Gestion de crise : les nouvelles pratiques et l'importance de l'interopérabilité des outils de communication.

Les crises sont inévitables et imprévisibles. Catastrophes naturelles, incidents d'exploitation, terrorisme, guerres technologiques, espionnage industriel… Leur fréquence et leur complexité s'accroissent. Conscients des nouveaux risques, l'État, les grandes entreprises - et notamment les Organismes d'Importance Vitale (OIV) - font évoluer leurs pratiques en créant des unités spéciales et des services dédiés, des procédures standardisées et des exercices d'entrainements spécifiques. Mais qu'en est-il de leurs outils ? Comment leurs systèmes d'information et communication (SIC) se transforment pour améliorer leur gestion ?

Lors de la conférence organisée le 7 février au Millennium Hôtel Paris Opera par StreamWIDE et le CDSE, des représentants du Ministère de l'Intérieur et des troupes d'élites de l'Etat ont partagé leur expérience terrain et partagé les réflexions mises en œuvre au plus haut niveau. Trois enjeux principaux dessinent les contours du changement.

La démocratisation des outils de communication
Pendant des décennies, l'État a bénéficié d'un ascendant technologique pour coordonner plus rapidement les forces de sécurité et de secours. Les OIV et le reste de la population en profitaient indirectement. Avec le perfectionnement et la démocratisation de SIC comme WhatsApp ou Telegram, les adversaires ont parfois repris une longueur d'avance grâce à des technologies « simples mais perfectionnées », accessibles au grand public et non traçables.

La qualité du traitement de l'information
Avec l'explosion du nombre de données accessibles (images de drones ou de vidéosurveillance, capteurs bactériologiques, rapports d'incidents…) et la multiplication du nombre d'acteurs à coordonner, l'acheminement, le traitement, le partage et la protection de l'information sont devenus encore plus complexes. La coordination en temps réel devient critique et il n'est plus question de s'appuyer exclusivement sur des officiers de liaison.

L'adoption des solutions
Malgré la création de scénarios d'anticipation de plus en plus élaborés, les personnes à l'avant poste de la détection et de la gestion de crise ne sont jamais totalement préparées à y faire face. « Quand elle survient pour de vrai », il est crucial d'avoir pris en compte le facteur humain pour que les solutions se rapprochent le plus possible du quotidien des collaborateurs.

Pour répondre à ces nouveaux enjeux, les SIC de l'État et des Organismes d'Importance Vitale (OIV) doivent respecter de nouveaux impératifs.

L'interopérabilité
Qu'elle soit métier, technique ou internationale, l'interopérabilité à tous les niveaux devient la clé de voûte de la réussite en temps de crise (Molenbeek) ou lors d'événements de grande ampleur (JO2024). Une réflexion politique accrue au niveau de l'Union Européenne est d'ailleurs conduite actuellement pour arriver à une harmonisation des normes technologiques et une meilleure anticipation de leurs évolutions.

L'interopérabilité doit aussi permettre de construire ou de renforcer la « confiance opérationnelle », ce qui inclut les échanges de best practices et les RETEX avec tous les acteurs concernés par la crise.

La résilience
Les SIC doivent être accessibles partout, tout le temps. La désorganisation provoquée par les dégâts de l'Ouragan Irma à Saint-Martin nous a malheureusement démontré l'importance de la résilience des SIC. Les systèmes et solutions doivent pouvoir fonctionner lorsque le réseau principal « tombe », pour ne pas retarder ou fragiliser la résolution de crise.

L'intuitivité
Un bon outil de communication de crise est un outil qui sait se faire oublier, qui épouse les habitudes et les comportements quotidiens de ses utilisateurs. Lorsque la crise survient, son utilisation doit être intuitive et de l'ordre du réflexe, de sorte qu'elle n'entraîne ni retard, ni erreur… ni passage vers une solution grand public qui ne serait pas sécurisée.

Pour relever ces nouveaux défis de la communication critique, l'Etat et les OIV doivent se doter d'outils plus agiles et plus fonctionnels. Leur conception doit se faire au plus près des exigences métier et avec des coûts supportables pour en assurer la viabilité économique et opérationnelle.

Le Réseau Radio du Futur et sa première brique « PC Storm » illustrent ces changements de paradigme. Dans le cadre de ce projet, le Ministère de l'Intérieur s'est équipé et a ainsi déployé l'application logicielle all-in-one « Team On Mission » de StreamWIDE. Grâce à cette plateforme sécurisée, intuitive et totalement interopérable, les forces de sécurité et de secours disposent désormais d'un outil digital commun de communication critique et de gestion de crise. Cela leur permet de garder le contrôle en toutes circonstances et ainsi communiquer, s'informer en temps réel, suivre des process automatisés, le tout dans un environnement sécurisé.

Pour conclure cette soirée, une mise en garde en forme d'appel à l'humilité a été formulé. Malgré les meilleurs plans et les entrainements les plus rigoureux, la disponibilité des ressources et de la technologie (réseaux, application, matériel) sont incontestablement des impératifs fondamentaux*. Qui plus est dans le cadre de la résolution de la crise, tout doit fonctionner, partout, tout le temps.

** EBIOS 2010 (Expression des Besoins et Identification des Objectifs de Sécurité) - ANSSI (Agence nationale de la sécurité des systèmes d'information)*