Les infrastructures critiques face au terrorisme

Autor(en): **Wigger, Bernhard**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2019)**

Heft 1

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-867920

Par nature, les réseaux ferrés, électriques, de transport d'énergie, etc sont difficiles à sécuriser car une interruption en n'importe quel point peut interrompre l'ensemble du fonctionnement du système.

Réseau national de sécurité

Les infrastructures critiques face au terrorisme

Bernhard Wigger
Dr. phil., historien, major et officier de renseignement, chef de projet ERNS 19

Aux fins de mieux comprendre le développement et la persistance de la menace terroriste illustrée par l'ERNS 19 et d'affiner le scénario, trois niveaux d'escalade sont décrits.

Le premier niveau d'escalade voit naître la propagande et le chantage politique; les cyberattaques jouent en l'occurrence un rôle de première importance.

Le deuxième niveau d'escalade peut être le théâtre d'attaques d'infrastructures critiques. Cette partie du scénario sert à mettre en lumière les défis d'une menace terroriste pour la protection de la population. Les infrastructures critiques vulnérables sont des cibles attrayantes pour un adversaire irrégulier, dans la mesure où il peut accentuer sa pression par l'interruption de lignes vitales d'approvisionnement et de communication.

Le troisième niveau d'escalade comprend des attentats contre des rassemblements de foule, provoquant de nombreuses victimes décédées, gravement blessées ou traumatisées. Si, en cas de situation de terrorisme durable, les niveaux d'escalade décrits ci-avant quant à une campagne de propagande ou une mise en danger des infrastructures critiques viennent à persister, la menace d'attentats contre la population constitue un important défi pour la conduite en cas de crise. Outre les armes à feu et les explosifs, les substances radiologiques, biologiques et/ou chimiques peuvent également servir de moyens d'intimidation. À terme, une telle escalade de la menace porte atteinte au bon fonctionnement du pays et des institutions, et sabote la souveraineté de l'Etat ainsi que la cohésion sociale.

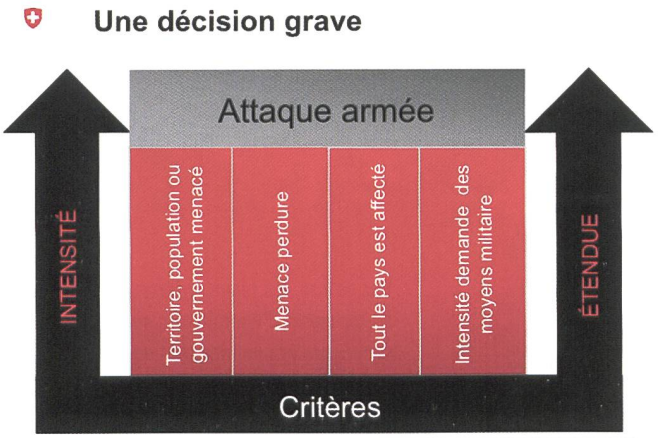
Les trois niveaux d'escalade forment les grandes lignes de l'événement en vue du développement du canevas d'exercice. L'escalade de la menace découle d'une part de l'intensification croissante des attaques et, d'autre part, de l'addition des trois intrigues et événements concomitants survenant avec l'actualisation du scénario.

Le terrorisme et les infrastructures critiques

Selon le scénario, les événements et menaces déstabilisent la population. Les services compétents élèvent par conséquent leur niveau de disponibilité opérationnelle et déclenchent des dispositifs préarrangés. La présence policière est intensifiée, les exploitants d'infrastructures critiques et d'autres entreprises prennent des mesures considérables pour accroître leurs préparatifs de sécurité. L'objectif stratégique de la gestion de crise, et plus particulièrement de ce scénario, en cas de menace terroriste durable, est d'empêcher d'autres attaques.

Les cyberattaques représentent de puissantes armes pour le sabotage d'infrastructures critiques. Elles permettent en effet à un ennemi potentiel de provoquer des dégâts considérables où que ce soit en prenant peu de risques. La numérisation, l'interconnexion et l'automatisation augmentent la vulnérabilité des infrastructures critiques ainsi que le risque de réactions en chaîne telles que des difficultés d'approvisionnement. Ainsi, une partie adverse peut se procurer un accès numérique à un dispositif de commande électronique pour saboter des systèmes critiques. De telles attaques peuvent être encadrées par l'engagement d'initiés. En cas d'attaques graves, le fonctionnement du gouvernement, des processus économiques et de la vie sociale peut être entravé.

Pour le *Global Liberation Front* (GLF), l'adversaire fictif, qui a été développé au plus proche de la réalité pour l'ERNS 19, des attaques spectaculaires contre des bâtiments publics, des ouvrages et des installations jouant des rôles clés pour le fonctionnement du pays, offrent la possibilité d'augmenter par étape la pression effective sur la Suisse au moyen de campagnes de propagande et de la maintenir ainsi durablement à un haut niveau. Par ailleurs, la mise en danger des ouvrages critiques pour l'approvisionnement en énergie, le réseau de transports, la communication ou le système financier peut se produire sous forme de leurre tactique pour lier ponctuellement



les forces de sécurité et détourner l'attention accordée à l'attaquant. Pour terminer, il y a dans l'idéologie GLF aussi le souhait d'ébranler les fondements du monde occidental et industriel en recourant au terrorisme et à la violence.

Tous les domaines de la sécurité, tant au niveau fédéral que cantonal, mais aussi dans l'économie privée sont concernés par le risque accru auquel sont exposées les infrastructures critiques. Les acteurs de la protection de la population sont sollicités pour garantir la résilience et surmonter les conséquences d'événements. La police doit tenir compte des interactions et des répercussions sur la sécurité publique. Quant à l'armée, elle doit gérer non seulement la protection de ses propres installations et systèmes mais aussi les demandes d'appui subsidiaire.

Quand est-ce qu'il s'agit d'une attaque armée?

En cas d'attaque terroriste contre des infrastructures critiques, il convient de se poser la question de son intensité et de l'ampleur des dégâts potentiels : quels sont les éléments qui permettent de qualifier une attaque terroriste d'attaque militaire? Par le passé, une attaque militaire contre le territoire suisse pouvait être effectuée exclusivement par des forces armées étatiques externes. Aujourd'hui, il faut envisager la possibilité que des forces irrégulières internes à un pays passent à l'action. Un tel emploi de la force se ferait avant tout contre les infrastructures critiques et pour entraver le fonctionnement de l'Etat.

Des adaptations de la doctrine sont actuellement en cours tant au niveau international que national. Ainsi, l'OTAN a développé des scénarios de référence et étendu le droit à l'autodéfense contre des attaques militaires. Jamie Shea, secrétaire général adjoint de l'OTAN, revendiquait en 2015 déjà le fait qu'une cyberattaque d'une certaine ampleur devait être considérée comme une attaque armée. L'UE, l'OSCE, et l'ONU redéfinissent également la notion d'attaque militaire dans le contexte de menace actuel. En 2014, des spécialistes allemands du droit international ont précisé quant à la clause d'assistance mutuelle du traité de Lisbonne de 2007 qu'une attaque armée au sens de la charte de l'ONU devait être comparable de par son ampleur et son étendue (*scale and effects*) à des opérations militaires entre Etats. De même le sommet du G7, organisé en 2016 au Japon, a également proclamé le droit à une autodéfense armée lors d'importantes cyberattaques.

Puis la Suisse, dans son Rapport sur la politique de sécurité 2016, a étendu sa définition de la notion de défense. Le Conseil fédéral est parvenu à la conclusion que le seuil équivalent à une attaque armée peut aussi être atteinte lorsque des groupements non étatiques la soutiennent et opèrent depuis l'intérieur du pays. De tels acteurs non étatiques peuvent avoir accès aujourd'hui aux technologies de l'espace aérien et du cyberespace et paralyser des infrastructures vitales.

En Suisse comme partout ailleurs, deux facteurs sont décisifs pour qu'une attaque soit assimilée à une attaque militaire :
- l'intensité ou l'ampleur de l'attaque ;
- l'ampleur des dégâts qu'elle occasionne.

Pour déterminer si le niveau d'une attaque militaire est atteint, le Rapport sur la politique de sécurité 2016 a défini quatre critères, qui doit permettre au Conseil fédéral et au Parlement de justifier un cas de défense militaire:
- premièrement, soit le territoire suisse, soit sa population ou encore l'exercice du pouvoir public doivent être concrètement menacés ;
- deuxièmement, la menace doit être durable ;
- troisièmement, la menace doit être nationale et ne pas concerner uniquement Genève, Bâle ou le Tessin ;
- et quatrièmement, l'usage de la violence contre la Suisse doit être si important qu'il nécessite le recours à des moyens militaires pour y répondre.

Pour pouvoir prendre sereinement des décisions si lourdes de conséquences, on doit s'y préparer mentalement. En bref, il faut exercer de tels scénarios. Une attaque terroriste en Suisse ferait tout de suite les gros titres dans le monde entier. Les médias internationaux s'empareraient aussitôt des événements se déroulant en Suisse. Il s'agit notamment de se préparer au fait qu'une attaque de grande ampleur contre des infrastructures critiques déclencherait un véritable raz-de-marée politique. Pour que nous puissions y résister, nous devons donc nous entraîner.

L'ERNS 19 offre à cet égard une bonne opportunité – saisissons-la !

B.W.