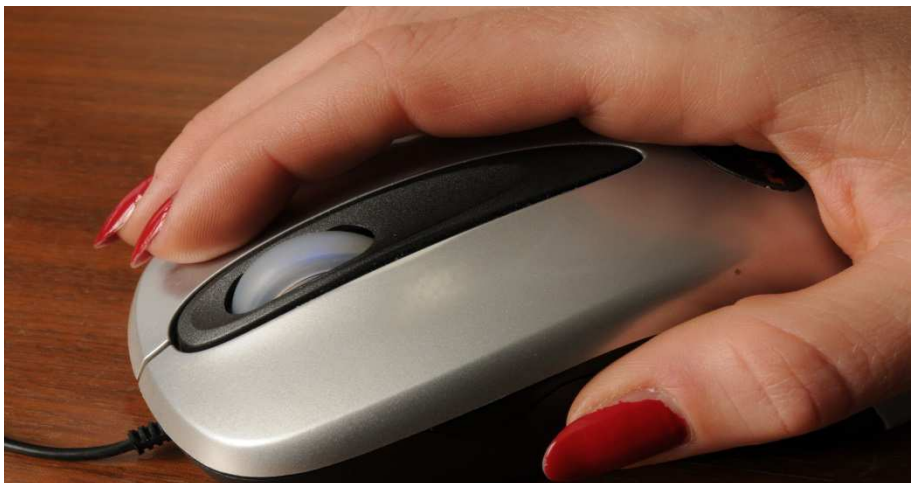
Cyberattaques



Définition

Une cyberattaque est une attaque réalisée par le biais d'infrastructures informatiques. Elle peut viser un Etat, une entreprise, un secteur économique ou la société. Ce type d'attaque peut avoir des motivations individuelles (p. ex. dans le cas de collaborateurs frustrés), politiques ou sociales, et peut viser des biens numériques (p. ex. des informations protégées), des personnes ou des biens matériels (voir Denning, 2006).

La menace causée par une cyberattaque découle avant tout de l'interconnexion informatisée d'infrastructures critiques dans des domaines tels que l'énergie, les transports ou les finances.

La cybercriminalité, quant à elle, a avant tout pour but l'enrichissement financier.

On parle de «cyberespionnage» lorsqu'une cyberattaque tente de pénétrer un système informatique ou d'y dérober des données à des fins d'information mais sans chercher à le modifier.

La «cyberguerre» caractérise une action entreprise par des acteurs étatiques présents dans le cyberespace dans le but de prendre un avantage militaire.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

30 juin 2015

Bundesamt für Bevölkerungsschutz BABS

Exemples d'événements

Décembre 2010 Suisse Attaque par déni de service distribué (DDoS), «Opération Représailles» («Operation Payback»)	Après le gel, par PostFinance Suisse, et la fermeture, par MasterCard et Visa, des comptes de Julian Assange, fondateur de WikiLeaks, les sites internet de ces prestataires de services financiers ont fait l'objet d'attaques massives par déni de service distribué (DDoS). Pendant des heures, ces sites n'ont plus été accessibles et non plus été en mesure d'effectuer des transactions en ligne. Il n'a pas été possible de chiffrer le montant exact des dommages subis. Cette opération de représailles a été attribuée à la mouvance du groupe Anonymous.
Avril - mai 2007 Estonie Attaque DDoS de grande envergure	Après que l'Estonie eut déplacé un monument célébrant l'armée soviétique du centre de Tallinn, sa capitale, dans un cimetière militaire éloigné, des inconnus ont paralysé à la fin d'avril et en mai 2007 plusieurs organisations estoniennes, dont le Parlement (y compris son serveur de messagerie), des ministères, des banques et des sites d'information au moyen de DDoS. Certains sites Internet ont été piratés et modifiés. Par ailleurs, des routeurs de backbone et des serveurs DNS ont également subi des attaques, ce qui a entraîné des interruptions de trafic (de moins de cinq minutes) au niveau des réseaux dorsaux. Les attaques contre les deux plus grandes banques du pays ont causé l'interruption des services bancaires par internet d'une de ces deux banques (pendant un peu moins de deux heures). Une banque visée a chiffré les pertes qu'elle a subies suite à cette cyberattaque à environ 1 million de dollars US. Aucune information n'a été donnée quant aux dégâts causés aux infrastructures et aux systèmes informatiques de l'Etat estonien. L'intégrité des systèmes les plus importants n'a pas été affectée, toutefois les systèmes ont été saturés et la population n'a plus eu accès, ou alors plus que difficilement, aux systèmes informatiques.
Printemps 2000 Queensland (Australie) Cyberattaque d'un ancien collaborateur	Au printemps 2000, un ancien collaborateur a pénétré dans le système de contrôle du réseau d'eau potable et d'élimination des eaux usées du comté de Maroochy, au Queensland (Australie). Il a pu manipuler ainsi 300 vannes de contrôle et neutraliser tous les messages d'alerte. En trois mois, il a réussi à provoquer le déversement de 800 000 litres d'eaux usées non traitées dans des parcs naturels et dans une rivière. Ont été souillés, entre autres, le terrain et les parcs d'une chaîne d'hôtels internationale, et l'écosystème de la nappe phréatique a été gravement pollué. L'auteur de cette cyberattaque a pu être arrêté par la suite et a été condamné à deux ans d'emprisonnement.

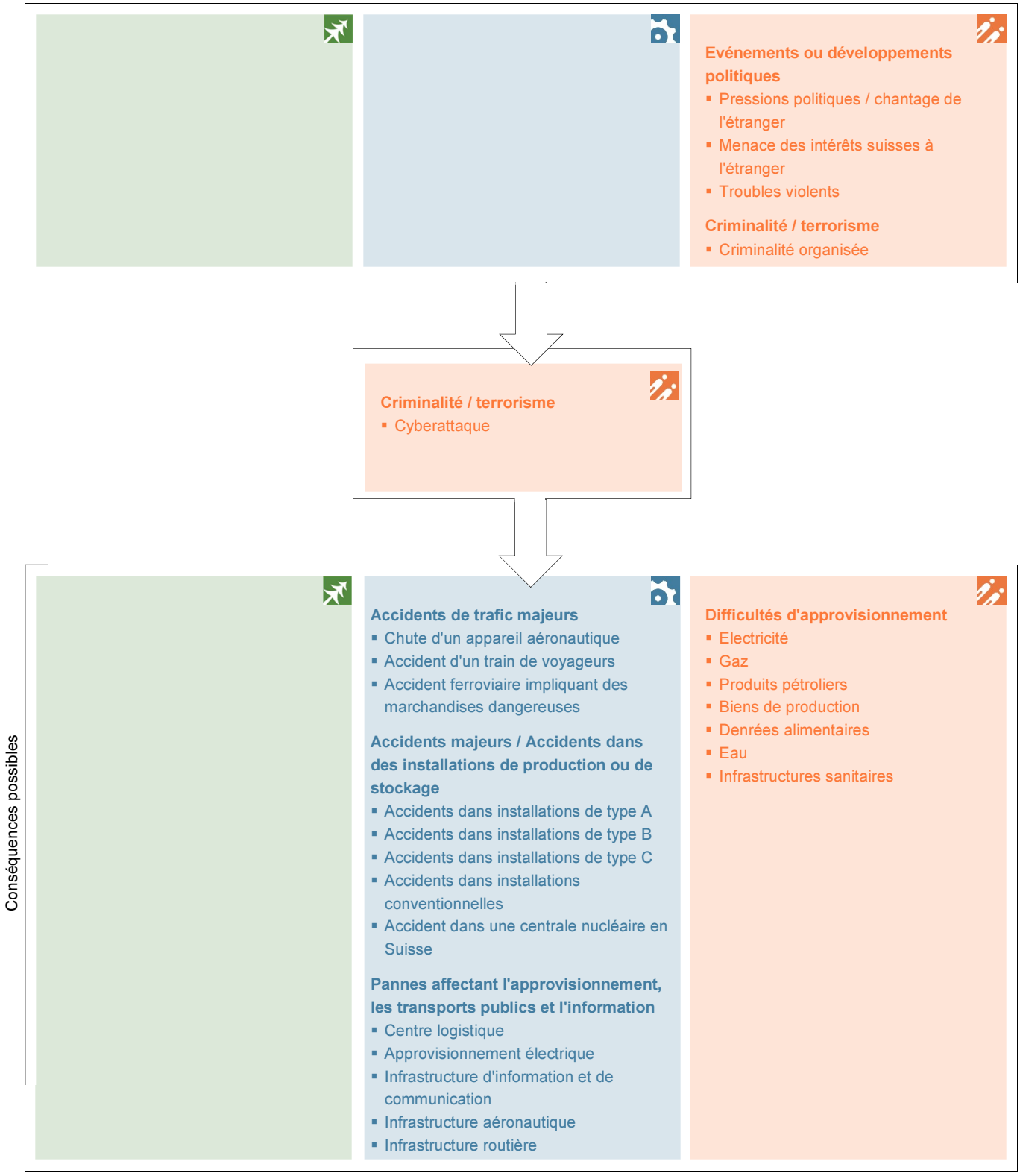
Facteurs d'influence

Les facteurs suivants peuvent influer sur la survenance, l'évolution et les conséquences d'un événement.

Sources de danger	▪ Caractéristiques des auteurs (idéologie, disposition à la violence, capacité de nuisance, savoir-faire, degré d'organisation, ressources, infrastructures contrôlées/déjà disponibles) ▪ Attitude d'un Etat tiers ou d'organisations (criminelles ou paraétatiques) présentes dans le pays ▪ Vulnérabilité des systèmes (perméabilité, mesures de protection, interfaces/points d'accès, ingénierie sociale, intégration lacunaire de la sécurité de l'information dans des processus de sécurité stratégiques intégraux)
Occurrence temporelle	▪ Généralement, en lien avec des décisions et des développements économiques, politiques ou sociaux ▪ La préparation des moyens d'action et des infrastructures nécessaires peut déjà avoir eu lieu dans un autre contexte. La manipulation illicite d'un système informatique peut être survenue antérieurement à la cyberattaque elle-même qui, selon les circonstances, peut être très brève
Lieu / étendue	▪ Taille et caractéristique de l'objet attaqué (objectif isolé, branche, secteur, degré d'interconnexion des secteurs, technologie spécifique, etc.) ▪ Source de l'attaque (lieu où se trouvent l'auteur et ses complices) ▪ Infrastructures utilisées (réseaux, interfaces, protocoles, etc.)
Déroulement de l'événement	▪ Efficacité des mesures préventives, y compris de la pratique juridique ▪ Efficacité des contre-mesures spécifiques prises ▪ Déroulement de l'attaque (le cas échéant, par paliers) ▪ Attitude des organisations concernées, des forces d'intervention et des autorités compétentes ▪ Réaction de la population et des milieux politiques

Interdépendances

Ci-après les événements et développements, tirés de l'inventaire des dangers potentiels de l'Office fédéral de la protection de la population (OFPP), pouvant être à l'origine ou la conséquence d'une cyberattaque.



Scénario

Intensité

Divers événements d'intensité variable peuvent se produire en fonction des facteurs d'influence. Les scénarios ci-après sont une sélection, parmi de nombreux développements envisageables, et non pas une prévision. Ils permettent de présager les conséquences d'événements afin de s'y préparer.

1 – importante	▪ Forme d'attaque relativement connue ▪ Existence de contre-mesures ou possibilité d'en développer rapidement ▪ Attaques visant des infrastructures critiques industrielles ou gouvernementales ▪ Vol de données concernant l'économie ou le gouvernement ▪ Prise de connaissance par le public après coup
2 – majeure	▪ Forme d'attaque relativement inconnue ou combinaison de formes connues ▪ Absence de contre-mesures, mais possibilité d'en développer en quelques jours ▪ Attaques visant des infrastructures critiques financières et gouvernementales, manipulation ciblée de l'information sur des sites internet ou des canaux d'information gouvernementaux ou privés, blocage de prestations informatiques fournies par des établissements financiers (e-banking) ▪ Vol de données concernant l'économie ou le gouvernement ▪ Public indirectement touché par les attaques, effets ressentis dans la vie quotidienne
3 – extrême	▪ Nouvelle forme d'attaque ▪ Absence de contre-mesures, dont le développement prendra des semaines ▪ Attaques visant des infrastructures critiques dans les secteurs des transports, de l'énergie et des télécommunications ▪ Manipulation et endommagement de systèmes de contrôle de trafic et d'énergie, perturbation massive des services de télécommunication ▪ Public au courant de l'attaque ▪ Public indirectement touché par les attaques, effets ressentis dans la vie quotidienne

Choix du scénario

Le scénario décrit ci-après se fonde sur une intensité «majeure». Il est tout à fait plausible que ce scénario survienne en Suisse.

Evénement

Situation initiale / phase préliminaire	Un événement politique (p. ex. un vote populaire mal accepté) ou l'activité tolérée en Suisse d'une organisation, d'une entreprise ou d'une branche économique est jugée inacceptable par une organisation étrangère ou un Etat tiers, qui décide de réagir par une cyberattaque.
Phase de l'événement	Divers sites d'organisations et portails d'information sont piratés sur la Toile, et de fausses informations sont propagées sciemment. Les médias sont les premiers touchés par ces attaques. Ces dernières s'étendent sur deux à trois mois. D'abord isolées, elles deviennent de plus en plus fréquentes. Plusieurs organisations touchées les signalent à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), aux autorités de poursuite pénale locales ou au Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI). MELANI et le SCOCI recoupent leurs informations pour obtenir une vue d'ensemble au niveau national, et le SCOCI les met à disposition des autorités de poursuite pénale locales dans le cadre de la coordination des actions. Au bout de trois mois, la Confédération prend position officiellement: la Suisse condamne les attaques contre les sites internet et défend sa position, perçue comme une provocation. Entre un et trois jours après la prise de position de la Confédération, les attaques se concentrent sur les sites internet des autorités, et plus particulièrement des départements et des offices fédéraux dont l'activité est en rapport avec la polémique. On suppose dans un premier temps que des serveurs cantonaux ont pu être piratés et servir de porte d'entrée aux attaques. Désormais, non seulement les sites internet, mais aussi les prestations en ligne des offices fédéraux concernés (cyberadministration) sont gravement perturbés. Par ailleurs, les messageries électroniques sont bombardées de spams, qui rendent très difficiles les échanges de courriels. Les départements et offices fédéraux concernés se voient contraints de recourir à d'autres canaux pour leurs contacts et leurs relations administratives. De surcroît, on enregistre des tentatives de pénétration des systèmes de données de la Confédération sans que l'on constate toutefois de vol de données. Les services de la Confédération concernés informent MELANI de ces événements.

Trois semaines plus tard, le secteur financier est attaqué à son tour: d'abord, les sites internet de différents prestataires de services financiers sont visés puis, pendant deux à trois semaines, des services importants sont gravement perturbés.

Pendant plusieurs jours, les communications de la bourse suisse sur internet sont rendues très difficiles. Les opérations interbancaires sont en partie perturbées mais fonctionnent encore. Outre les prestations en ligne des établissements financiers, les terminaux de paiement du commerce de détail sont touchés localement et temporairement du fait de la mise hors service pendant deux jours des serveurs. Ici et là, des distributeurs automatiques d'argent sont également bloqués.

En outre, les échanges de courriels sont considérablement perturbés par une avalanche de spams (parmi lesquels de nombreux courriels de propagande ou d'hameçonnage). Les organisations fournissant des services aux instituts financiers, en particulier celles qui fournissent des informations financières ou qui traitent les transactions, subissent elles aussi des attaques. On constate également des tentatives directes de pénétrer dans les systèmes informatiques de ces établissements.

Les organismes concernés en Suisse recherchent des mesures appropriées, soit par le biais du cercle de clients fermés de MELANI, soit en collaborant directement entre eux.

Un matin, alors que les bourses asiatiques ont ouvert à la baisse, la bourse de Zurich est attaquée par DDoS, apparemment à partir du territoire national, au moment précis de l'ouverture des transactions. Les pirates réussissent à activer des maliciels introduits au préalable dans une application smartphone courante. La bourse est contrainte de stopper les opérations et ne peut rouvrir que deux jours ouvrables plus tard, après la mise en place de mesures de protection supplémentaires.

En arrière-plan, les services fédéraux compétents travaillent en étroite collaboration avec leurs homologues d'autres pays depuis un certain temps. L'organisation criminelle responsable des attaques peut être identifiée et un Etat tiers réussit à la neutraliser, ainsi que son infrastructure. Les attaques diminuent ensuite très rapidement.

Phase de rétablissement

Les sites internet des autorités, des instituts financiers et des médias peuvent être rétablis au fur et à mesure et fonctionnent à nouveau normalement. La remise en service prend un peu plus de temps pour les fournisseurs de services internet moins bien protégés. A peu près un mois après la cessation des attaques, tous les sites internet fonctionnent à nouveau comme auparavant.

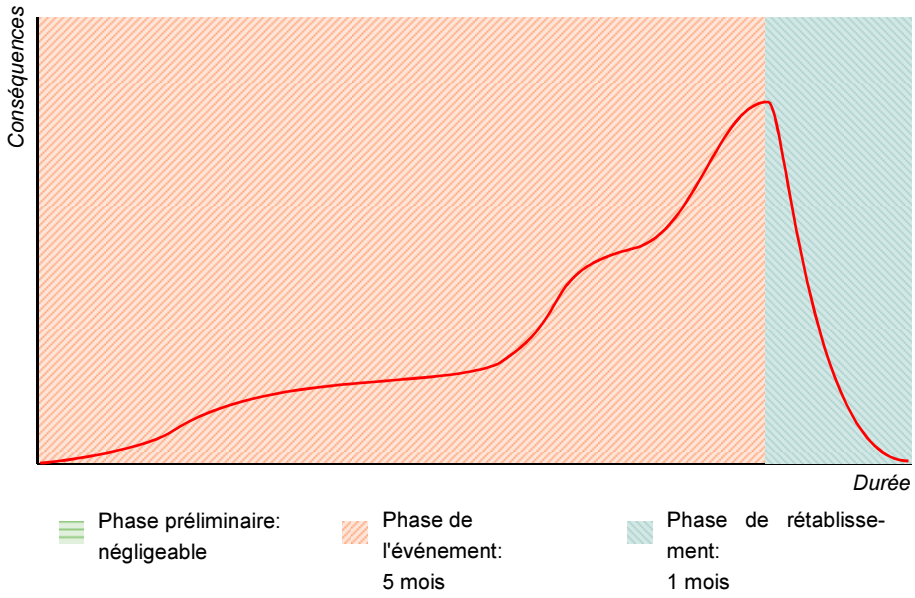
Une semaine après la fin des attaques, tous les sites internet de la Confédération et des établissements financiers visés sont à nouveau utilisables. Il ne peut pas être exclu que les pirates aient réussi à s'emparer de données dans les systèmes attaqués. Les services concernés sont occupés encore pendant des se-

maines après la fin des attaques à estimer l'ampleur des dégâts et des vols.

Pour la population, la situation est redevenue normale un mois après la fin des attaques.

Déroulement temporel

Les cyberattaques s'étendent sur cinq bons mois et surviennent en trois phases (1. Piratage de sites internet de médias, 2. Attaques des infrastructures informatiques de la Confédération, 3. Opérations contre les infrastructures informatiques du secteur financier). Les conséquences se font ressentir, en tout, sur une durée de près de six mois.



Etendue spatiale

Les attaques visent les médias en ligne, les pouvoirs publics et le secteur financier de la Suisse. D'une manière générale, elles sont perçues par toutes les personnes clientes des organisations concernées.

Conséquences

Population

L'événement peut causer quelques décès (p. ex. suite à un suicide) ou blessés. Des personnes peuvent avoir besoin d'assistance.

Environnement

L'événement n'occasionne pas de dégâts à l'écosystème.

Economie

La bourse est mise hors service pendant deux jours.

Les opérations interbancaires sont paralysées mais continuent à fonctionner sur le plan international.

Les organismes directement concernés doivent consentir des efforts supplémentaires en ressources techniques et humaines pour juguler et contrer les attaques et identifier leurs auteurs. Par ailleurs, ils doivent prendre des me-

sures de sécurité supplémentaires.

Le trafic des paiements du commerce de détail est perturbé localement et temporairement. Même si certains distributeurs automatiques de billets sont mis hors service, il reste possible de retirer de l'argent liquide à d'autres appareils ou aux guichets. Etant donné que les services proposés en ligne sont fortement restreints et parfois même indisponibles, davantage d'opérations se déroulent aux guichets.

Le trafic des paiements est perturbé par le blocage des services des instituts financiers visés. Du coup, une partie des clients se rendent directement aux guichets pour effectuer leurs opérations bancaires, ce qui leur prend davantage de temps et contribue à surcharger le personnel. Certains clients, qui ont perdu confiance, mettent un terme à leur relation commerciale. Plusieurs plaintes et demandes de dédommagement sont déposées lorsque la clientèle n'est plus en mesure d'effectuer des paiements.

Les établissements concernés subissent par ailleurs des dommages financiers, d'une part du fait de la surcharge de travail de leur personnel et des investissements techniques nécessaires pour contrer les attaques et procéder à une évaluation de la perte de données et, d'autre part, de la perte d'affaires résultant de l'impossibilité d'offrir les prestations habituelles.

Les dégâts directs et les frais de remise en état sont estimés à quelque 870 millions de francs. L'événement a occasionné une perte de près de 150 millions de francs en raison de la réduction des activités économiques qu'il a entraînée.

Société

Les interruptions dans la fourniture de prestations financières dues aux cyberattaques touchent plusieurs milliers de personnes, certains jours. Toutefois, la paralysie des établissements financiers concernés n'entraîne pas de rupture importante d'approvisionnement.

Aucun processus vital ou d'importance majeure n'est touché. Certains fournisseurs de services internet sont contraints de débrancher les serveurs qui ont été utilisés par les pirates pour lancer leurs attaques.

Les événements suscitent l'inquiétude de la population, mais pas de panique. Par contre, sa confiance dans les autorités et les établissements financiers est ébranlée. Les établissements concernés doivent engager du personnel de sécurité supplémentaire en raison de l'afflux de clients aux guichets. L'ordre et la sécurité intérieure sont préservés sans restrictions.

Les médias étrangers rendent compte de la gestion de la cyberattaque de manière factuelle, et leur couverture de l'événement ne dure que quelques jours.

Suite aux attaques, les médias suisses se montrent très critiques pendant plusieurs semaines («Une Suisse si vulnérable!»), et la polémique ne reste pas sans effets sur le débat public et la perception de l'opinion publique. Le lien entre le cyberespace, la possible violation de l'intégrité territoriale ainsi que les mesures susceptibles d'être prises contre d'autres attaques suscitent des discussions passionnées.

Diagramme des conséquences

Illustration de l'ampleur des dégâts dans le scénario décrit, en fonction des indicateurs de dommage. Le dommage augmente du facteur 3 par classe d'ampleur.

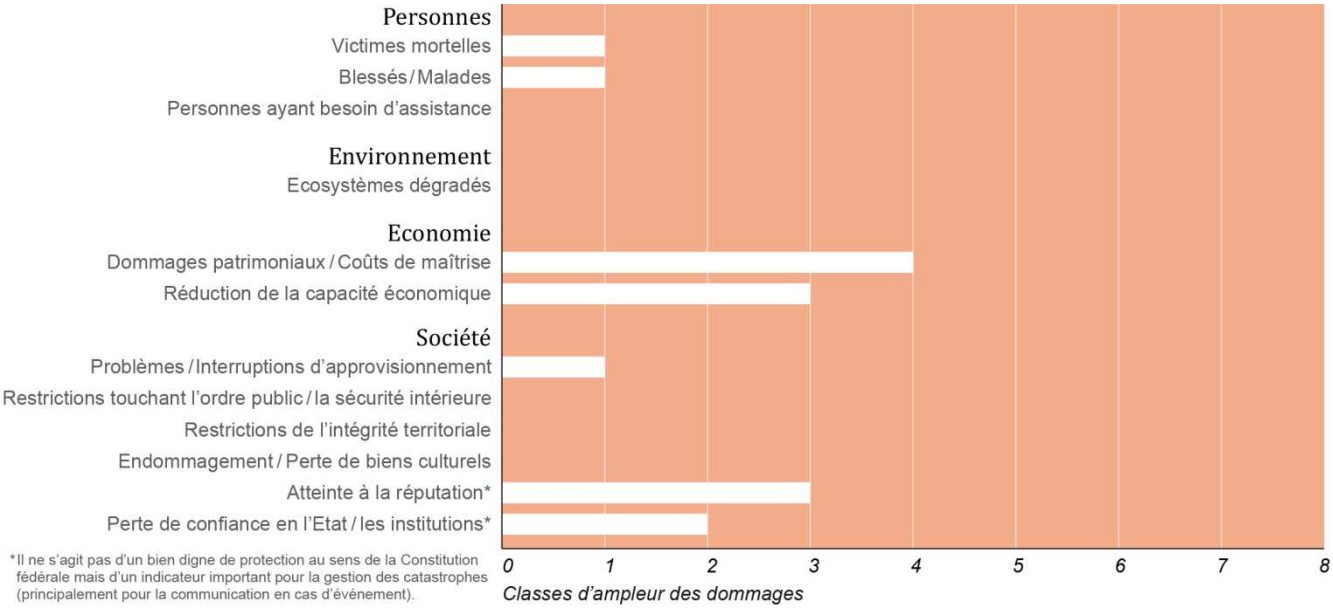
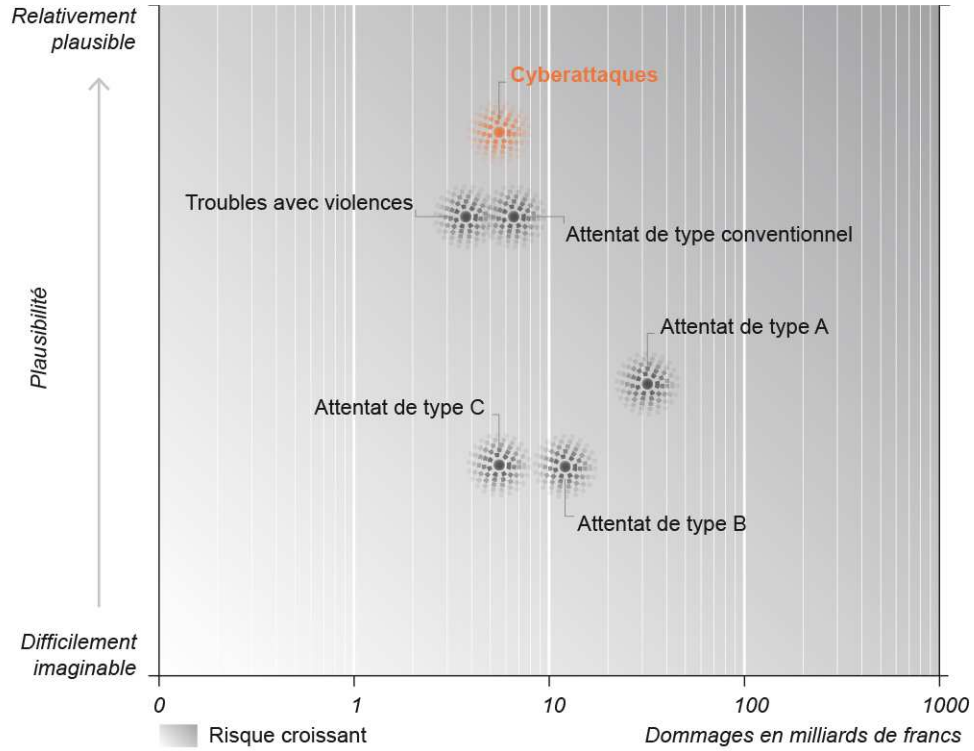


Diagramme des risques

Illustration du risque lié au scénario décrit, conjointement avec les autres mises en danger qui ont été analysées. Plus un scénario se situe en haut à droite, plus le risque qu'il simule est élevé. Les événements occasionnés volontairement sont attribués aux classes de plausibilité, les autres aux classes de fréquence. Les dommages sont agrégés et monétarisés.



Bases juridiques et références

Constitution

Lois	▪ Code pénal suisse du 21 décembre 1937; RS 311.0. ▪ Loi fédérale du 30 mars 1911 complétant le Code civil suisse (Livre cinquième: Droit des obligations); RS 220. ▪ Loi fédérale du 19 juin 1992 sur la protection des données (LPD); RS 235.1. ▪ Loi fédérale du 8 octobre 1982 sur l'approvisionnement économique du pays (LAP); RS 531. ▪ Loi fédérale du 6 octobre 2001 sur la surveillance de la correspondance par poste et télécommunications (LSCPT); RS 780.1. ▪ Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI); RS 120.
Ordonnance	▪ Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD); RS 235.11.
Autres documents et sources	▪ Stratégie nationale pour la protection des infrastructures critiques, Conseil fédéral, 27 juin 2012. ▪ Stratégie nationale de protection de la Suisse contre les cyberrisques, Conseil fédéral, 27 juin 2012. ▪ Convention sur la cybercriminalité, Conseil de l'Europe, 2001.
Autres sources	▪ Denning, D., 2006: A View of Cyberterrorism Five Years Later. Naval Post Graduate School, Monterey, Canada. ▪ Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI): Rapports semestriels ▪ Ministère estonien de l'économie et des communications, Département d'Etat des systèmes d'information, 2008: Information Technology in Public Administration of Estonia. Yearbook 2007. Tallinn. ▪ Davis, J., 2007: Hackers Take Down the Most Wired Country in Europe. Wired Magazine, Issue 15/09.
Source de la photo	▪ FOCP