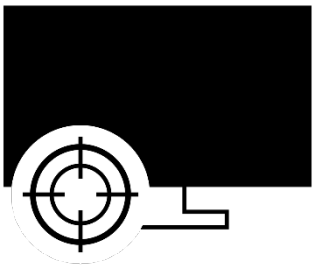
Cyberattaque



Le présent dossier fait partie de l'analyse nationale des risques « Catastrophes et situations d'urgence en Suisse »

Définition

La Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) définit les cyberattaques comme des actes illicites commis par des acteurs privés ou étatiques dans le cyberespace dans le but de nuire à l'intégrité, à la confidentialité ou à la disponibilité d'informations ou de données ; selon la nature de l'attaque, celle-ci peut avoir des conséquences sur le plan physique.

Les cyberattaques se répartissent entre différents domaines en fonction de la motivation de leurs auteurs et des moyens dont ces derniers disposent :

- cybercriminalité : infractions commises dans le cyberespace ou avec des cybermoyens dans un but d'enrichissement
- cyberextorsion : chantage exercé à l'aide de rançongiciels
- cybersabotage et cyberterrorisme : dommages infligés aux infrastructures informatiques et à des biens physiques, parfois dans un but de démonstration de force et d'intimidation
- cyberespionnage : accès non autorisé à des informations économiques, politiques ou militaires (confidentielles)
- désinformation et propagande : désorientation du public par la diffusion ciblée de fausses informations
- cyberattaques lors de conflits : attaques hybrides et asymétriques pouvant aller jusqu'à une véritable cyberguerre

Les frontières entre les différentes formes de cyberattaques sont poreuses.

novembre 2020

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral de la protection de la population OFPP

Exemples d'événements

Les exemples concrets aident à mieux comprendre la nature d'un type d'événement. Ils illustrent la manière dont il survient, son déroulement et ses conséquences.

---

27 juin 2017
Ukraine

Attaque au moyen d'un rançongiciel

En juin 2017, le rançongiciel NotPetya affecte des ordinateurs dans le monde entier, en particulier en Ukraine. Des données sont verrouillées sur le disque dur et la victime se voit ordonner de payer une rançon pour obtenir le déverrouillage. L'attaque touche non seulement des organisations ukrainiennes mais aussi des multinationales comme l'armateur danois Maersk, la compagnie pétrolière russe Rosneft, le groupe pharmaceutique américain Merck Sharp & Dohme ou le géant de l'agroalimentaire Mondelez. Maersk chiffre à 300 millions de dollars américains les dommages qu'elle subit. D'autres entreprises déclarent des dommages équivalents.

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 font l'objet d'attaques massives par déni de service distribué (DDoS). Cette opération de représailles est attribuée à la mouvance du groupe Anonymous. Pendant des heures, les sites attaqués sont inaccessibles et incapables d'effectuer des transactions en ligne. Il n'est pas possible de chiffrer le montant exact des dommages.

Avril / mai 2007
Estonie

Attaque DDoS de grande envergure

Suite au déplacement par les autorités estoniennes d'un monument célébrant l'armée soviétique du centre de Tallinn vers un cimetière militaire situé en périphérie, des inconnus paralysent 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 sont piratés et modifiés. Par ailleurs, des routeurs de backbone et des serveurs DNS subissent également des attaques, ce qui entraîne des interruptions de trafic (de moins de cinq minutes) au niveau des réseaux dorsaux. Les attaques contre les deux plus grandes banques du pays causent l'interruption des services bancaires par internet de l'une d'entre elles (pendant un peu moins de deux heures). Une banque visée chiffre les pertes subies suite à cette cyberattaque à environ 1 million de dollars américains. Aucune information n'est donnée quant aux dégâts causés aux infrastructures et aux systèmes informatiques de l'État estonien. L'intégrité des systèmes les plus importants n'est pas affectée, toutefois les systèmes sont saturés et la population n'a plus accès, ou alors difficilement, aux systèmes informatiques.

Facteurs d'influence

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

Source de danger	— Caractéristiques des auteurs (idéologie et motivations, disposition à la violence, capacité de nuisance, savoir-faire, degré d'organisation et de professionnalisation, ressources financières et informatiques, infrastructures contrôlées / déjà disponibles) — Attitude d'un État tiers ou d'organisations (criminelles ou paraétatiques) présentes dans le pays — Vulnérabilité des systèmes cibles (maintenance lacunaire ou impossible, sous-estimation des risques par les dirigeants, gouvernance et processus de sécurité informatique lacunaires, interconnexion des systèmes, interdépendances et complexité, degré de perméabilité de l'État, de l'économie et de la société, monoculture informatique, logiciels et matériel défectueux, manque de conformité, négligence, mesures de protection d'ordre organisationnel, technique ou architectural mises en œuvre)
Moment	— Généralement, en lien avec des décisions et des développements économiques, politiques ou sociaux — Jour ouvrable, jour férié ou week-end, en général à un moment inattendu pour la victime — Les préparatifs de l'attaque peuvent avoir lieu nettement plus tôt. La préparation des moyens d'action et des infrastructures nécessaires peut déjà avoir eu lieu dans un autre contexte.
Localisation / étendue	— Dimensions et caractéristiques de la cible (individu ou objectif isolé, organisation ou entreprise, branche, secteur, degré d'interconnexion des secteurs, technologie spécifique, institutions de l'État, etc.) — Source de l'attaque (lieu où se trouvent l'auteur et ses complices) — Infrastructures utilisées (matériel, logiciels, réseaux, interfaces, technologies, protocoles, etc.)
Déroulement	— Efficacité des mesures préventives, y compris de la pratique juridique — Préparation de l'attaque — Déroulement de l'attaque (unique ; par vagues ; montant lentement en puissance ou s'aggravant rapidement ; hybride, combinée avec des actions physiques) — Efficacité des contre-mesures spécifiques prises — Comportement et réaction des personnes, organisations, États concernés — Comportement et réaction des forces d'intervention, des autorités responsables et des experts impliqués — Réaction de la population et des milieux politiques

Intensité des scénarios

Selon les facteurs d'influence, différents événements peuvent se dérouler avec des intensités différentes. Les scénarios ci-après représentent un choix parmi de nombreuses possibilités et ne constituent pas une prévision. Ils permettent d'anticiper les conséquences potentielles d'un événement afin de pouvoir s'y préparer.

---

1 — Considérable

- Forme d'attaque connue
- Existence de contre-mesures ou possibilité d'en développer rapidement
- Attaque prévisible et unique
- Attaques visant des infrastructures critiques industrielles ou gouvernementales
- Vol de données concernant l'économie ou le gouvernement
- Le public n'est pas visé par l'attaque
- Le public ne prend connaissance de l'attaque qu'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
- Attaque par vagues, pas complètement imprévisible
- Vol de données concernant l'économie ou le gouvernement
- 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)
- Le public est informé des attaques pendant leur déroulement
- Public indirectement touché par les attaques, effets ressentis dans la vie quotidienne

---

3 — Extrême

- Forme d'attaque nouvelle ou perfectionnée (p. ex. rançongiciels avec back-ups verrouillés)
- Absence de contre-mesures, dont le développement prendra des semaines ou est impossible dans un délai utile
- Attaque totalement imprévisible, dont la forme évolue, avec une escalade
- 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
- Le public se rend tout de suite compte des attaques
- Public directement touché par les attaques, effets ressentis dans la vie quotidienne

Scénario

Le scénario suivant est fondé sur le degré d'intensité majeur.

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 État 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 aux autorités compétentes (Centrale d'enregistrement et d'analyse pour la sûreté de l'information [MELANI] / Centre national pour la cybersécurité [NCSC]) ou aux autorités de poursuite pénale locales. MELANI/NCSC évalue les informations et les transmet aux autorités compétentes et aux entreprises touchées. Le Conseil fédéral condamne les attaques et défend la position de la Suisse. Un à trois jours après la déclaration du Conseil fédéral, les attaques se concentrent sur les sites internet des pouvoirs publics 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. De plus, un grand nombre de collaborateurs choisis au hasard sont bombardés d'e-mails contenant des pièces jointes renfermant un logiciel de verrouillage. Le nettoyage et la réinitialisation des ordinateurs touchés prennent beaucoup de temps. De surcroît, on enregistre des tentatives de pénétration des systèmes de données de la Confédération sans que l'on constate toutefois de vol. 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 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. Pour ce faire, on commence par attaquer

les fournisseurs de services informatiques de ces instituts financiers pour tenter d'accéder ensuite aux systèmes et aux données via leurs droits d'accès direct.

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 État 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. Pour les fournisseurs de services internet moins bien protégés, la remise en service prend un peu plus de temps ou s'avère impossible. À 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 semaines après la fin des attaques à estimer l'ampleur de la perte de données.

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

Déroulement dans le temps

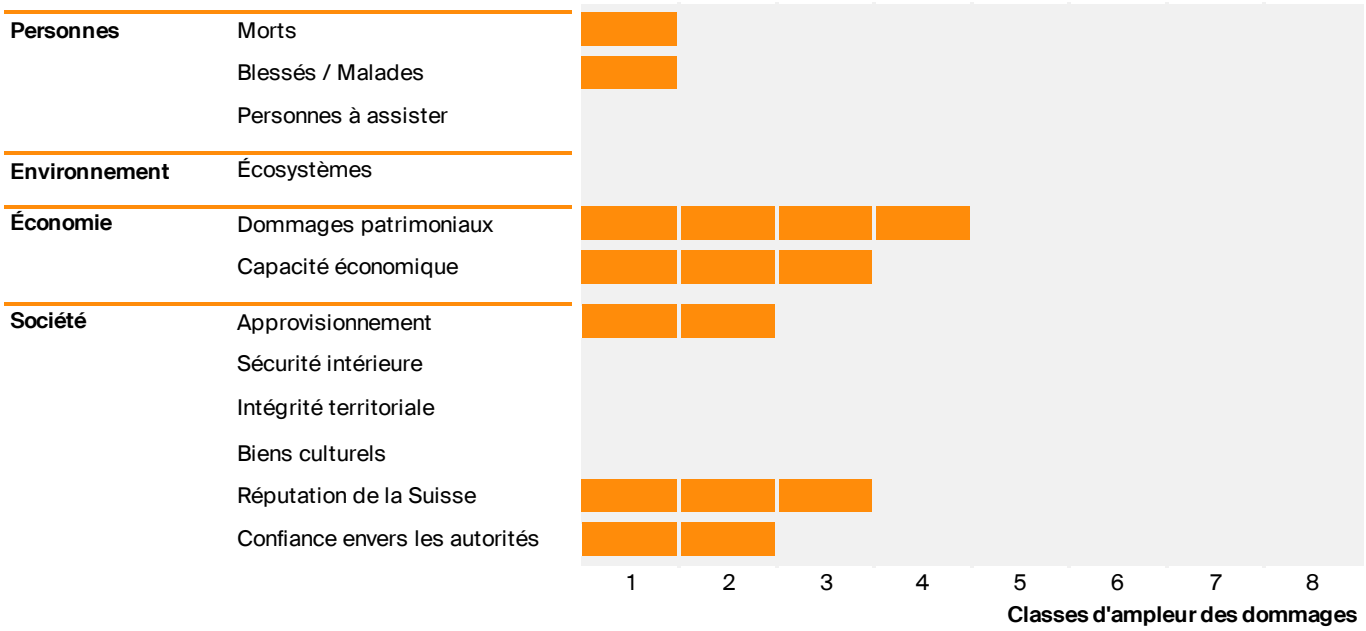
Les cyberattaques s'étendent sur cinq bons mois et surviennent en trois phases (1. piratage de sites internet de médias, 2. attaques des infrastructures informatiques de la Confédération, 3. opérations contre les infrastructures informatiques du secteur financier). Les conséquences se font ressentir,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

Extension dans l'espace

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

Pour évaluer les conséquences d'un scénario, on l'examine à l'aune de douze indicateurs répartis dans quatre domaines. L'ampleur attendue du scénario décrit est représentée dans le diagramme et commentée dans le texte ci-après. Chaque classe d'ampleur supérieure correspond à une augmentation des dommages de facteur trois.



Personnes	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 aux écosystèmes.
Économie	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 mesures 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. Étant 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.

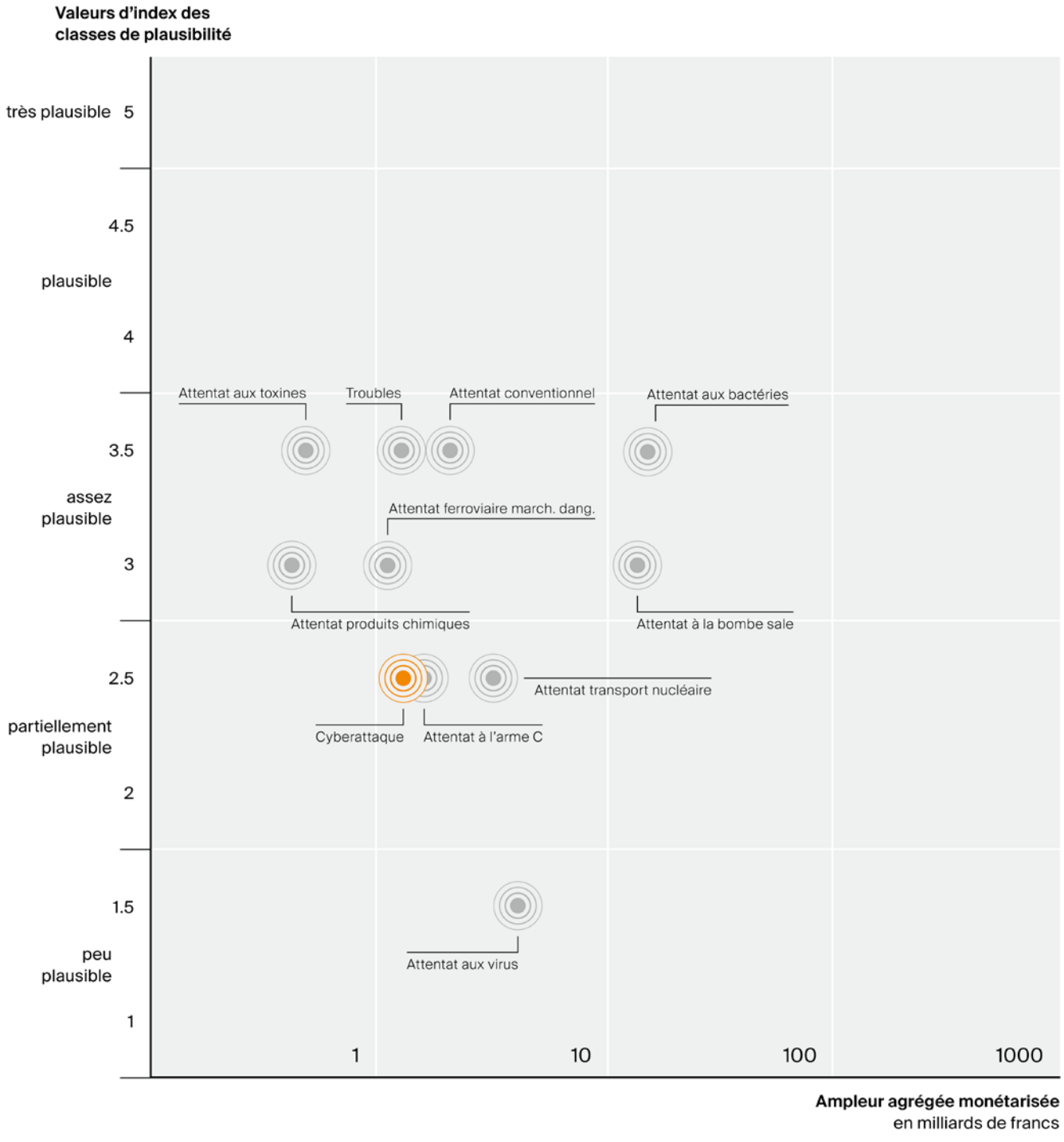
Les événements suscitent l'inquiétude de la population, mais pas de panique. Par contre, sa confiance dans les autorités et les établissements financiers est ébranlée. Les établissements concernés doivent engager du personnel de sécurité supplémentaire en raison de l'afflux de clients aux guichets. L'ordre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

Risque

La plausibilité et l'ampleur des dommages liés au scénario décrit sont comparées à celles des autres scénarios analysés dans une matrice de plausibilité (voir ci-dessous). La plausibilité des scénarios d'événements sciemment provoqués est représentée sur l'axe des y (5 classes de plausibilité) et l'ampleur des dommages est agrégée et monétarisée en CHF sur l'axe des x (échelle logarithmique). Le produit de la plausibilité et de l'ampleur des dommages représente le risque lié à un scénario. Plus un scénario se situe en haut à droite de la matrice, plus le risque est élevé.



Bases juridiques

Lois	— Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI) ; RS 120. — 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. — Code pénal suisse du 21 décembre 1937 ; RS 311.0. — Loi fédérale du 17 juin 2016 sur l'approvisionnement économique du pays (LAP) ; RS 531. — Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunications (LSCPT) ; RS 780.1.
Ordonnances	— Ordonnance du 27 mai 2020 sur les cyberrisques (OPCy) ; RS 120.73. — Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD); RS 235.11. — Ordonnance du 2 mars 2018 sur l'État-major fédéral Protection de la population (OEMFP) ; RS 520.17.
Autres bases légales	— Conseil de l'Europe (2001) : Convention européenne sur la cybercriminalité.

Informations complémentaires

Au sujet du danger de cyberattaque

- Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) (différentes années) : Sûreté de l'information. Situation en Suisse et à l'étranger. Rapports semestriels. DFF et DDPS, Berne.
- Check Point (2019) : Cyber Attack Trends: 2019 Mid-Year Report.
- Le Conseil fédéral (2018) : Strategie nationale de protection de la Suisse contre les cyberrisques (SNC) 2018–2022. UPIC, Berne.
- Le Conseil fédéral (2012) : Strategie nationale de protection de la Suisse contre les cyberrisques. DDPS, Berne.
- Le Conseil fédéral (2017) : Stratégie nationale de protection des infrastructures critiques 2018–2022. Berne.
- Le Conseil fédéral (2012) : Stratégie nationale de protection des infrastructures critiques. Berne.
- Denning, D. E. (2007) : A View of Cyberterrorism Five Years Later. In: Himma, K. (Hrsg.): Internet Security. Hacking, Counterhacking and Society. Jones and Bartlett, Boston.
- European Union Agency for Network and Information Security (ENISA) (2019) : ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. EU, Heraklion.
- Ministry of Economic Affairs and Communications: Department of State Information Systems (2008) : Information Technology in Public Administration of Estonia. Yearbook 2007. Tallinn.

Au sujet de l'analyse nationale des risques

- Office fédéral de la protection de la population (OFPP) (2020) : À quels risques la Suisse est-elle exposée ? Catastrophes et situations d'urgence en Suisse 2020. OFPP, Berne.
- Office fédéral de la protection de la population (OFPP) (2020) : Méthode d'analyse nationale des risques. Catastrophes et situations d'urgence en Suisse 2020. Version 2.0. OFPP, Berne.
- Office fédéral de la protection de la population (OFPP) (2020) : Rapport sur l'analyse nationale des risques. Catastrophes et situations d'urgence en Suisse 2020. OFPP, Berne.
- Office fédéral de la protection de la population (OFPP) (2019) : Liste des dangers. Catastrophes et situations d'urgence en Suisse. 2e édition. OFPP, Berne.

Office fédéral de la protection de la population OFPP

Guisanplatz 1B
CH-3003 Berne
risk-ch@babs.admin.ch
www.protpop.ch
www.risk-ch.ch