens de nous adapter à notre environnement en mutation et de concevoir des produits innovants pour l'avenir. Pour reprendre une ancienne formule, on ne peut pas relever les défis du 21è siècle avec le mode de pensée du 20è siècle. La force de l'Alliance réside dans sa vocation duale, à la fois civile et militaire. La meilleure manière de faire face aux nouveaux défis est de s'assurer que le civilo militaire devienne la norme pour la planification et la conduite des opérations.

La difficulté est de trouver le juste équilibre. En tant qu'organisation, l'OTAN doit bien entendu faire face aux défis sécuritaires actuels et futurs les plus urgents, mais elle doit aussi éviter de se disperser en voulant toucher à tout au risque de n'être bonne à rien. Les discussions qui auront lieu dans les prochains mois autour du nouveau concept stratégique contribueront à définir les priorités et à trouver ce juste équilibre.

CEP Quote

Indépendamment des menaces les plus facilement identifiables, la dernière décennie a vu l'émergence de toute une série de défis qui, nous le constatons de plus en plus, ont des incidences en matière de sécurité. Je veux parler ici de la sécurité énergétique ou de la défense contre les cyberattaques et de notre prise de conscience des incidences croissantes des changements climatiques sur la stabilité des États, ainsi que du partage international des ressources précieuses, comme l'eau.

Extrait du discours prononcé par M. Jaap de Hoop Scheffer à l'occasion de l'ouverture du séminaire sur le nouveau concept stratégique, le 7 juillet 2009

Face aux menaces et aux défis nouveaux, les PCU jouent un rôle clé, compte tenu de leur engagement actif et ouvert à l'égard des partenariats. Depuis longtemps déjà, les pays partenaires ont la possibilité de participer aux discussions sur la mise en oeuvre concrète de la politique de l'OTAN, dans un esprit d'ouverture et de solidarité. Nombreux sont ceux qui possèdent en outre une expertise considérable dans des domaines spécifiques et auprès desquels l'OTAN peut apprendre beaucoup.

Devant ces nouvelles menaces, la coopération avec d'autres organisations internationales demeure essentielle pour éviter les doubles emplois inutiles. Ainsi, par exemple, bon nombre des menaces dont il est question dans ce numéro sont aussi du ressort de l'Union européenne. Et il est souvent bien difficile de savoir exactement où commence le mandat d'une organisation et où s'arrête celui d'une autre.

En conclusion, aucun pays n'est à l'abri des menaces planétaires, et la coopération demeure une nécessité face aux défis communs. Les activités de l'OTAN dans le domaine des plans civils d'urgence restent l'occasion privilégiée de partager efficacement les informations et les meilleures pratiques. Les PCU sont déjà à pied d'œuvre et s'apprêtent à adopter des approches novatrices pour faire face à ces défis. On pourrait sans aucun doute exploiter mieux encore tout le potentiel des PCU pour la planification civilo militaire et le soutien des opérations, notamment en faisant jouer les relations établies avec les partenaires, dont l'expertise spécifique pourrait être mise à profit. Une chose est claire : la valeur ajoutée des PCU provient d'abord et surtout des immenses possibilités d'un réseau offrant de multiples interfaces avec des agences civiles dans des domaines aussi variés que la planification industrielle ou les questions médicales. C'est là une excellente base, sur laquelle nous pouvons construire des structures efficaces qui nous aideront à mieux protéger les populations et à limiter l'impact des crises dès leur apparition.

LE SAVIEZ-VOUS ?

À ce jour, 28 pays ont signé le mémorandum d'entente sur la facilitation des transports civils transfrontières d'importance vitale : l'Albanie, l'Allemagne, l'Arménie, l'Autriche, la Bosnie-Herzégovine, la Bulgarie, le Canada, la Croatie, le Danemark, l'Espagne, l'Estonie, les États-Unis, l'ex-République yougoslave de Macédoine*, la Finlande, la Géorgie, la Hongrie, la Lituanie, le Moldova, la Norvège, les Pays-Bas, la Pologne, le Portugal, le Royaume-Uni, la Slovaquie, Slovénie, la Suède, la Turquie, et l'Ukraine. Il s'agit d'un instrument multilatéral visant à améliorer la rapidité et l'efficacité de l'assistance aux victimes de catastrophes et de crises humanitaires, y compris celles provoquées par des incidents chimiques, biologiques, radiologiques ou nucléaires (CBRN) au sein des pays du CPEA

* La Turquie reconnaît la République de Macédoine sous son nom constitutionnel.

1

2

3

M. Martin Howard signe le MoU en présence de M. l'ambassadeur Ivo Daalder (Etats-Unis), M. l'ambassadeur Boguslaw Winid (Pologne) et de M. l'ambassadeur Jüri Luik (Estonie).

L'article qui suit a été fourni par la Lituanie, pays membre de l'OTAN ayant des compétences et des priorités spécifiques dans le domaine de la sécurité énergétique. On trouvera ensuite un papier de Dieter Urban, président du Comité de planification industrielle (IPC) de l'OTAN, sur les activités menées dans le domaine de la protection des infrastructures énergétique critiques - l'un des principaux axes de travail de l'IPC.

Point de vue de la Lituanie sur la sécurité énergétique

La sécurité énergétique est une composante indispensable au bon fonctionnement de l'économie, ainsi qu'un élément clé de la sécurité nationale et de la protection civile. Un approvisionnement diversifié et fiable en ressources énergétiques, ainsi qu'une utilisation durable et efficace de ces ressources, contribuent très largement à la prospérité d'un État. La sécurité énergétique favorise donc la stabilité de la communauté internationale dans son ensemble. Il est apparu ces dernières années que les défis posés par la sécurité énergétique dépassaient le simple cadre national ou régional, de par leur nature, et qu'ils appelaient donc des solutions globales.

Cela fait relativement peu de temps que la sécurité énergétique figure à l'ordre du jour de l'OTAN. Dans la mesure où les perturbations de flux énergétiques pourraient affecter la sécurité des Alliés, nous estimons que l'OTAN, en tant qu'organisation politico-militaire, a aussi un rôle à jouer en matière de sécurité énergétique. Il n'existe pas d'organisation internationale qui ait le monopole dans ce domaine. L'OTAN ne devrait donc pas limiter son rôle à la seule protection des infrastructures énergétiques critiques - qui est bien sûr un point important, mais pas suffisant pour autant. Il conviendrait aussi de réfléchir à la dimension politique de la sécurité énergétique. Nous avons besoin d'une approche assurant cohérence et équilibre entre la dimension technique et la dimension politique.

La question de la sécurité énergétique est particulièrement importante en Lituanie. Les circonstances historiques ont fait que la Lituanie a évolué indépendamment des pays de l'UE et de l'OTAN dans le domaine énergétique. En outre, le pays est totalement dépendant des importations de gaz russe et, dans une large mesure, des exportations de pétrole russe. La situation pourrait devenir encore plus compliquée après la fermeture de la centrale nucléaire d'Ignalina, qui répond actuellement à la plupart des besoins énergétiques du pays. L'intégration du secteur énergétique lituanien dans le marché commun européen de l'énergie et la réduction de la dépendance de la Lituanie à l'égard d'un fournisseur externe unique sont donc nos principaux objectifs dans l'avenir prévisible.

Dès lors que la dépendance à l'égard d'un seul fournisseur d'énergie est reconnue comme l'un des principaux problèmes en matière de sécurité énergétique, il devient stratégiquement important de diversifier les sources d'approvisionnement en énergie. Afin d'atteindre cet objectif, nous avons besoin d'intensifier encore le dialogue entre les producteurs d'énergie, les consommateurs et les pays de transit. Il conviendrait de fonder ce dialogue sur les principes de la transparence, de la non-discrimination, de la confiance mutuelle, de la réciprocité et du libre accès aux voies de transit, lesquels principes sont inscrits dans le Traité sur la Charte de l'énergie. L'OTAN pourrait servir de trait d'union entre les pays, en servant de cadre à la coopération dans le secteur de l'énergie.

Il conviendrait de noter que la diversification des sources d'approvisionnement en énergie ne constitue toutefois qu'une partie du problème. Nous avons également besoin de diversifier nos ressources énergétiques. Les réserves d'énergie traditionnelle s'épuisent, les prix fluctuent et l'augmentation de la consommation d'énergie a des effets négatifs sur le climat à l'échelle mondiale. La question du réchauffement planétaire, qui est l'un des problèmes majeurs au niveau mondial, peut être traitée essentiellement grâce à deux mesures : a) une meilleure utilisation des ressources énergétiques et b) une plus grande consommation d'énergies renouvelables et respectueuses du climat, dont l'énergie nucléaire.

Jurgita Bilvaisiene, division responsable des orientations en matière de sécurité énergétique, ministère lituanien des Affaires étrangères

Il existe un lien direct entre la sécurité des ressources essentielles et la sécurité des populations des pays de l'Alliance - qui est l'une des principales responsabilités incombant aux Plans civils d'urgence (PCU) de l'OTAN. Le rôle des PCU dans le domaine de la sécurité énergétique pourrait surtout consister à examiner les questions techniques dans les forums internationaux. Dans un avenir proche, le ministre lituanien des Affaires étrangères, le Comité de planification industrielle de l'OTAN et le Comité pour la science au service de la paix et de la sécurité prévoient de mener des projets conjoints en matière de sécurité énergétique, qui seront destinés à promouvoir le dialogue mutuel dans le secteur de l'énergie, ainsi que la protection des infrastructures essentielles.

Seuls des efforts concertés, un esprit d'anticipation et une approche stratégique de la sécurité énergétique nous donneront l'ouverture d'esprit nécessaire pour faire face aux grands défis à venir.

Contributions du Comité de planification industrielle de l'OTAN à la sécurité énergétique

Compte tenu des nouveaux défis auxquels l'Alliance est confrontée et des efforts déployés par l'OTAN dans le domaine de la sécurité énergétique, le Comité de planification industrielle (IPC) s'occupe, depuis juin 2004, des questions de sécurité énergétique liées aux PCU, sous l'autorité du Haut Comité pour l'étude des plans d'urgence dans le domaine civil (SCEPC). Depuis le début, l'idée qui prévaut sur le plan politique est que l'IPC ne devrait traiter que les aspects physiques de la protection des infrastructures énergétiques critiques. Les questions relatives à l'approvisionnement en ressources énergétiques critiques et à la sécurité de ces ressources ne sont pas analysées au sein de l'IPC. Les activités de ce dernier consistent principalement à suivre de près la question des menaces liées à la sécurité (notamment le terrorisme), qui relève des autorités nationales ou doit faire l'objet d'une coordination des secteurs public et privé de l'industrie.

La priorité de l'IPC a été de se focaliser sur la protection des infrastructures électriques critiques dans la mesure où ces infrastructures ont une incidence directe sur la plupart des industries et sur les principaux secteurs d'activité de la société. Par la suite, le Comité s'est également penché sur la question des infrastructures pétrolières et gazières.

Dans la mesure où les réseaux d'infrastructures énergétiques s'étendent au-delà des frontières nationales, la coopération entre les pays membres de l'OTAN et en particulier avec les pays partenaires est très importante. Aussi l'IPC associe-t-il très étroitement les pays du Conseil de partenariat euro-atlantique (CPEA) à ses travaux sur la sécurité énergétique. Il analyse les infrastructures énergétiques situées sur les territoires des pays de l'OTAN et du CPEA et s'intéresse en particulier aux connexions transfrontalières. Comme les infrastructures énergétiques sont souvent la propriété d'exploitants privés, les partenariats entre les secteurs public et privé sont considérés comme très importants pour les analyses de l'IPC.

Les travaux de l'IPC visent à mieux sensibiliser les planificateurs dans les administrations à la question de la sécurité énergétique, à partager les informations dans ce domaine, à renforcer le dialogue et à développer des contacts bilatéraux entre les représentants des pays auprès de l'IPC et les experts du secteur industriel, ainsi qu'entre les autres comités OTAN traitant des infrastructures énergétiques critiques.

Pendant ses séminaires et réunions plénières, l'IPC, soutenu par des experts de l'industrie spécialisés dans les questions énergétiques, examine des mesures de protection, partage des données d'expérience et fait le point sur les différents marchés de l'énergie. Compte tenu des divers systèmes de protection qui existent, l'IPC estime qu'il est plus utile d'élaborer une politique de partage des meilleures pratiques plutôt qu'un inventaire des mesures de protection. Il ne définit ni politique contraignante ni mesures obligatoires. Ces meilleures pratiques visent à promouvoir l'échange d'informations, à donner des avis généraux et à coordonner les informations destinées aux autorités gouvernementales qui ont besoin d'orientations et sont chargées d'assurer la protection des infrastructures énergétiques critiques.

Des meilleures pratiques ont ainsi été élaborées en ce qui concerne la protection des infrastructures électriques et gazières critiques. Un catalogue des meilleures pratiques pour les infrastructures pétrolières critiques est également en cours d'élaboration. Les autorités compétentes peuvent utiliser ces politiques pour s'assurer qu'elles mêmes appliquent bien ces meilleures pratiques et que les opérateurs prennent les mesures nécessaires pour garantir la protection des infrastructures critiques.

Dieter Urban, président du Comité de planification industrielle

Les attaques qui ont visé l'Estonie au printemps 2007, menées par le biais de l'Internet contre des sites web publics, ont rappelé combien, dans les sociétés modernes ouvertes, les systèmes clés étaient vulnérables aux agissements hostiles. Ligia Ferreira, présidente du Comité d'étude des télécommunications civiles (CCPC) de l'OTAN, explique les risques et les défis que pose une société d'information interconnectée. Suleyman Anil, chef du Centre de coordination et de soutien pour la cyberdéfense (CDCSC) de l'OTAN, explique les mesures prises par l'OTAN pour renforcer la protection de ses systèmes d'information et de communication contre les attaques qui visent à perturber ces systèmes en y accédant de manière illégale.

Risques et défis dans une société interconnectée

Les réseaux de communications électroniques constituent l'ossature de la société de l'information d'aujourd'hui. Ces « systèmes répartis » interconnectés et complexes ont entraîné, dans tous les secteurs, une augmentation massive de l'utilisation d'ordinateurs, d'infrastructures, de services et d'applications électroniques, que l'on désigne collectivement par le terme technologies de l'information et de la communication (TIC). En outre, l'infrastructure nécessaire pour faire fonctionner ces systèmes 24 heures sur 24 et 7 jours sur 7 dans le monde entier est, par nécessité, interconnectée et interdépendante. Tous ces facteurs créent un environnement extrêmement difficile – et vecteur de risques – dans lequel les pays doivent évoluer. Heureusement, l'OTAN possède plusieurs organes et mécanismes pour faire face à bon nombre de problèmes que pose cette situation. À ce titre, le Comité d'étude des télécommunications civiles (CCPC) est un organe essentiel.

Le CCPC, créé il y a plus de 50 ans, est chargé de donner des avis aux pays membres de l'OTAN et du Conseil de partenariat euro atlantique (CPEA) sur toutes les questions relatives aux télécommunications civiles dans le cadre de la préparation du secteur civil aux situations d'urgence. Il a également pour mission de développer et de coordonner les dispositions nécessaires afin de garantir dans toute la mesure possible, en période de crise, une disponibilité constante des télécommunications civiles. Cela implique, entre autres, d'élaborer et d'adresser aux pays des recommandations concernant les technologies nouvelles et naissantes, s'agissant notamment de la cybersécurité et de la cybedéfense.

La cybersécurité, qui consiste à protéger les informations en prévenant et en détectant les attaques et en y répondant, est essentielle à tous les niveaux. Les gouvernements doivent sécuriser leurs réseaux et systèmes d'information électroniques afin de protéger toutes les activités publiques comme la défense militaire, la logistique, le transport et les systèmes financiers, les infrastructures, et les informations personnelles des citoyens. L'une des préoccupations majeures, pour les gouvernements, tient au fait qu'une cyberattaque dirigée contre un système ou un secteur gouvernemental pourrait bien avoir de graves conséquences pour d'autres.

Les auteurs de cyberattaques peuvent être des personnes, des éléments criminels ou des aventuriers, ou ils peuvent agir pour le compte de gouvernements ou d'organisations transnationales hostiles. Leur capacité, leur motivation et leur volonté d'exploiter des faiblesses semblent sans limites. De plus, il est presque impossible de remonter jusqu'à la véritable source d'attaques complexes, et l'anonymat dont bénéficient par conséquent les auteurs de cyberattaques crée des problèmes importants pour les pays touchés qui essaient de réagir face aux attaques.

Des cyberattaques menées lors de catastrophes naturelles ou technologiques, ou lors d'autres crises comme des attaques terroristes, pourraient avoir des conséquences catastrophiques pour la viabilité d'un pays. De telles attaques pourraient perturber gravement la circulation normale des informations entre les différents ministères ou organismes gouvernementaux. Elles pourraient empêcher les communications avec les parties touchées de la population. Elles pourraient également entraver l'action menée par les organismes de secours d'urgence en vue d'intervenir rapidement et de manière appropriée dans les zones touchées. Enfin, elles pourraient entraver la capacité d'un pays à coopérer avec ses voisins ou avec des partenaires régionaux dans le cadre d'opérations de réponse à une crise ou une catastrophe multinationale.

Ligia Ferreira, présidente du Comité d'étude des télécommunications civiles (CCPC) de l'OTAN

Le CCPC participe directement aux efforts en matière de cybersécurité depuis 2003. Dans le cadre de son programme de travail actuel, il évalue au niveau des pays les vulnérabilités existantes et potentielles des réseaux de communications électroniques vis-à-vis des cyberattaques. D'autres menaces sont également étudiées, notamment celles liées à la fuite passive d'informations émanant de composants ou de systèmes électroniques. À la demande des pays, le CCPC a déjà étudié d'autres questions liées à la cybersécurité : conséquences des cyberattaques, protection des infrastructures d'information critiques, utilisation éventuelle de schémas de hiérarchisation afin d'atténuer les effets de surcharges ou de pannes des systèmes.

Un groupe d'experts de la cyberdéfense, basés dans les pays mais à l'écoute des besoins de l'OTAN dans le cadre des dispositions pour la gestion des crises dans le domaine des plans civils d'urgence, vient compléter les efforts du Comité. Ces experts peuvent répondre à des demandes de soutien et d'avis émanant de pays du CPEA, du Dialogue méditerranéen et de l'Initiative de coopération d'Istanbul, ou du secteur militaire de l'OTAN. Certains pays ont déjà sollicité un tel soutien pour faire face à de véritables situations de crise ou pour faciliter la mise en place de programmes relatifs à la cyberdéfense. Les mêmes experts peuvent aussi aider d'autres organes de l'OTAN qui s'occupent de cybsersécurité, par exemple le Centre OTAN de réaction aux incidents informatiques (voir article de M. Anil), le Bureau des C3 de l'OTAN et d'autres structures.

Évidemment, le CCPC ne travaille pas de manière isolée. Le Comité est composé de hauts représentants des ministères nationaux chargés des communications, dont un grand nombre participent aussi en tant que représentants nationaux aux activités des secteurs des technologies de l'information et de la communication dans des organisations internationales comme l'Union internationale des télécommunications (UIT) des Nations Unies ou l'Union européenne. Il existe par conséquent une importante circulation informelle croisée d'informations entre les organisations, ce qui contribue à limiter les doubles emplois.

La société de l'information interconnectée d'aujourd'hui reflète les besoins actuels en même temps qu'elle donne des indications sur l'environnement futur. Les dépendances des personnes, des pays et des alliances internationales vis-à-vis des services, des infrastructures et des applications électroniques iront certainement croissant, ce qui devrait entraîner parallèlement une augmentation des besoins en matière de cybersécurité. Les pays de l'Alliance ont clairement défini le rôle de l'OTAN dans ce domaine, et le CCPC continuera de remplir ses responsabilité dans le cadre de l'équipe.

Défense contre les cyberattaques

Les premiers cas de cyberattaques contre des systèmes d'information de l'OTAN ont été signalés vers la fin des années 1990, pendant les opérations menées par l'OTAN dans les Balkans. Certaines de ces attaques ont entraîné la compromission de systèmes d'information et de communication de l'OTAN, provoquant des interruptions de services opérationnels. S'appuyant sur les enseignements tirés des opérations dans les Balkans, les gouvernements ont appelé en 2002, lors du sommet de l'OTAN à Riga, à « améliorer la protection des systèmes d'information clés contre les cyberattaques ». Cette déclaration a ouvert la voie à plusieurs initiatives internes à l'OTAN, destinées à améliorer le dispositif de cybersécurité de l'Alliance. L'effort le plus significatif et le plus ambitieux a été le lancement du projet de capacité OTAN de réaction aux incidents informatiques (NCIRC), en 2003. La NCIRC, opérationnelle depuis fin 2005, a pour mission de réagir face aux incidents de sécurité signalés sur les réseaux de l'OTAN.

En mai 2007, le monde a assisté aux cyberattaques qui ont frappé les infrastructures informatiques et les services en ligne d'un pays membre de l'OTAN – l'Estonie – à la suite d'un conflit politique. Ces attaques, les premières du genre, ont duré environ trois semaines et ont mis en évidence le chaos et les perturbations que des attaques visant un cyberespace national peuvent provoquer au niveau des services publics et financiers comme au niveau des médias. Après les cyberattaques, les pays membres de l'OTAN ont décidé de prendre d'autres mesures afin d'améliorer les capacités de cyberdéfense de l'Alliance, l'objectif étant notamment de pouvoir fournir une aide technique et opérationnelle à un pays membre qui en ferait la demande.

Süleyman Anil, chef du Centre de coordination et de soutien pour la cyberdéfense de l'OTAN – siège de l'OTAN, Bruxelles.

Cybersécurité

La politique de cyberdéfense de l'OTAN est exposée en détail dans une série de documents de haut niveau qui définissent les principes, les processus de prise de décisions et les procédures, l'objectif étant de garantir une approche commune et coordonnée de l'OTAN vis-à-vis de la cyberdéfense ainsi qu'une capacité de réaction face aux cyberattaques. L'Autorité de gestion de la cyberdéfense (CDMA) de l'OTAN est chargée de prendre et de coordonner les mesures de cyberdéfense immédiates et effectives requises au sein de l'OTAN et entre les pays, lorsque cela est nécessaire. En tant que partie prenante à la CDMA de l'OTAN, les PCU jouent un rôle important dans l'aide apportée aux pays membres et partenaires en établissant des procédures et en facilitant les contacts au sein de l'OTAN.

Les menaces qui concernent l'OTAN sont les cyberattaques parrainées par les États qui visent l'OTAN et les pays membres lors d'un conflit politique ou militaire. Ces formes d'attaques, auxquelles il est le plus difficile de répondre, peuvent avoir des conséquences importantes, en particulier pour les pays possédant des infrastructures informatiques nationales de mauvaise qualité ou de faibles dimensions. De telles attaques peuvent déstabiliser la sécurité nationale, provoquer des pertes économiques considérables et perturber les services publics et commerciaux pendant des jours ou des semaines. Les cyberattaques parrainées par des États sont aussi fréquemment utilisées à des fins d'espionnage et de collecte d'informations. Les cybermenaces émanant de groupes terroristes sont actuellement considérées comme faibles, mais elles devraient s'accroître à court terme.

La mise en œuvre d'une capacité nationale efficace de cyberdéfense est techniquement difficile, mais faisable si elle bénéficie d'une bonne planification et d'un soutien politique. En supposant qu'une stratégie nationale de cyberdéfense soit élaborée et mise en application grâce à une législation appropriée, la mise en œuvre d'une capacité nationale de cyberdéfense nécessiterait : (1) un centre opérationnel, chargé d'assurer les services techniques et opérationnels; (2) un centre de coordination, chargé d'élaborer et de coordonner une stratégie et des concepts, de régler les aspects juridiques, et d'entretenir des relations avec l'industrie et les organisations internationales; (3) un organe exécutif, au sein duquel les décisions seraient proposées, examinées et entérinées en vue de leur mise en application. Le Centre opérationnel de la cyberdéfense mobiliserait la plus grande partie du financement et des ressources humaines. Le coût dépend du volume du cyberespace à protéger (c'est-à-dire, des réseaux et des infrastructures informatiques) et du type de services centralisés que propose le Centre.

L'actuelle structure de cyberdéfense de l'OTAN (NCIRC – Capacité OTAN de réaction aux incidents informatiques) gère quotidiennement des centaines de milliers d'événements électroniques en vue de détecter d'éventuelles activités malveillantes et de réagir de manière appropriée. À ce jour, plus de 800 incidents de cybersécurité – dont certains auraient pu avoir d'importantes conséquences – ont été suivis de manière formelle. Ces incidents vont des défacements sur le web au cyberespionnage, en passant par les pénétrations importantes de réseaux.

Pour l'avenir proche, l'OTAN prévoit de mettre en œuvre des mesures destinées à renforcer davantage ses capacités de cyberdéfense et à améliorer l'assistance aux pays ainsi que la collaboration avec l'industrie et les organisations internationales.

Photos du Centre opérationnel de la Capacité OTAN de réaction aux incidents informatiques (NCIRC).

Le défi grandissant que représente la piraterie dans le golfe d'Aden et au large de la corne de l'Afrique menace l'action humanitaire internationale, ainsi que la sécurité des routes maritimes commerciales. À la demande de l'ONU, l'OTAN contribue activement à accroître la sécurité en menant des opérations de lutte contre la piraterie dans la région. Dans l'article qui suit, Jim Caponiti décrit le rôle joué par le Bureau d'étude des transports océaniques de l'OTAN dans la prévention des actes de piraterie, ainsi que d'autres efforts de coordination au niveau international.

Aider à prévenir les actes de piraterie

Le Bureau d'étude des transports océaniques (PBOS), l'un des huit bureaux et comités d'étude qui relèvent du Haut Comité pour l'étude des plans d'urgence dans le domaine civil (SCEPC), donne des avis à l'OTAN sur les mesures antiterroristes visant à protéger les moyens maritimes civils et suit tous les développements liés à la sécurité ayant des incidences sur les transports maritimes commerciaux. La piraterie est actuellement un problème qui a des incidences sur les transports maritimes commerciaux, notamment au large des côtes somaliennes.

Le PBOS, par l'intermédiaire de ses représentants nationaux et de ses experts civils des transports maritimes, axe essentiellement ses travaux sur la piraterie et sur l'identification des pratiques permettant de prévenir les actes de piraterie. À l'origine, c'est le détroit de Malacca et ses environs qui étaient au centre des préoccupations ; plus récemment, ce sont le golfe d'Aden et les eaux situées au large des côtes somaliennes qui sont passés au devant de l'actualité. Les actes de piraterie sont des délits qui menacent la liberté de navigation, la sécurité des équipages et les échanges commerciaux.

Le PBOS continue d'échanger des informations sur la piraterie, d'analyser les efforts visant à régler ce problème, de donner aux autorités militaires de l'OTAN (NMA) et aux autorités nationales des avis sur des questions de transport maritime, d'apporter des contributions en ce qui concerne les meilleures pratiques permettant de prévenir les actes de piraterie, et de faire connaître ces dernières. Le PBOS est bien placé pour fournir aux pays alliés et aux pays partenaires des directives, contraignantes ou non, destinées à prévenir les actes de piraterie.

De nombreuses actions sont actuellement entreprises pour prévenir les actes de piraterie et le PBOS s'en félicite. La poursuite de la coopération entre les gouvernements et le secteur industriel aidera à réduire le nombre des actes de piraterie.

Un autre groupe, étroitement aligné sur le PBOS, traite lui aussi de la lutte contre la piraterie. Il s'agit du Groupe de contact sur la piraterie au large de la Somalie (CGPCS), qui a été créé dans le cadre de l'application de la résolution 1851 du Conseil de sécurité des Nations Unies. Le CGPCS, qui est composé de vingt-huit pays et de six organisations internationales, dont l'OTAN, sert de point de contact commun entre les pays, les organisations régionales et les organisations internationales pour tous les aspects liés à la lutte contre les actes de piraterie et les vols à main armée perpétrés au large des côtes somaliennes. Le CGPCS dispose de quatre groupes de travail, qui se réunissent régulièrement et formulent des recommandations pour la prévention des actes de piraterie.

Le premier groupe de travail, dirigé par le Royaume-Uni, se concentre sur les aspects militaires et s'occupe de la coordination opérationnelle et du développement de capacités régionales. Le deuxième groupe de travail, dirigé par le Danemark, s'emploie à recenser des solutions pratiques et juridiquement valables, qui permettent de poursuivre en justice les personnes suspectées d'actes de piraterie. Le troisième groupe de travail, dirigé par les États-Unis, travaille en priorité sur la protection et la sensibilisation du secteur industriel. Le quatrième groupe de travail, dirigé par l'Égypte, s'occupe de la diplomatie publique et des communications.

Des progrès sont réalisés pour régler le problème de la piraterie mais il reste des défis à relever. Le PBOS continuera de collaborer avec les organisations compétentes pour régler le problème de la piraterie et pour recenser les mesures et les processus qui aideront les transporteurs commerciaux à éviter, à prévenir et à empêcher les actes de piraterie.

James E. Caponiti, président du Bureau d'étude des transports océaniques de l'OTAN

Les problèmes de santé publique, comme les pandémies (SIDA, grippe, etc.), transcendent les frontières nationales. Ils peuvent être porteurs de risques majeurs pour l'ordre social, et les approches traditionnellement suivies en matière de santé publique peuvent s'avérer inadéquates. De plus, les États n'étant pas en mesure de faire face seuls à de tels problèmes, la coopération internationale est indispensable. Éric Lecarpentier, président du Comité médical mixte de l'OTAN, fait le point sur l'épidémie de grippe A(H1N1) et sur les mesures prophylactiques appropriées.

La Grippe A(H1N1)

La grippe est une infection respiratoire aiguë, très contagieuse, due aux virus Influenzae. Au XXe siècle, on a dénombré trois pandémies grippales. En 1918-1919, la pandémie dite de la «grippe espagnole» (virus A/H1N1) a touché le monde entier. Les estimations, disponibles sur le site de l'Organisation mondiale de la santé (OMS), indiquent qu'au moins 40 millions de personnes en sont décédées.
Les pandémies suivantes ont été beaucoup moins sévères : en 1957-58, la «grippe asiatique» (virus A/H2N2) et en 1968-69, la «grippe de Hong-Kong» (virus A/H3N2).
Les épidémies de grippe surviennent chaque année au cours de l'automne et de l'hiver dans les régions tempérées. Elles provoquent des hospitalisations et des décès principalement parmi les groupes à haut risque (très jeunes, personnes âgées ou maladies chroniques). Au niveau mondial, ces épidémies annuelles sont responsables d'environ trois à cinq millions de cas de maladies graves, et 250 000 à 500 000 décès. La plupart des décès associés à la grippe dans les pays industrialisés surviennent parmi les personnes âgées de 65 ans ou plus. Dans certains pays tropicaux, les virus grippaux circulent tout au long de l'année avec un ou deux pics au cours de la saison des pluies.
Les virus grippaux se répartissent en différents types : A, B et C. Les virus A et B sont à l'origine des épidémies saisonnières, seul le virus A peut être responsable de pandémies. Le virus C occasionne des cas sporadiques. Les virus grippaux se caractérisent par leurs fréquentes mutations. Cette évolution génétique se fait :

- soit par glissement (« shift ») lors des épidémies saisonnières;
- soit par cassure (« drift »). Ce dernier phénomène ne concerne que les virus de type A. Il est responsable de l'apparition de nouveaux virus contre lesquels la population n'est pas protégée et génère des pandémies grippales.

Les virus grippaux de type A se subdivisent en sous-types en fonction des différentes sortes et associations de protéines de surface du virus. Les sous-types des virus grippaux sont du type A(HxNx). Dans l'épidémie actuelle, il s'agit d'un « nouveau » virus qui se transmet d'homme à homme il appartient à la famille A(H1N1). Il résulte de phénomènes de recombinaisons à partir de virus de porc, humain et aviaire. Ce virus est différent du virus H1N1 de la grippe saisonnière, virus d'origine humaine qui circule habituellement durant la saison hivernale.

L'épidémie de grippe saisonnière survient chaque année dans l'hémisphère nord entre les mois de novembre et d'avril. Elle dure en moyenne 9 semaines. La mortalité imputable à la grippe saisonnière concerne essentiellement les sujets âgés (plus de 90 % des décès liés à la grippe surviennent chez des personnes de 65 ans et plus).

Une pandémie et une épidémie se définissent toutes deux comme une forte augmentation des cas d'une même maladie à un moment donné. La différence se situe dans l'étendue du phénomène : la pandémie se caractérise par une diffusion géographiquement très étendue à plusieurs ou tous les continents à l'occasion de l'apparition d'un nouveau sous-type de virus résultant d'une modification génétique. Le virus possédant des caractéristiques nouvelles, l'immunité de la population est faible ou nulle. Il peut en résulter un nombre important de cas graves ou de décès. La plupart des gens ne sont pas ou sont peu immunisés contre celui-ci et il pourrait donc provoquer davantage d'infections que la grippe saisonnière. La majorité des personnes qui contractent le virus sont atteintes de la forme bénigne de la maladie et guérissent sans traitement antiviral ni soins médicaux. Parmi les cas plus graves, plus de la moitié des personnes hospitalisées souffraient de pathologies sous-jacentes ou avaient un système immunitaire affaibli.
On défini :

la virulence par la capacité d'un virus ou d'un agent infectieux d'induire une maladie grave;
la contagiosité par la capacité d'un virus ou d'un agent infectieux d'être transmis d'une personne à l'autre.

En raison de l'extension mondiale de l'épidémie de grippe à nouveau virus A(H1N1), l'OMS a déclaré le 11 juin 2009 le passage en phase 6 de son plan et confirmé la situation de pandémie mondiale.
Le virus se transmet d'homme à homme aussi facilement que celui de la grippe saisonnière normale.
Pour prévenir la propagation de la maladie, les personnes malades doivent se couvrir le nez et la bouche lorsqu'elles toussent ou éternuent, rester chez elles si elles ne se sentent pas bien, se laver les mains régulièrement et se tenir autant que possible à l'écart des personnes bien portantes. On n'a connaissance d'aucun cas d'infection humaine consécutive à une exposition à des porcs ou à d'autres animaux. Les premiers signes de la grippe A(H1N1) sont de type grippal: fièvre supérieure à 38°, ou

Dr Eric Lecarpentier, président du Comité médical mixte - OTAN

courbatures, ou grande fatigue et toux ou difficultés respiratoires, maux de tête, maux de gorge et écoulements nasals, parfois accompagnés de vomissements ou de diarrhée.

Dans le cadre de l'épidémie actuelle, la transmission se fait de la même manière que celle d'une grippe saisonnière :
- par la voie aérienne, c'est-à-dire la dissémination dans l'air du virus par l'intermédiaire de la toux, de l'éternuement ou des postillons;
- par le contact rapproché avec une personne infectée (lorsqu'on l'embrasse ou qu'on lui serre la main);
- par le contact avec des objets touchés et donc contaminés par une personne malade (exemple : une poignée de porte).

Une personne malade est contagieuse dès les premiers symptômes et pendant environ 7 jours, La période d'incubation peut aller jusqu'à 7 jours. Elle doit donc s'isoler et porter un masque anti-projections quand elle est en présence d'une autre personne pendant toute cette période pour éviter de contaminer son entourage.
Pour diminuer le plus possible la transmission du virus il faut:
- éviter tout contact avec une personne malade;
- se laver régulièrement les mains au savon ou les désinfecter avec une solution hydro-alcoolique (disponible en pharmacies et grandes surfaces), notamment après avoir toussé ou s'être mouché;
- se couvrir la bouche et le nez quand on tousse ou éternue avec un mouchoir à usage unique (à jeter dans une poubelle fermée, si possible par un couvercle et équipée d'un sac plastique), ou avec le bras ou la manche ou avec les mains (s'il est possible de se les laver immédiatement après).

Il existe deux 2 types de masques :
- le masque anti-projections (de type chirurgical) réservé aux personnes malades (à porter dès les premiers symptômes) afin qu'elles évitent de contaminer d'autres personnes/leur entourage (lorsqu'elles toussent, éternuent…). Le virus se transmet par dissémination dans l'air. Le risque de contamination existe à partir d'une proximité, en face à face, de moins d'un mètre d'une personne malade;
- le masque de protection respiratoire (masque FFP2) réservé aux professionnels dont le rôle en situation de pandémie serait capital et qui seraient amenés à être en contact régulier et rapproché avec des malades (professionnels de santé, services de secours…). C'est un appareil de protection respiratoire jetable qui protège celui qui le porte contre l'inhalation d'agents infectieux transmissibles par voie aérienne.

En cas d'apparition de symptômes grippaux, chaque pays a mis une organisation spécifique en place. En France il est actuellement recommandé d'aller chez son médecin traitant ou d'appeler le centre départemental de coordination des urgences médicales le centre 15. En Angleterre, un centre national de réception des appels et de coordination sanitaire à été créé. Toutes les organisations s'accordent à préconiser l'isolement des patients et de les encourager à rester à domicile. Seuls les cas graves ou les personnes à risque (femmes enceintes, enfants en bas âges, personnes immunodéprimés, personnes fragiles…) sont susceptibles d'être hospitalisées.

Lors de la période d'isolement volontaire d'un proche malade, une prise en charge médicale et un suivi régulier sont assurés par des médecins. Vous devez limiter les contacts rapprochés avec cette personne. Si vous devez entrer en contact avec lui durant sa période d'isolement volontaire, veillez à lui faire porter un masque et à respecter strictement les gestes d'hygiènes (mesures barrière) pour éviter d'être contaminé à votre tour :

- ne pas embrasser ni serrer les mains du malade;
- réduire les visites au strict minimum;
- faire porter un masque anti-projections au malade;
- observer une hygiène rigoureuse des mains : au domicile, lavage des mains au savon ordinaire (distinct de celui du malade) ou désinfection avec une solution hydro-alcoolique, en particulier après chaque contact :
  - avec le malade;
  - avec le matériel utilisé par lui;
  - avec ses effets personnels;
  - avec des surfaces ayant été touchées par le malade (poignées de portes, meubles, chasse d'eau…);
- bien aérer l'endroit où l'on vit en ouvrant les fenêtres;
- laver au savon ou produits ménagers habituels et à l'eau chaude les objets courants du patient (serviettes, couverts, linge, etc.);
- nettoyer les surfaces ayant été touchées par le malade (poignées de portes, chasse d'eau, télécommande, téléphone…) au savon et à l'eau chaude ou avec les produits ménagers habituels.

Si vous ne vous sentez pas bien, présentez une forte fièvre, de la toux et/ou un mal de gorge :

- restez chez vous et évitez de vous rendre sur votre lieu de travail, votre école ou à des rassemblements;
- reposez-vous et absorbez des liquides en abondance;
- couvrez-vous le nez et la bouche de mouchoirs en papier lorsque vous toussez et que vous éternuez et éliminez-les ensuite correctement. Lavez-vous ensuite les mains soigneusement avec du savon ou une solution hydroalcoolique;
- si vous n'avez pas de mouchoirs en papier pour vous moucher ou pour tousser, faites-le dans le creux de votre coude;
- lavez-vous les mains à l'eau et au savon fréquemment et soigneusement, surtout après avoir toussé ou éternué;
- informez votre famille et vos amis de votre maladie et recherchez de l'aide pour les tâches ménagères qui supposent des contacts avec d'autres gens, par exemple les courses.

QUELS SONT LES TRAITEMENTS DISPONIBLES ?

Seul un médecin peut juger de la prescription d'un traitement, qu'il adaptera à chaque patient, en fonction de son état de santé. Ce traitement peut ne comporter qu'une prescription de médicaments contre la fièvre et des conseils en matière d'hygiène ou un traitement antiviral.
Les masques anti-projections doivent être portés par la personne malade dès les premiers symptômes pour éviter de contaminer son entourage.

Un vaccin sera disponible à partir de l'automne 2009.
Les médicaments antiviraux : l'oseltamivir (Tamiflu ®) et le zanamivir (Relenza ®) sont efficaces sur ce virus.
Ils sont délivrés que dans le cadre d'une prescription médicale après consultation et diagnostic réalisés par un médecin, dès l'apparition des premiers symptômes. Ils ne constituent en aucun cas un traitement préventif.
Les produits antiviraux sont des médicaments employés pour le traitement précoce de la grippe. Quand ils sont pris rapidement dès le début de la maladie, ils peuvent atténuer les symptômes de la grippe, raccourcir la durée de la maladie et probablement prévenir les complications. Les traitements antiviraux réduisent la capacité de reproduction du virus, mais par contre n'immunisent pas contre le virus.
Les vaccins sont le principal outil de prévention de la maladie causée par la grippe, comme d'autres infections. Ils provoquent l'immunisation du patient en stimulant sa production d'anticorps contre le virus.
Un délai prévu de plusieurs semaines est encore nécessaire pour que le vaccin soit disponible. En fonction des tests cliniques, des autorisations de mise sur le marché et des rendements de production, la livraison du vaccin pourrait s'échelonner sur quatre mois à partir de l'automne.

En ce qui concerne les voyages internationaux il est conseillé la prudence aux voyageurs qui se rendent dans les pays où la transmission communautaire du virus est confirmée.
A ce jour, l'Organisation mondiale de la Santé (OMS) ne recommande pas de restreindre les voyages à cause de la nouvelle grippe A(H1N1). Aucune recommandation particulière n'a été émise au niveau européen.
Il est préconisé de :

- se conformer aux recommandations émises par les autorités sanitaires locales;
- respecter les mesures d'hygiène de base (se laver les mains fréquemment, aérer les lieux de vie), éviter tout contact avec une personne malade;
- en cas de fièvre ou de symptômes grippaux : consulter un médecin localement.

Le programme OTAN « La science au service de la paix » permet régulièrement à des scientifiques et à des experts des pays de l'OTAN et des pays partenaires de participer à des programmes d'intérêt commun. Il vise à contribuer à la sécurité, à la stabilité et à la solidarité entre pays en appliquant les derniers développements scientifiques à la résolution de problèmes. Le projet ci-dessous concerne les activités PCU visant la mise en place de capacités de cyberdéfense dans les pays partenaires.

Le programme scientifique de l'OTAN contribue à la cybersécurité dans les pays partenaires

La sécurité des infrastructures et des systèmes informatiques est un véritable défi. Lorsqu'un incident survient en matière de sécurité informatique, les organisations doivent être à même de réagir rapidement et efficacement afin de limiter les éventuels dégâts.

Disposer d'une équipe de réaction aux incidents de sécurité informatique (CSIRT) permet d'améliorer de manière efficace la capacité de réaction rapide et d'atténuer les conséquences d'attaques futures. Les CSIRT sont de petites unités d'une à trois personnes équipées et formées pour réagir rapidement, 24 heures sur 24 et 7 jours sur 7. Leur objectif est de transmettre efficacement des informations importantes relatives à la sécurité.

En 2006, dans le cadre de son programme pour la science au service de la paix et de la sécurité, l'OTAN a lancé un projet visant à créer des CSIRT dans quinze pays n'ayant aucun système de sécurité informatique : Afghanistan, Albanie, Arménie, Azerbaïdjan, Bélarus, Bulgarie, Géorgie, Kazakhstan, République kirghize, ex-République yougoslave de Macédoine*, Moldova, Tadjikistan, Turkménistan, Ukraine et Ouzbékistan.

Grâce à ce projet, chaque pays a obtenu un « kit de démarrage » lui permettant de mettre les CSIRT sur pied. Il s'agissait d'un serveur dédié avec un système de logiciels de gestion des incidents, d'une station de travail, d'un routeur, d'un commutateur, de logiciels, d'une imprimante multifonctions, d'une déchiqueteuse et de manuels. L'OTAN a veillé à ce que les équipements soient livrés à chaque pays et a apporté son aide pour l'installation et la mise en route. En outre, les fonds OTAN ont permis de former, à des normes mondiales bien précises, jusqu'à trois opérateurs par pays.

Bien que la supervision générale du projet et de son exécution continue de se faire dans le cadre du programme pour la science au service de la paix et de la sécurité, d'autres acteurs clés sont intervenus. Le réseau national de recherche et d'enseignement (NREN) de chaque pays était chargé de la sécurité du personnel et des bureaux nécessaires. L'association de constitution de réseaux en Europe centrale et orientale qui regroupe les NREN des pays d'Europe centrale, d'Europe du Sud-Est, du Caucase et d'Asie centrale, a coordonné l'acquisition et la livraison des équipements et a apporté l'assistance technique requise pour leur installation.

Par ailleurs, tous les aspects des projets ont été étroitement coordonnés avec l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).

Jusqu'à présent, les résultats sont très encourageants. Les CSIRT fonctionnent bien dans la plupart des pays et les progrès sont minutieusement et régulièrement suivis.

Le programme pour la science au service de la paix et de la sécurité devrait continuer de prévoir ce type d'activité à l'avenir, l'objectif étant de mettre au point des capacités d'audit et de certification de sécurité. En outre, le projet permettra de préparer les NREN et les CSIRT en vue de leur participation à une série d'exercices de réaction rapide en matière de sécurité informatique prévus pour 2010 2011. La participation à de tels exercices à l'échelle mondiale est en effet le fruit des travaux que les équipes des pays partenaires mènent depuis 2006.

Le projet est en outre un excellent exemple des résultats concrets que la coopération pratique entre l'OTAN et ses Partenaires peut donner dans le domaine de la cyberdéfense.

* La Turquie reconnaît la République de Macédoine sous son nom constitutionnel.

Jayne Clinton, Publications scientifiques et projets de marketing, Division Diplomatie publique de l'OTAN

DÉVELOPPEMENTS INTERVENUS AU SEIN DU HAUT COMITÉ POUR L'ÉTUDE DES PLANS D'URGENCE DANS LE DOMAINE CIVIL (SCEPC)

Cet automne, le SCEPC et les PB&C aborderont plusieurs questions de principe importantes. Le SCEPC examinera notamment les recommandations formulées à l'occasion de l'atelier sur le soutien à l'Afghanistan dans le cadre des PCU, qui s'est tenu au siège de l'OTAN les 1er et 2 juillet 2009, et il décidera de la marche à suivre pour les concrétiser. Cet atelier avait en effet pour but de déterminer, en fonction des demandes, comment les acteurs des PCU de l'OTAN peuvent, conjointement avec les acteurs civils nationaux et internationaux, contribuer à répondre aux besoins en matière de soutien à apporter aux autorités afghanes et à la FIAS dans le domaine civil.

La prochaine directive ministérielle pour les PCU, qui tiendra compte du contexte OTAN général et des résultats de la revue des PCU, sera élaborée dans les prochaines semaines. Comme le prévoit le cycle d'établissement et d'examen des PCU, la directive ministérielle et les programmes de travail des PB&C porteront désormais sur une période de quatre ans. Le SCEPC examinera et approuvera le programme de travail 2010-2013 au cours du premier trimestre 2010. L'élaboration de la directive ministérielle fait intervenir toutes les parties prenantes et fixe les objectifs des PCU de l'OTAN pour les quatre années à venir. Les partenaires de l'OTAN sont associés à ce processus dans toute la mesure possible.

Plusieurs activités pratiques et séminaires feront avancer les projets PCU. L'exercice de secours en cas de catastrophe « ZHETYSU 2009 » notamment, qui est organisé par l'EADRCC, se tiendra du 5 au 11 septembre 2009. Cet exercice a pour but d'améliorer l'interopérabilité entre les primo-intervenants et de constituer dans les pays membres et dans les pays partenaires, des capacités qui leur permettront de gérer des situations d'urgence complexes. Le séminaire sur les transports est un autre événement important, qui se tiendra du 26 au 28 octobre 2009 en Belgique et auquel participeront principalement les PB&C chargés des transports (le Comité d'étude de l'aviation civile, le Bureau d'étude des transports océaniques et le Bureau d'étude des transports intérieurs de surface). Ce séminaire sur les transports multimodaux examinera les incidences de la conjoncture économique sur le secteur des transports et sur le soutien que celui-ci peut apporter aux opérations de l'OTAN.

Chantiers du SCEPC

- Directive ministérielle pour 2010-2013
- Suite à donner à l'atelier sur le soutien à l'Afghanistan dans le cadre des PCU

REGARD VERS L'AVENIR

Calendrier du SCEPC et des PB&C

1-3 septembre	Séminaire et réunion plénière du CPC	Cracovie, Pologne
9-10 septembre	Réunion plénière du CAPC	Siège de l'OTAN, Belgique
14-15 septembre	Réunion plénière du PBOS	Siège de l'OTAN, Belgique
18 septembre	Réunion plénière du CPC	Siège de l'OTAN, Belgique
30 sept – 2 oct	Conférence médicale de l'OTAN	Lisbonne, Portugal
26-27 octobre	Réunion plénière du CCPC	Siège de l'OTAN, Belgique
26-28 octobre	Séminaire sur les transports	Anvers, Belgique
5-6 novembre	Réunion plénière du Comité médical mixte	Siège de l'OTAN, Belgique
11-12 novembre	Séminaire sur les infrastructures énergétiques essentielles	Vilnius, Lituanie
12-13 novembre	Séminaire et réunion plénière de l'IPC	Vilnius, Lituanie
17-18 novembre	Réunion plénière du FAPC	Siège de l'OTAN, Belgique
23-24 novembre	Réunion plénière du PBIST	Siège de l'OTAN, Belgique
24-25 novembre	Réunion plénière du SCEPC	Siège de l'OTAN, Belgique
3-4 décembre	Réunion des ministres des Affaires étrangères des pays de l'OTAN	Siège de l'OTAN, Belgique

Le Centre euro-atlantique de coordination des réactions en cas de catastrophe (EADRCC)

Le Centre euro-atlantique de coordination des réactions en cas de catastrophe (EADRCC) est un organisme du Partenariat auquel Partenaires et Alliés participent sur un pied d'égalité. Il est l'organe centralisateur pour l'échange d'informations sur les catastrophes dans les pays du CPEA. Le programme d'exercices sur le terrain de l'EADRCC est l'un des meilleurs au monde. L'article qui suit décrit un nouveau projet appelé Aidmatrix, qui vise à faciliter la diffusion d'informations sur les secours en cas de catastrophe.

Aidmatrix

L'EADRCC recherche depuis un certain temps une solution moderne permettant de diffuser des informations sur les secours en cas de catastrophe. Habituellement, le centre établit des rapports par cycles de 12 à 24 heures qui sont ensuite envoyés aux pays du CPEA par courriel ou par fax. C'est une manière éprouvée de communiquer des informations et le centre continuera de l'utiliser. Il existe toutefois des méthodes plus perfectionnées consistant à afficher en permanence sur un panneau électronique virtuel l'information, qui peut être extraite sur demande.

NATO OTAN

aidmatrix
Right Aid. Right People. Right Time.™

Grâce à la délégation des États-Unis auprès de l'OTAN, qui a facilité la mise en relation entre l'EADRCC et l'Aidmatrix Foundation, le centre a pu trouver un outil moderne pour la diffusion d'informations sur les secours en cas de catastrophe. Ce nouvel outil, qui s'appelle Aidmatrix, accé-lérera les comptes rendus sur les secours en cas de catastrophe, lesquels seront aussi plus transparents et plus efficaces.

Aidmatrix a pour devise de fournir « l'aide appropriée aux personnes voulues au bon moment ». Aidmatrix est un organisme à but non lucratif qui met en rapport, par l'intermédiaire de son réseau, les donateurs avec les personnes qui ont besoin d'aide. Trente-huit États américains, l'agence américaine FEMA, le Honduras et la Roumanie ont recours à ce réseau. Il est utilisé pour la plupart des dons d'aide alimentaire aux États Unis et pour les dons de produits médicaux.

Dans le domaine des secours en cas de catastrophe, Aidmatrix s'est lancé le défi de créer un « tableau pour les secours en cas de catastrophe », qui améliore l'acheminement de l'aide humanitaire lors des interventions et pendant la reprise des activités. Ce tableau automatise en effet une grande partie du processus contraignant qui d'ordinaire est exécuté manuellement. Le réseau Aidmatrix propose en particulier un emplacement unique pour la saisie et le compte rendu de l'ensemble des besoins, des dons et de l'acheminement en temps réel; il communique en outre les besoins sur place à des donateurs potentiels et vice versa.

Günter Bretschneider, chef du Centre euro-atlantique de coordination des réactions en cas de catastrophe (EADRCC)

Actualisation de l'EADRCC

En ce qui concerne la gestion des dons, Aidmatrix met en relation les associations à but non lucratif, les services gouvernementaux et le secteur commercial, ce qui permet d'améliorer les secours en cas de catastrophe. Cette solution est appliquée aux situations de catastrophe, mais aussi dans le cadre de la gestion courante des dons dans les États fédéraux qui participent au projet.

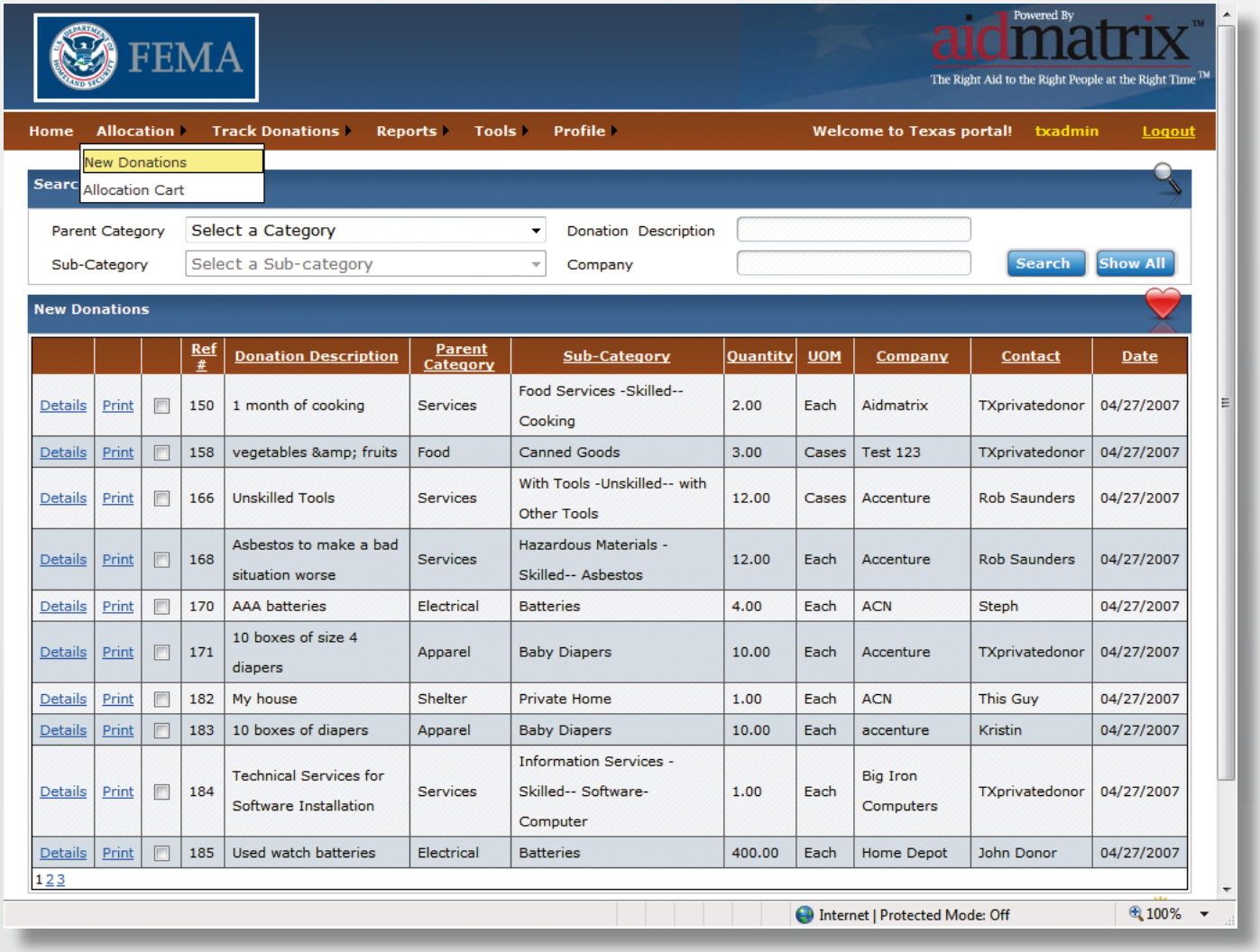
Ce tableau décrit le fonctionnement du mécanisme central d'échange d'informations.

La ligne du bas indique que le Home Depot a fait don de 400 piles de montres. Les différents dons sont répertoriés et administrés par un organisme de situation d'urgence et un bénéficiaire inscrit qui a besoin d'aide peut en faire la demande.

Comment le tableau ci-dessous s'applique-t-il à l'EADRCC et à sa fonction de coordination de l'information ?

Les populations dans le besoin sont les habitants d'un pays sinistré qui demandent de l'aide par l'intermédiaire d'un organisme public chargé de gérer la situation d'urgence. Les donateurs sont les pays du CPEA qui répondent à une demande d'aide. L'EADRCC coordonne, analyse et administre le processus.

Aidmatrix a mis son « tableau pour les secours en cas de catastrophe » à la disposition de l'EADRCC, des pays du CPEA et d'autres pays partenaires aux termes d'un mémorandum d'entente signé en juin 2008. Depuis septembre 2008, l'EADRCC utilise le « tableau pour les secours en cas de catastrophe » d'Aidmatrix en complément de ses outils habituels de compte rendu.



			Ref #	Donation Description	Parent Category	Sub-Category	Quantity	UOM	Company	Contact	Date
Details	Print		150	1 month of cooking	Services	Food Services -Skilled-- Cooking	2.00	Each	Aidmatrix	TXprivatedonor	04/27/2007
Details	Print		158	vegetables & fruits	Food	Canned Goods	3.00	Cases	Test 123	TXprivatedonor	04/27/2007
Details	Print		166	Unskilled Tools	Services	With Tools -Unskilled-- with Other Tools	12.00	Cases	Accenture	Rob Saunders	04/27/2007
Details	Print		168	Asbestos to make a bad situation worse	Services	Hazardous Materials - Skilled-- Asbestos	12.00	Each	Accenture	Rob Saunders	04/27/2007
Details	Print		170	AAA batteries	Electrical	Batteries	4.00	Each	ACN	Steph	04/27/2007
Details	Print		171	10 boxes of size 4 diapers	Apparel	Baby Diapers	10.00	Each	Accenture	TXprivatedonor	04/27/2007
Details	Print		182	My house	Shelter	Private Home	1.00	Each	ACN	This Guy	04/27/2007
Details	Print		183	10 boxes of diapers	Apparel	Baby Diapers	10.00	Each	accenture	Kristin	04/27/2007
Details	Print		184	Technical Services for Software Installation	Services	Information Services - Skilled-- Software-Computer	1.00	Each	Big Iron Computers	TXprivatedonor	04/27/2007
Details	Print		185	Used watch batteries	Electrical	Batteries	400.00	Each	Home Depot	John Donor	04/27/2007

1 2 3

Activités dans le domaine des PCU

Les activités des PCU de l'OTAN n'étant pas menées en vase clos, on trouvera dans le tableau ci-dessous des liens utiles avec d'autres organisations qui jouent elles aussi un rôle actif dans ce domaine.

ORGANISATION	SITE WEB
Commission européenne	http://ec.europa.eu/environment/civil
	http://ec.europa.eu/dgs/justice_home/terrorism/dg_terrorism_en.htm
Centre de suivi et d'information (MIC) de l'UE	http://ec.europa.eu/environment /civil/prote/mic.htm
Office d'aide humanitaire de la Commission européenne (ECHO)	http://ec.europa.eu/echo/index_en.htm
Bureau de la coordination des affaires humanitaires (BCAH) des Nations Unies	http://ochaonline.un.org
Organisation pour la sécurité et la coopération en Europe (OSCE)	http://osce.org
Agence internationale de l'énergie atomique (AIEA)	http://iaea.org
Centre des incidents et des urgences (CIU) de l'AIEA	http://www-ns.iaea.org/tech-areas/emergency/incident-emergency-centre.htm
Manuel de l'AIEA destiné aux premiers intervenants en cas d'urgence radiologique	http://www-ns.iaea.org/tech-areas/emergency/emergency-response-actions.asp
Organisation pour l'interdiction des armes chimiques (OIAC)	http://www.opcw.org

ACTIVITÉS DANS LE DOMAINE DES PCU

On trouvera ci-dessous une liste des activités qui seront menées prochainement par d'autres organisations internationales :

ORGANISATION	ACTIVITÉ	DATE	LIEU
OIAC	Stage sur l'assistance et la protection	7-11 septembre	Kuopio, Finlande
Service de sauvetage suédois	Stage sur les catastrophes écologiques internationales	7 septembre	À déterminer, Suède
BBK, Alemagne	5e congrès européen sur la protection civile et la gestion des catastrophes	5-6 novembre	Bonn, Allemagne
Ecole de l'OTAN	Stage sur les plans civils d'urgence de l'OTAN	16-21 novembre	Oberammergau, Allemagne
Ecole de l'OTAN	Stage OTAN sur la défense contre le terrorisme	23 novembre	Oberammergau, Allemagne
Commission européenne	3e forum sur la protection civile	25-26 novembre	Bruxelles
AIEA	Renforcement du régime mondial de sûreté et de sécurité nucléaires	14-18 décembre	Cape Town, Afrique du sud
Wilton Park	Une politique énergétique européenne intelligente	3-12 décembre	Wilton park, UK

De plus amples informations sont disponibles sur ePRIME, le système d'information, de gestion et d'échange en temps réel pour le Partenariat.

1420-09 NATO PRINTING & GRAPHICS STUDIO

Si vous souhaitez contribuer à « aPerÇU », le bulletin d'information des PCU, veuillez vous adresser à **Clare Roberts, PCU, siège de l'OTAN, cepd@hq.nato.int**