LA PROTECTION DES INFRASTRUCTURES CRITIQUES – DÉFIS ACTUELS

Dan Fifoiu*

Abstract: *Considering that in the European Union's plan, it has not been identified a solution for surpassing the legal differences between states (derived from priorities and different interests), Romania continues the program of alignment towards increasing its own standards and interconnecting internal critical infrastructures with the European and regional ones. This process is a lasting one, fact revealed also by the distance, in terms of time, between the first approaches, at a European level, of the problems of critical infrastructures, at the implementation of Directive 114/2008 provisions. The steps taken by the authorities in Bucharest are intended to drive Romania towards a level of development compatible both with the integration in a single European space of critical infrastructures and the fulfillment of an important role in stating the future strategies of the European Union. Currently, Romania's alignment to the European Union and international standards creates the optimum framework for developing and implementing some specific provisions which, at this time, are materialized as the steps of a single national plan for protecting critical infrastructures, on the way of being configured.*

Keywords: *protection, critical infrastructure, energy, transportation, telecommunication*

Tendances au niveau européen**

Au niveau communautaire, il y a toute une série de directions d'action dans l'aire de la protection des infrastructures critiques[1] et quelques projets lancés, qui incluent la Banque Mondiale et des acteurs privés. Néanmoins, il est encore difficile d'obtenir une approche unitaire à cause:

- des intérêts et visions nationaux différents et de l'insuffisante coopération interétatique pour prévenir et contrecarrer;
- des divergences inhérentes au niveau des fournisseurs, systèmes et zones de transit;
- de l'exposition inégale à des potentielles violences (d'origine terroriste ou guerre) et la compétition qui gouverne les marchés européens d'énergie;
- de l'élargissement des connexions entre les différents secteurs visés (énergie, transport, financier - bancaire), dus à la propagation rapide de la technologie de l'information;

* **Dan Fifoiu** has a Bachelor Degree in Letters, obtained at Ovidius University in Constanţa, with the specialization french-italian, a Master Degree in National Security Intelligence Activities Management, obtained in 2008, and another Master Degree in Intelligence Analysis, obtained at the Department of Sociology and Social Work of Bucharest University. His academic areas of interest are: sociology and intelligence analysis and EU legislation. E-mail: danfifoiu@yahoo.fr

** La traduction du roumain en français de cet article a été éfectuée par Cristian Iordan.

[1] La directive du Conseil de l'Union européenne 2008/ 114/ EC sur l'identification et la désignation des infrastructures critiques européennes; le Programme Européen dans le domaine de la Protection des Infrastructures Critiques/ PEPIC; Communication de la Commission 2009/149 „Protéger l'Europe contre les attaques cybernétiques et des perturbations d'ampleur: améliorer le niveau de préparation, de la sécurité et de la résilience".

- de la réticence des opérateurs privés de communiquer aux autorités les attaques de type *cyber* sur leurs systèmes ou les nouvelles plateformes avec lesquelles elles travaillent (parmi les causes, se retrouve la peur de perte de la réputation).

Les attaques cybernétiques – principale menace envers les systèmes critiques

Le manque de communication et la méfiance entre les différents acteurs obligent les institutions habilitées au plan de la sécurité nationale de s'adapter en marche aux risques et menaces de type *cyber*, en hausse et de plus en plus raffinées (effectuées par des individus, organisations de crime organisé, nationalistes ou terroristes, gouvernements hostiles, etc.).

La plupart des infrastructures critiques dépendent, directement ou non, d'équipements connectés à travers des lignes privées, radio ou VPN (*Virtual Private Networks*), via Internet ou à l'aide des liaisons téléphoniques.

L'utilisation des modems, même dans les conditions de protection avec un firewall puissant ou sécurité du réseau, peut être accédée de manière non-autorisée, sauf un mot de passe adéquat. Egalement, la pratique de l'attaque par l'intermédiaire des lignes téléphoniques („*wardialing*"[2]), très utilisée dans les années '80, semble reprendre en popularité. Toutefois, on considère que la plus simple méthode d'avoir accès à un réseau SCADA (*Supervisory Control and Data Acquisitions*[3]) est de recruter des employés mécontents, provenant de l'intérieur de la compagnie. Par exemple, en 2000, un ancien constructeur a pris le contrôle sur le système de canalisation et traitement des eaux dans la zone de Maroochy, dans l'Etat du Queensland (Australie), utilisant une connexion wireless et un ordinateur volé. Le résultat a été le déversement de quelques millions de litres de résidus dans un réseau de ruisseaux et parcs.

Les vulnérabilités dans l'espace virtuel ont un haut potentiel de risque dans tous les secteurs de la vie publique et privée, le milieu d'affaires internes et internationales, les politiques de défense nationale, les organisations internationales comme l'UE et l'OTAN. La nouvelle forme de la guerre asymétrique du XXIe siècle – „Digital Pearl Harbor" – devient de plus en plus réelle. Pendant les dernières années, ont été déclenchées des attaques massives avec des différentes formes de malware sur les serveurs gouvernementaux, les publications électroniques, banques, compagnies de téléphonie mobile et d'autres corporations. Parmi les cas d'attaques informatiques les plus médiatisés: Estonie/ mai 2007, Lituanie/ juin - juillet 2008, Géorgie/ août 2008 et Corée du Sud/ juillet 2009. Moins connues sont celles contre: Gazprom/ 1998 (prise de contrôle sur la principale route vers l'UE); la plateforme nucléaire de Davis-Besse, États-Unis/ 2003 (le système de monitorisation étant fermé pour 5 heures); la compagnie australienne Integral Energy/ 2009.

On a estimé[4] une croissance, en 2010, des menaces contre la sécurité bancaire, tout comme du nombre de réseaux de type *botnet*[5] et des attaques orientées contre les réseaux

[2] *War dialer* est un logiciel utilisé pour identifier de numéros de téléphone à travers lesquels on achève une connexion avec un modem qui supprte VOIP.
[3] Système qui collecte des données provenant de différents senseurs, les stocke et les transmet à un ordinateur central
[4] *„2010 Threat Predictions"*, McAfee Labs: http://www.mcafee.com.
[5] Selon le portail IT "TehnoPol", un réseau *botnet* représente une série d'ordinateurs infectés, interconnectés, qui peuvent être contrôlés de loin (sans le savoir ou le consentement de l'utilisateur) et utilisés par des hackers pour envoyer des mesages *spam*, pour attaquer d'autres sites ou pour le vol de données confidentielles.

d'affaires. Les réseaux botnet représentent l'instrument principal utilisé par les cyber criminels pour commettre des actions qui varient de messages «spam» jusqu'au vol d'identité. Un des plus connus exemples de menace *botnet* est le virus nommé *Conficker* ou *Kido*, qui a infesté, jusqu'en 2009, entre 9 et 15 millions d'ordinateurs. Sans une stratégie, ces réseaux peuvent agir de manière autonome, recruter et commander des millions d'ordinateurs au niveau global, pour des attaques coordonnées sur les infrastructures critiques.

En dépit du fait que, pendant les dernières années, nous sommes arrivés à une reconnaissance presque unanime au niveau gouvernemental de la gravité du phénomène, indifférent du pays de résidence, le progrès a connu une lente évolution. Une élimination totale des cyber menaces sur infrastructures critiques est pratiquement impossible, l'objectif étant leur réduction au minimum, sans compromettre la productivité et, de manière implicite, la consommation, dans le contexte de la libéralisation des marchés, la privatisation de la majorité des opérateurs d'État et de la dépendance de la technologie de l'information et de télécommunication (ICT).

L'interdépendance des infrastructures critiques - implications

Presque toutes les branches d'activité dépendent, directement ou indirectement, de la sécurité énergétique, avec ses réseaux (physiques et/ou virtuelles) devenus de plus en plus complexes. Si, dans la première partie du XX^{e} siècle, les systèmes d'approvisionnement en énergie électrique étaient décentralisés – et, par la suite, vulnérables en plan régional – l'interconnexion des réseaux (au-delà des frontières nationales, en présent) rend possible le transfert des capacités et la connexion des acteurs étatiques.

L'exemple le plus relevant peut être considéré l'interdépendance entre l'infrastructure de télécommunications et les secteurs énergétiques. Au cas d'une attaque sur un nœud de production ou distribution de l'énergie électrique, les services de téléphonie, autant que ceux de dates, sont inutilisables, pendant qu'une éventuelle chute des lignes de communications pourrait déterminer l'incapacité des opérateurs du domaine énergétique de surveiller et contrôler efficacement les installations de transport.

La diversification du système européen d'approvisionnement et transport du gaz naturel à travers des gazoducs – perçu comme la cheville d'Achille de l'Europe – a fait monter de manière exponentielle le nombre de risques et menaces. Ses sécurité et contrôle sont dépendants, conformément aux experts[6], de l'infrastructure ICT, d'une gestion de réseau efficiente, une hiérarchie cohérente des tâches (au niveau central, régional et local).

De manière similaire à la chaîne d'approvisionnement d'un supermarché, qui demande une coordination attentive et à temps dans la fourniture des produits, les systèmes électriques et d'approvisionnement avec gaz naturel sont essentiels pour le bon fonctionnement des grands opérateurs économiques. Au cas d'une éventuelle chute, peut être déclenché un «effet cascade» des conséquences négatives, avec des implications pour les systèmes de télécommunications et transport (service de secours, santé publique et alimentaire).

[6] Frank Umbach, Senior Associate, et Uwe Nerlich, directeur du *Centre for European Security Strategies* (CESS), München-Berlin, "European Energy Infrastructure Protection: Addressing the Cyber-warfare Threat", http://www.ensec.org - 27.10.2009.

Également, le système énergétique est interconnecté avec celui financier - bancaire, dont le fonctionnement optimal dépend, à son tour, de la sécurité des télécommunications, conformément aux standards imposés par le système de transfert financier électronique *Electronic Funds Transfer Systems* (EFT). En Europe, ce système est appelé TRANSFER (*Trans-European Automated Real-time Gross Settlement Express Transfer System*), pendant qu'aux États-Unis il est connu en tant que Fedwire, et au niveau international - SWIFTNet (*Society for Worldwide Interbank Financial Telecommunication Network*).

Coopération internationale

En dépit du fait que, jusqu'à présent, il n'y a pas eu une attaque simultanée sur plusieurs infrastructures critiques nationales, celui-ci est faisable de point de vue technique, étant difficile à anticiper et contrecarrer, sans connaître la planification des pas en vue d'atteindre les objectifs visés. Ainsi, pour une protection plus efficace des infrastructures critiques, au niveau européen et pas seulement, il est nécessaire de:

- accroître l'efficacité de l'application de la loi dans la lutte contre la cyber criminalité, étant donnée la rapidité croissante à laquelle évoluent les menaces de l'espace virtuel, les auteurs des attaques étant libres des contraintes géographiques ou des frontières physiques;
- réduire les différences évidentes entre experts gouvernementaux et les spécialistes dans la sécurité des réseaux;
- établir/ définir les standards uniques, de partage des responsabilités qui en résultent (au niveau des opérateurs, État, région etc.), respectivement des contributions de chaque partie;
- donner une impulsion au partenariat public-privé, à travers un échange d'informations et bonnes pratiques dans l'aire de la sécurité;
- développer la coopération entre États et organisations, ayant en vue le caractère intersectoriel et transnational de l'assurance de la sécurité énergétique;
- accroître la confiance entre les parties, ce qui peut être fait seulement par la consolidation du dialogue, où l'on répond aux questions et où l'on souligne la complexité des activités de *intelligence*, sur le fond des menaces accrues;
- accorder une attention spéciale au facteur logistique (secteur vital dans l'appui des processus macroéconomiques, des infrastructures critiques et l'approvisionnement des consommateurs), ce qui sera „le vrai mécanisme de réglage de l'économie" et qui „pourrait aider l'Union européenne à revenir rapidement après la crise globale"[7].

La composante de prévention des infrastructures critiques est prioritaire, ce qui impose l'implémentation de systèmes d'alerte et intervention rapide, surtout de l'infrastructure de transport des hydrocarbures.

L'importance de la préparation

L'apparition du *Centre Européen pour la Protection des Ressources Critiques* (CEPRC) à Bruxelles peut offrir aux spécialistes et experts gouvernementaux nationaux des stages sur la protection des infrastructures critiques: *Security Enforcement Training, avec des lecteurs renommés*, et *Security Awareness Training*, dans un simulateur VisioSpace.[8]

[7] "*Delivering tomorrow - Customer Needs in 2020 and Beyond*", http://www.europesworld.eu/ automne 2009

[8] François Gaspard et Alain Hubrech, les fondateurs du *Centre Européen pour la Protection des Infrastructures Critiques,* "Tackling Critical Energy Infrastructure Network Interdependencies", http://www.ensec.org - 23.03.2010

Roumanie – la continuation du processus d'alignement

Les recommandations formulées au niveau communautaire sur la protection des infrastructures critiques européennes (ICE), tout comme les actions communes engagées dans ce sens mettent l'accent sur l'irréversibilité de la connexion directe entre les objectifs/ stratégies autochtones et celles envisagées par les organismes de l'Union européenne et, en même temps, accélèrent leur marche sur la trajectoire de l'uniformisation et harmonisation, à caractère de nécessité et intérêt commun.

Néanmoins, le principal repère dans la formulation des prochains documents-cadre dans le domaine de la protection des infrastructures critiques, la *Directive 114/2008*, n'est qu'un premier pas dans le processus d'identification des ICE et d'évaluation de la nécessité d'amélioration de leur sécurité. Par la suite, si on vise les secteurs énergétique et du transport, on admet le fait qu'elle peut être modifiée en vue d'évaluer l'opportunité d'inclure d'autres secteurs dans son domaine d'application – le secteur de la technologie de l'information et des communications, inter alia. En plus, elle prévoit que "*la responsabilité principale et finale pour la protection des ICE revient aux Etats membres de l'Union européenne et, respectivement, aux propriétaires/ opérateurs de ces infrastructures*."

De manière similaire, le Programme Européen pour la Protection des Infrastructures Critiques (PEPIC), adopté en décembre 2006, accepte l'idée du développement, par les Etats membres, de leurs propres mécanismes de sécurisation des infrastructures, en fonction des intérêts et menaces. Pourtant, il met l'accent sur l'importance de l'interconnexion de ces mécanismes par l'intermédiaire de « points de contact ».

Les documents ont plutôt le rôle d'accélérer le développement par les Etats membres de systèmes propres de protection unitaire des infrastructures critiques, d'une telle façon que, une fois cet objectif accompli, les respectifs systèmes permettent la création d'une autorité centrale européenne.

En ce qui concerne la Roumanie, l'absence d'un modèle actualisé au cadre de l'UE et la persistance de la diversité des intérêts des pays membres conduisent au maintien au même niveau d'importance des objectifs d'intégration en matière de sécurité des infrastructures, respectivement de développement des propres projets dans le domaine. A la fois, le manque d'une formule communautaire unique assure la conservation, à court terme, du format actuel des organismes compétents dans le domaine sur ces composantes:

— prévention des menaces et gestion des risques – les structures de sécurité nationale, membres de la communauté nationale de renseignements, à côté des entités qui composent le Système National de Gestion des Situations d'Urgence ou SNGSU (conformément à l'Ordonnance d'Urgence du Gouvernement 21/ 2004);

— intervention et gestion des situations de crise – le Ministère de l'Administration interne, par l'intermédiaire de l'Inspectorat pour les Situations d'Urgence, ensemble avec les organismes spécialisés, en fonction de la nature de l'événement;

— assurance de la capacité de résilience et reconstruction suite aux événements/ crises – structures subordonnées/ coordonnées par les ministères qui ont les infrastructures critiques en compétence.

À présent, la responsabilité de la gestion des problèmes de sécurité des deux catégories d'infrastructures critiques (le fonctionnement en bons termes et la prévention des menaces, gestion des risques, respectivement de la capacité de résilience), revient, en grande

mesure, aux opérateurs qui agissent sous la direction/ dans la coordination du Ministère de l'Économie, du Commerce et du Milieu des Affaires (MECMA), la Commission Nationale pour le Contrôle des Activités Nucléaires (CNCAN), respectivement le Ministère des Transports et de l'Infrastructure (MTI).

Le Service Roumain de Renseignements fait partie des autorités publiques avec des attributions en ce qui concerne la protection des infrastructures critiques:

- la technologie de l'information et des communications (avec les sous-domaines communications et transmissions de données interconnectées au niveau national), le Service ayant des responsabilités dérivant de ses qualités d'autorité nationale dans le domaine:
- CYBERINT (conformément à la décision du Conseil Suprême de Défense du Pays), avec des attributions dans l'implémentation du projet CYBERINT, destiné à assurer l'accroissement du potentiel de défense de la Roumanie contre les menaces venues de l'espace cybernétique, en assurant les capacités de prévention, protection, réaction et gestion des conséquences en cas de cyber attaques;
- de l'implémentation du Système Informatique Intégré;
- la lutte contre le terrorisme;
- la protection des informations classifiées.

L'échec de l'initiative de constitution de l'Autorité Nationale pour la Protection des Infrastructures Critiques (ANPIC)

La proposition législative sur la protection des infrastructures critiques et la constitution de l'Autorité Nationale pour la Protection des Infrastructures Critiques (subordonnée au Gouvernement) a été repoussée en Parlement au 23 mars 2009[9], ce qui a mis un délai à l'apparition en Roumanie d'un organisme capable d'assumer, selon la Directive CE 114/2008, le rôle de responsable avec la coordination et l'organisation du système autochtone de profile et, en même temps, d'interface entre la Roumanie et l'Union européenne.

Conformément à cet acte normatif, l'Autorité aurait eu un rôle de coordination, monitorisation et contrôle des activités de protection des infrastructures critiques, qui inclut l'élaboration des procédures d'identification, évaluation et gestion adéquate des vulnérabilités et risques à leur sécurité, pendant que les attributions auraient été les suivantes:

- la réglementation et coordination, au niveau national, de la protection des infrastructures critiques;
- l'élaboration de la « Stratégie Nationale de Protection des Infrastructures Critiques » (un document destiné à la définition du programme stratégique visant l'identification des infrastructures critiques, l'analyse des vulnérabilités et des risques, des dépendances et interdépendances, la définition des mesures qui améliorent leur protection);
- la création du « Plan National de Protection des Infrastructures Critiques », partie composante de la Stratégie Nationale de Protection des Infrastructures Critiques, document classifié, qui aurait inclus les plans individuels pour chaque infrastructure critique et aurait compris ses éléments descriptifs et les mesures de protection revenant aux propriétaires/ opérateurs/ administrateurs d'infrastructures critiques;
- la constitution du «Système National Informatique de Protection des Infrastructures Critiques» - le système informatique de gestion

[9] http://webapp.senat.ro/pdf/09L125PV.pdf

et traitement de données et informations, monitorisation, direction et contrôle du complexe de mesures et mécanismes associés à la protection des infrastructures critiques contenues dans la Stratégie Nationale de Protection des Infrastructures Critiques. Le système aurait dû être connecté à la structure d'alerte précoce du Système National de Gestion des Situations d'Urgence et au réseau similaire qui existe au niveau de l'UE;

- l'élaboration de la stratégie d'identification/ gestion des risques et planification de la protection à travers une approche unitaire capable d'encourager l'implication responsable des secteurs public et privé;
- la représentation dans les relations avec les tiers;
- la promotion, l'implémentation et le suivi des décisions de l'UE et de l'OTAN dans ce domaine;
- l'implémentation des réglementations nationales et internationales et l'adaptation du cadre légal dans ce sens;
- de solliciter et d'obtenir de la part des institutions publiques ou privées les informations dans le domaine de compétence.

La décision du Conseil Législatif du Parlement a été motivée par le manque de constitutionnalité de l'initiative, car le projet d'acte normatif n'a pas été formulé par le Gouvernement (mais par un membre de la Chambre des Députés), la seule autorité capable de proposer la création d'une structure dans sa subordination. Les autres arguments présentés par le Conseil (qui peuvent être interprétés comme recommandations pour la prochaine démarche similaire), ont invoqué:

- le caractère trop général de la proposition, avec l'observation qu'elle pourrait être analysée à travers la compatibilité de ses dispositions avec l'acquis communautaire général;
- l'absence des dispositions spécifiques qui établissent le rapport entre l'Autorité Nationale pour la Protection des Infrastructures Critiques et les autres composantes du Système National de Gestion des Situations d'Urgence (sachant que l'Autorité devrait être partie du Système), conformément aux réglementations de l'OUG nr.21/2004 visant la composition et les attributions du SNGSU;
- le manque de relevance de la proposition législative de point de vue de la transposition d'une directive ou d'une décision communautaire (même si elle traite « un domaine sensible dans tout l'espace européen »);
- le fait que l'initiative n'a pas comme fin la création du cadre nécessaire à l'application d'un règlement communautaire.

Exemples de bonnes pratiques au niveau national

Le rejet de la démarche de création de l'ANPIC n'a pas empêché la continuation des programmes existants, l'évolution du cadre conceptuel et normatif ou l'apparition de nouvelles initiatives dans l'aire des infrastructures critiques, mais a contribué à la limitation de la capacité d'interconnexion, respectivement au développement d'un niveau supérieur de réglementation de la problématique de la protection et sécurisation.

A partir du mois d'avril 2009, on peut remarquer, au plan interne, sur les deux paliers majeurs établis par la Directive CE 114/2008:

– Energie

• La dotation des stations de distribution de l'énergie électrique (au cours de l'année 2009 et au début de 2010) avec des systèmes SCADA, avec support de communication par fibre optique, qui permet la monitorisation de l'état technique des installations en

temps réel et l'intervention rapide en cas de problèmes. En parallèle, ont continué les programmes de renouvellement des stations de transformation au niveau national[10];

• La création, par la Décision du Gouvernement 623 du 20.05.2009, au cadre de la Direction Générale Réglementation, Autorisation et Contrôle Activités de la Commission Nationale pour le Contrôle des Activités Nucléaires (CNCAN) du Service Garanties Nucléaires, Transports et Protection Physique des Objectifs Gérés[11];

• L'inclusion (04.03.2010) dans le programme de financement de la Commission Européenne pour les initiatives dans les domaines du gaz et de l'énergie électrique de trois projets de développement et sécurisation où est impliquée la compagnie « Transgaz »;

o des équipements qui permettent le changement de la direction du flux de livraison au cas d'une intérromption à court terme (1,56 millions €);

o l'interconnexion des réseaux de gaz entre la Roumanie et l'Hongrie (16,6 millions €);

o l'interconnexion des réseaux de gaz entre la Roumanie et la Bulgarie (8,9 millions €)[12];

• L'octroi de garanties d'Etat (OUG nr.9 du 17.02.2010) pour le cofinancement des projets déroulés en Roumanie, au niveau local, à travers des fonds européens, dans le domaine de l'infrastructure énergétique;

• L'élaboration (Adina Vălean, MPE) du projet de règlement européen sur la procédure de rapport, aux niveaux national et régional, par la Commission Européenne, des investissements dans l'infrastructure énergétique (pétrole, gaz, électricité et biocarburants)[13]. Le projet, adopté le 26.02.2010, vise la facilitation de la possibilité de planifier et identifier le besoin d'investissements supplémentaires dans l'infrastructure énergétique, sans affecter la nature confidentielle des activités sur le marché.

– Transports

• La loi nr. 94 du 08.04.2009[14] sur l'audit de sécurité dans le domaine de l'aviation civile, qui assure le cadre pour adapter et appliquer efficacement le Programme national de sécurité de l'aviation civile, pour prévenir les actes d'intervention illicite et assurer la sécurité des infrastructures afférentes;

• L'Autorité Navale Roumaine a démarré, en mai 2009, l'implémentation de la 2e phase du projet «Système de gestion du trafic sur le Danube et information sur le transport sur les eaux internes – RORIS 2»[15]. C'est un système complexe de monitoring et gestion du trafic de navires sur tout le secteur roumain du Danube, en conformité avec la Directive 2005/44/CE;

• La Décision du Gouvernement nr.117/17.02.2010[16] approuve le Règlement d'investigation des accidents et incidents, de développement et amélioration de la sûreté ferroviaire (les chemins de fer et le réseau de métro). Le Règlement est obligatoire pour l'Autorité Ferroviaire Roumaine/ AFER et les opérateurs économiques avec des opérations de transport du genre:

[10] http://www.ccib.ro/afacerea/stire-3149-.htm
[11] http://www.gov.ro/upload/articles/105680/nf-hg-623-2009.pdf
[12] http://media.hotnews.ro/media_server1/document-2010-03-4-6990739-0-lista-celor-43-proiecte-energetice.pdf
[13] http://www.euractiv.ro/uniunea-europeana/articles%7CdispalyArticle/articleID_19536/Proiect-de-regulament-european-privind-raportarea-catre-CE-a-investitiilor-realizate-in-infrastructura-energetica.html
[14] http://www.legestart.ro/Legea-94-2009-auditul-securitate-domeniul-aviatiei-civile-(Mzl5MzM0).htm
[15] http://www.rna.ro/Noutati/prezentare%20Sistem%20RIS%20II.pdf
[16] http://fstfr.ro/hotararea-117-din-17-februarie-2010.html

- les administrateur/s d'infrastructure ferroviaire;
- les gestionnaires d'infrastructure ferroviaire non-intéropérable;
- les opérateurs de transport ferroviaire;
- l'opérateur économique qui assure le transport avec le métro;
- les opérateurs économiques qui détiennent, en propriété, en leasing ou avec loyer, des chemins de fer industriels raccordés à l'infrastructure ferroviaire publique et/ ou l'infrastructure ferroviaire privée ouverte à la circulation publique;
- les opérateurs économiques qui détiennent, en propriété ou avec loyer, des véhicules ferroviaires qui circulent sur l'infrastructure ferroviaire;
- les opérateurs économiques qui mènent des activités connexes et adjacentes au transport ferroviaire.

Selon le Règlement, AFER est désigné l'agence spécialisée d'intervention, qui a l'obligation d'agir au cas des appels d'urgence, d'accident ou incident ferroviaire;

- la proposition (03.02.2010) du projet de Stratégie Nationale de Gestion du Risque aux Inondations à moyen et long terme, comme nécessité d'adaptation du cadre autochtone d'action à la Directive 2007/60/CE du 23.10.2007 sur l'évaluation et la gestion des risques d'inondation;
- la signature, le 26.02.2010, de la Déclaration de Madrid sur l'implémentation du programme *Single European Sky*[17], qui a comme objectif principal l'harmonisation des pratiques dans le domaine aéronautique au niveau de l'UE, en spécial en ce qui concerne la révision du cadre légal, l'utilisation de technologies avancées et l'amélioration de la sécurité de l'infrastructure aérienne;
- la clôture, le même jour, du Mémorandum d'entente entre les Ministères des Transports de Roumanie et Bulgarie sur la création du Bloc Aérien Fonctionnel „Danube" (Danube Functional Airspace Block – Danube FAB), dans le cadre du programme *Single European Sky*;
- l'adoption, par ordre du Ministre des Transports et l'Infrastructure nr.184 du 08.03.2010, du Plan de Sécurité des ports Constanţa et Midia[18] (conformément au Code International pour la Sécurité des Navires et des Facilités Portuaires - Code ISPS - élaboré suite aux événements du 11.09.2001 et adopté par Résolution nr. 2 de la Conférence Diplomatique des Gouvernements Contractants de l'Organisation Maritime Internationale, à Londres, le 09.12.2002).

Les facilités portuaires disposent d'un officier de sécurité, qui gère l'implémentation et le maintien d'un Système de gestion de la sécurité, destiné à la conservation d'un climat de pleine sûreté sur les plateformes portuaires. Annuellement, chaque facilité portuaire prépare une Evaluation de sécurité qui est analysée et approuvée par l'Autorité Portuaire, et qui est suivie par un audit externe de sécurité du Système;

- la signature, le 06.04.2010, du contrat d'acquisition, par l'Administration des Canaux Navigables (ACN) Constanţa, du système électronique River Information Services – RIS de gestion du trafique de navires sur le Canal Danube – Mer Noire et d'information sur le transport sur les eaux internes. Le contrat a une validité de deux ans et il est financé des fonds européens, par le Programme Opérationnel Sectoriel de Transport (71,12%) et du budget d'État (28,88%). Le système mettra à la disposition de l'utilisateur la carte électronique des

[17] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/199&format=HTML&aged=0&language=en
[18] http://www.portofconstantza.com/apmc/portal/vizstire.do?bifa=true&method=showNews&id_stire=1004&tip_stire=3

canaux navigables, des informations sur le trafic, pour les commandants, sur les conditions hydrométéorologiques de la zone de navigation, la gestion des écluses et la surveillance vidéo sur le déroulement du trafic. Il est déjà implémenté en Allemagne, Hongrie, Slovaquie et Autriche, et il sera fonctionnel en Croatie, Serbie, Bulgarie, Roumanie et Ukraine, couvrant, ainsi, tout le cours du Danube, respectivement le Corridor VII Pan-Européen[19].

Défis actuels

Les actions des organismes autochtones avec des responsabilités dans les deux secteurs majeurs d'infrastructures critiques – énergie et transports – relèvent la convergence, au niveau national, vers l'accomplissement des principaux objectifs pour leur sécurisation, respectivement l'adaptation du cadre normatif roumain, la dotation avec des technologies actualisées et le développement de la coopération avec des partenaires étrangers. Les objectifs en cause sont inclus dans la Stratégie Energétique de la Roumanie 2007-2020 et la Stratégie pour un transport durable 2007-2030.

Dans le contexte actuel, interne et externe, le nécessaire de sécurité des infrastructures critiques, dans ses aspects relevants (sécurité des ressources et des voies d'accès, avec des implications géopolitiques prononcées, respectivement la sécurité des infrastructures critiques associées), impose le rapport du cadre d'action de Roumanie à:

- *l'impératif de l'amélioration, dans les conditions de la crise économique, de la gestion de la qualité*, qui découle du vieillissement et la détérioration des infrastructures sur le fond de l'intensification de leur utilisation; les investissements insuffisants pour le renouvellement; la gestion sous les paramètres optimaux du partenariat public-privé dans le développement des infrastructures; la diminution du nombre des employés. En dépit des efforts pour surmonter ces défis, la crise économique et financière continue d'influencer l'ampleur et l'efficacité des actions;
- *la nécessité d'améliorer l'adaptabilité des infrastructures et du potentiel d'interconnexion* – conditions de la hausse de l'efficacité de la gestion de risque. Les perspectives de développement des réseaux de transport des hydrocarbures – les gazoducs Constanţa-Soci et AGRI Interconnector[20], objectifs d'intérêt majeur également pour d'autres États de l'UE – tracent simultanément le cadre et la nécessité de l'intensification de la coopération pour assurer leur sécurité physique. A ce point, on peut mentionner la montée du niveau de risque, engendrée par l'association avec des partenaires provenant de zones d'instabilité accrue et les menaces considérables envers les infrastructures (similaire aux problèmes de l'oléoduc Baku-Tbilisi-Ceyhan pendant les luttes entre la Russie et la Géorgie, de l'été de 2008);
- *l'accroissement de la capacité de résilience comme moyen d'agir contre/ minimaliser la menace terroriste*. Ensemble avec la composante de prévention, assurée par des politiques spécifiques et des actions des structures de sécurité nationale, le potentiel d'absorption de l'impact, d'adaptation/ intervention dans des conditions extrêmes, de réduction de la durée et de l'intensité de l'agression, la capacité de reconstruction suite à une attaque constituent les principaux

[19] http://www.rna.ro/Noutati/prezentare%20Sistem%20RIS%20II.pdf

[20] http://www.minind.ro/presa_2010/aprilie/13_ap_2010_com_semnare_GNL.pdf - le site du Ministère de l'Economie, du Commerce et du Milieu des Affaires (MECMA) de Roumanie

moyens de lutter contre les menaces représentées par le phénomène terroriste;

- *les nouvelles menaces cybernétiques*. Dans les conditions de l'évolution rapide de la complexité/ perfectionnement des attaques cybernétiques et des vulnérabilités créées par les technologies novatrices, les prévisions concernant la sécurité des infrastructures critiques ont indiqué, pour 2010, la montée des menaces envers les réseaux informatiques. Le projet de Loi concernant la défense cybernétique, prévue au cadre du Programme législatif du Parlement roumain pour la période 2009-2012, vise explicitement la protection des infrastructures critiques de point de vue de la technologie de l'information;
- *les situations imprévues entraînées par des épidémies, des phénomènes naturels et des changements climatiques* – inondations, tremblements de terre, éruptions volcaniques etc. – ont testé constamment la capacité d'interopérabilité des infrastructures critiques, conduisant à l'élargissement et la consolidation des connexions entre elles. Le but consiste dans la prise, par un certain secteur, des mesures destinées à atténuer les effets d'une situation de crise sur un autre secteur (dans les conditions de la paralysie du trafic aérien européen, les communications, respectivement l'infrastructure routière, navale et ferroviaire ont été essentielles pour la stabilisation de la situation);
- *la culture de sécurité*. La prise de conscience sur l'utilité d'une coopération approfondie et efficace entre tous les acteurs impliqués dans l'opération/ sécurisation des infrastructures critiques est devenue décisive sur toutes les coordonnées d'action dans le domaine de la sécurisation des infrastructures critiques, en spécial en ce qui concerne la synchronisation et la complémentarité des services assurés par le secteur privé, autorités étatiques, institutions du milieu académique ou de recherche. D'autre part, la communication, l'information et l'instruction de la population, combiné avec la transparence des relations entre les institutions responsables (Ministères de la Défense, de l'Administration Interne, Service Roumain de Renseignements, Service de Renseignements Étrangers, Service de Télécommunications Spéciales, Service de Protection et Garde, l'Office du Registre National des Informations Secrètes d'État, l'Office de Surveillance du Secret d'État et d'autres structures dont l'activité est partiellement classifiée) et la contribution du milieu académique/ de recherche (Fondation EURISC) contribuent à la réception positive des efforts en vue de sécuriser les infrastructures critiques et une meilleure mobilisation des citoyens au soutien des autorités.

L'importance de la problématique associée au processus de protection des infrastructures critiques a monté en importance dans le contexte de la croissance des cas de dommages au niveau des infrastructures, l'apparition des phénomènes météo extrêmes et la hausse des actions d'entrée non-autorisée. Dans la transpositions des lignes directrices destinées à la gestion efficace des dysfonctions et/ ou vulnérabilités qui peuvent surgir, on peut utiliser le schéma présenté en annexe (particularisé en fonction du domaine auquel appartiennent les infrastructures).

Conclusions

L'état actuel d'alignement de notre pays aux standards communautaires et internationaux permet le développement et l'implémentation de mesures spécifiques, qui, pour le moment, représentent des étapes d'un plan unitaire, national, en cours de configuration, de protection des infrastructures critiques. Ce processus est de durée, fait souligné aussi par la distance temporelle entre les premières approches européennes

de la problématique de la protection des infrastructures critiques et l'implémentation de stipulations de la Directive 114/ 2008.

Au niveau communautaire, on n'a pas identifié une solution pour dépasser les différences législatives inter-étatiques (provenant de priorités et intérêts qui diffèrent). La Roumanie continue le programme d'alignement en ce qui concerne les standards propres et l'interconnexion des infrastructures critiques autochtones à celles européennes et régionales.

Les actions de Bucarest visent à positionner l'État roumain à un niveau de développement correspondant à l'intégration dans un espace unique européen des infrastructures critiques et de remplir un rôle important dans l'énonciation des futures stratégies de l'Union européenne.

BIBLIOGRAPHIE:

- Baker, Stewart; Waterman, Shaun; Ivanov, George, *In the Crossfire. Critical Infrastructure in the Age of Cyber War. A global report on the threats facing key industries*, McAfee, (http://www.mcafee.com/ 2009)
- *Delivering tomorrow - Customer Needs in 2020 and Beyond* (http://www.europesworld.eu/ automne 2009)
- Gaspard, François; Hubrech, Alain, *Tackling Critical Energy Infrastructure Network Interdependencies* (http://www.ensec.org/ 23.03.2010)
- Gheorghe, Adrian V., *Analiza de risc şi de vulnerabilitate pentru infrastructurile critice ale societăţii informatice – societate a cunoaşterii*, Universitatea Politehnică Bucureşti, Swiss Federal Institute of Technology (ETH), Zürich
- McAfee Labs, *2010 Threat Predictions* (http://www.mcafee.com/ 2009)
- Umbach, Frank; Nerlich, Uwe, *European Energy Infrastructure Protection: Addressing the Cyber-warfare Threat*, (http://www.ensec.org/ 27.10.2009)
- http://webapp.senat.ro/pdf/09L125PV.pdf
- http://www.ccib.ro/afacerea/stire-3149-.htm
- http://www.gov.ro/upload/articles/105680/nf-hg-623-2009.pdf
- http://media.hotnews.ro/media_server1/document-2010-03-4-6990739-0-lista-celor-43-proiecte-energetice.pdf
- http://www.euractiv.ro/uniunea-europeana/articles%7CdispalyArticle/articleID_19536/Proiect-de-regulament-european-privind-raportarea-catre-CE-a-investitiilor-realizate-in-infrastructura-energetica.html
- http://www.legestart.ro/Legea-94-2009-auditul-securitate-domeniul-aviatiei-civile-(MzI5MzM0).htm
- http://www.rna.ro/Noutati/prezentare%20Sistem%20RIS%20II.pdf
- http://fstfr.ro/hotararea-117-din-17-februarie-2010.html
- http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/199&format=HTML&aged=0&language=en
- http://www.portofconstantza.com/apmc/portal/vizstire.do?bifa=true&method=showNews&id_stire=1004&tip_stire=3
- http://www.rna.ro/Noutati/prezentare%20Sistem%20RIS%20II.pdf
- http://www.minind.ro/presa_2010/aprilie/13_ap_2010_com_semnare_GNL.pdf

Annexe : La protection des infrastructures critiques