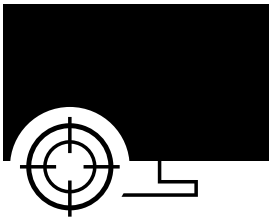
Cyberattaque



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

Définition

La Cyberstratégie nationale (CSN) définit les cyberattaques comme des actes illicites intentionnels commis par des acteurs privés ou étatiques via des technologies de l'information et de la communication (TIC) 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 également 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
- Cyberespionnage : accès non autorisé à des informations (confidentielles) économiques, politiques ou militaires
- Cybersabotage : dommages causés intentionnellement à des technologies de l'information et de la communication (TIC) et à des biens physiques dans un but de démonstration de force et d'intimidation
- Cybersubversion : affaiblissement du système politique d'un autre État par des acteurs étatiques, proches de l'État ou politiques
- Cyberopérations dans des conflits armés : attaques hybrides et asymétriques pouvant aller jusqu'à une véritable cyberguerre

Les formes de cyberattaques sont souvent combinées et leurs frontières sont poreuses. Le présent dossier traite notamment de la cybercriminalité, du cybersabotage et de la cybersubversion.

Février 2026

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral de la protection de la population OFPP

Contenu

Exemples d'événements 3

Facteurs d'influence 4

Intensité des scénarios 6

Scénario 7

Conséquences 9

Risque 12

Bases juridiques 13

Informations complémentaires 14

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.

Janvier 2025 **Suisse** **Attaques DDoS**	En janvier 2025, la Suisse a subi plusieurs attaques par déni de service distribué (Distributed Denial-of-Service, DDoS) revendiquées par deux groupes d'hacktivistes différents. Le 6 janvier 2025, les distributeurs automatiques d'argent, le site Internet et l'application d'e-banking d'une banque suisse sont bloqués par une attaque par déni de service distribué mais la plupart des services redeviennent disponibles en fin de journée. Le groupe d'hacktivistes pro-musulman RooTDoS a revendiqué ces attaques et les a justifiées par le fait que la Suisse a adopté une loi islamophobe avec l'entrée en vigueur de la loi sur l'interdiction de se dissimuler le visage. Le 10 janvier, d'autres attaques sont menées sur les services Web de l'administration fédérale suisse par ce groupe d'hacktivistes. Pendant environ 45 minutes, des services tels que la téléphonie, Outlook et divers sites Web et applications spécialisées de la Confédération ont été touchés mais la situation a pu être stabilisée grâce à des contre-mesures. Du 20 au 26 janvier 2025, le groupe d'hacktivistes pro-russe NoName057(16) a perpétré quotidiennement des attaques DDoS contre divers sites Web suisses, dont des sites Web de la région de Davos, du secteur des médias, de banques suisses, de communes et cantons ainsi que de portails d'accès à des services publics. Ces attaques se sont produites lors du Forum économique mondial (FEM) à Davos lors de la visite du président ukrainien Volodymyr Zelensky. NoName057(16) a revendiqué ces attaques. L'Office fédéral de la cybersécurité (OFCS) s'attendait à de telles attaques lors du FEM et avait averti au préalable les exploitants d'infrastructures critiques.
Février 2022 **Ukraine** **Cybersabotage**	Le 24 février 2022, les connexions aux satellites KA-SAT de l'entreprise américaine ViaSat ont été interrompues à maintes reprises. De nombreux utilisateurs privés, sociétés et administrations européens utilisent ce satellite de communication pour l'accès à Internet, notamment dans les régions reculées. L'incident a entraîné des perturbations en Ukraine, mais également au-delà de ses frontières. En Allemagne par exemple, l'accès à des systèmes de surveillance et de commande à distance de parcs d'éoliennes n'était plus possible. ViaSat a publié une analyse de l'incident. Celle-ci montre qu'il s'agissait d'une cyberattaque ciblée destinée à toucher uniquement la partie du réseau satellitaire couvrant l'Ukraine mais dont les répercussions n'ont pas pu être limitées. En outre, depuis le début de la guerre en Ukraine, différents wipers sont apparus. L'objectif de ces maliciels est de détruire des données, en les rendant illisibles ou en les cryptant et donc de les effacer définitivement. Des organisations de divers domaines de l'administration publique ainsi que des secteurs énergétique et financier ont été visées.
De mars à décembre 2020 **États-Unis** **Cyberespionnage**	Le 13 décembre 2020, les autorités américaines ont annoncé qu'un groupe de hackers s'était introduit dans leur réseau via une mise à jour compromise du logiciel Orion IT. En mars 2020, une porte dérobée a effectivement été créée dans la mise à jour officielle du programme. Environ 18 000 utilisateurs de ce logiciel avaient téléchargé la mise à jour. Les hackers ont cherché des cibles intéressantes pour poursuivre l'attaque et ont refermé cette porte dérobée chez les victimes collatérales concernées. Selon des sources américaines, cette opération faisait partie d'une campagne d'espionnage à plus grande échelle qui concernait également d'autres entreprises.

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, accès à des ressources financières et informatiques et à des infrastructures – Comportement de l'auteur concerné (étatique ou non étatique) – Vulnérabilité des systèmes cibles (sous-estimation des risques de cybermenaces, gouvernance et processus de sécurité de l'information lacunaires, logiciels et matériel défectueux, maintenance lacunaire ou inexistante, manque de conformité, négligence, mesures de protection d'ordre organisationnel, technique ou architectural inexistantes) – Interdépendances et complexité des systèmes (Cloud Services, risques pesant sur les chaînes d'approvisionnement, etc.), degré de perméabilité de l'État, de l'économie et de la société – Nouvelles possibilités techniques d'attaques contre lesquelles il n'existe éventuellement pas encore de dispositif de défense (intelligence artificielle, informatique quantique, etc.)
Moment	– Généralement, en lien avec des décisions et des développements économiques, politiques ou sociaux – Heure de la journée et jour de la semaine : le moment de la cyberattaque est souvent choisi de telle sorte que la victime dispose de peu de ressources pour détecter et réagir (week-end, période de vacances). – Les préparatifs de la cyberattaque peuvent avoir lieu nettement plus tôt que l'attaque elle-même. 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 l'objet attaqué ou du système cible (individu ou objet isolé, organisation ou entreprise, branche, secteur, degré d'interconnexion des secteurs, technologie spécifique, institutions de l'État, etc.) – Identification des auteurs (attribution) et localisation (lieu où se trouvent les auteurs et leurs complices) – Ressources utilisées (matériel, logiciels, réseaux, interfaces, technologies, protocoles, ressources humaines, etc.)

Déroulement	– Prévisibilité du moment et du lieu de survenance, du type et de l'intensité de l'événement (délais de préalerte, moment de la diffusion de consignes de comportement) – Forme et caractéristiques de l'attaque (connues / inconnues) – Efficacité des mesures de protection préventives – Déroulement de l'attaque (unique ; par vagues ; montant lentement en puissance ou s'aggravant immédiatement ; hybride, combinée avec des actions physiques) – Efficacité des contre-mesures spécifiques prises – Comportement et réaction des personnes, organisations et États concernés – Comportement et réaction des forces d'intervention, des autorités responsables et des experts et prestataires de sécurité impliqués (Computer Security Incident Response Team (CSIRT), Computer Emergency Response Team (CERT), Security Operation Center (SOC), etc.) – 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 – Ne survient qu'une seule fois – 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	– Combinaison de formes d'attaques connues ou forme d'attaque relativement inconnue – Absence de contre-mesures, mais possibilité d'en développer en quelques jours – Survient par vagues – 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 (p. ex. e-banking) – Le public est informé des attaques pendant leur déroulement – Public touché par les attaques, effets ressentis dans la vie quotidienne (p. ex. retrait d'argent liquide impossible ; les transactions ne peuvent pas être effectuées)
3 — Extrême	– Forme d'attaque nouvelle ou améliorée – Absence de contre-mesures, dont le développement prendra des semaines ou est impossible dans un délai utile – Forme d'attaque changeante, aggravation de l'attaque – Attaques visant des infrastructures critiques dans les secteurs de l'énergie, des télécommunications et des transports – Manipulation et endommagement physiques 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

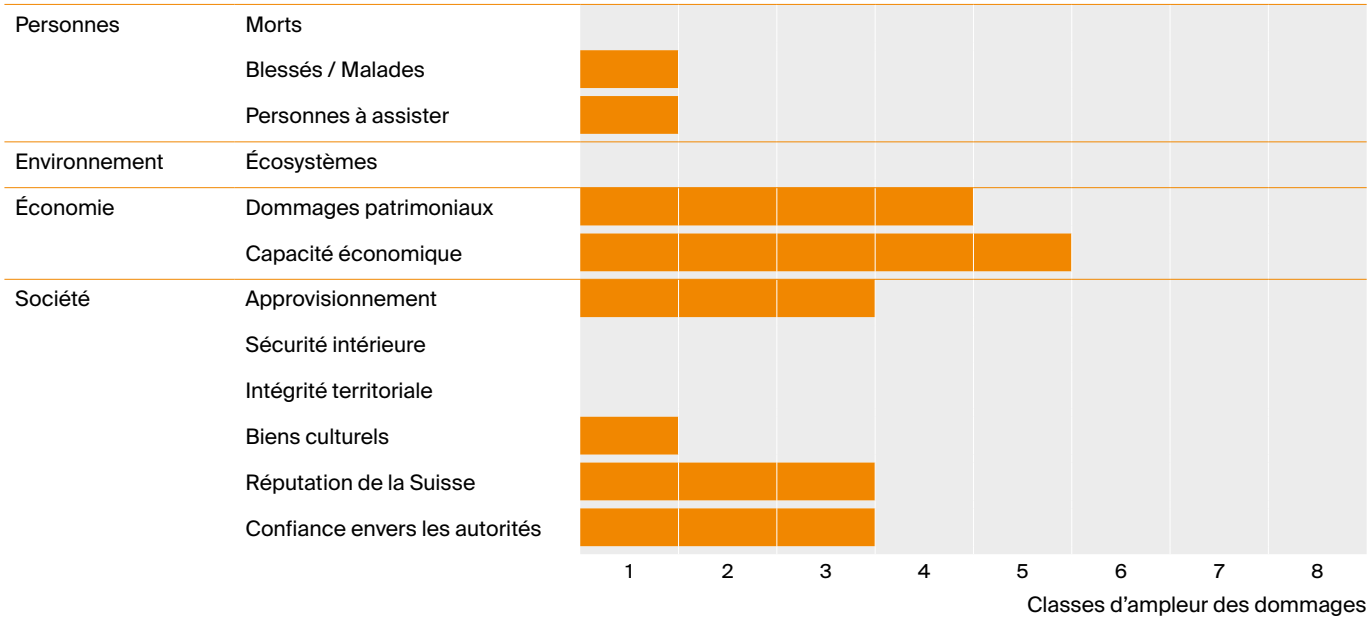
Le scénario suivant est fondé sur le degré d'intensité majeur.

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 Internet d'organisations et de portails d'information sont compromis. De fausses informations sont volontairement diffusées via des sites Internet manipulés et sur les réseaux sociaux. 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, à savoir l'Office fédéral de la cybersécurité (OFCS) ou les autorités de poursuite pénale locales. L'OFCS évalue ces informations dans leur ensemble et transmet ses résultats aux autorités compétentes et aux entreprises touchées. Dans une prise de position officielle, le Conseil fédéral condamne les attaques sur les sites Internet et défend la position de la Suisse ressentie comme une provocation. Un à trois jours après la déclaration du Conseil fédéral, les attaques DDoS 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 municipaux et cantonaux ont pu être piratés et servir de porte d'entrée aux attaques. Désormais, en plus de la manipulation des sites Internet, les prestations en ligne des offices fédéraux concernés (cyberadministration) sont également gravement perturbées. De plus, un grand nombre de collaboratrices et de collaborateurs choisis au hasard sont bombardés d'e-mails contenant des pièces jointes renfermant un rançongiciel. Le nettoyage et la réinitialisation des ordinateurs touchés prennent beaucoup de temps. Quelques tentatives d'intrusion dans des systèmes TIC de la Confédération sont également signalées. Aucun transfert de données n'a toutefois été constaté. Les services de la Confédération concernés informent l'OFCS de ces événements. Trois semaines plus tard, les attaques touchent le secteur financier. Ce sont d'abord les sites Internet de divers prestataires financiers qui sont attaqués. Des fonctions importantes sont fortement perturbées pendant deux à trois semaines. Pendant plusieurs jours, les communications de la bourse suisse sur son site 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 de plusieurs commerçants de détail sont touchés dans toute la Suisse du fait de la mise hors service pendant deux jours des serveurs correspondants. Une grande partie des distributeurs automatiques d'argent dans toute la Suisse n'est pas disponible ou seulement partiellement.

	Les échanges de courriels sont considérablement perturbés par une avalanche de spams (parmi lesquels de nombreux courriels de propagande) et d'e-mails d'hameçonnage. Les organisations fournissant des services aux établissements financiers, en particulier celles qui fournissent des informations financières, subissent elles aussi des attaques. Le traitement de transactions est également perturbé. Pour s'introduire dans les systèmes informatiques des établissements financiers, les hackers commencent par attaquer les fournisseurs de services informatiques de ces établissements pour tenter d'accéder ensuite aux systèmes et aux données via leurs droits d'accès direct. La bourse de Zurich est attaquée par un malware apparemment depuis l'extérieur de la Suisse peu après l'ouverture des transactions. Les auteurs parviennent à insérer un malware dans un système qui est lié aux systèmes de la bourse suisse. La bourse est alors 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. Ils parviennent à identifier l'organisation responsable des attaques. Un État tiers parvient à rendre inoffensive l'infrastructure utilisée pour perpétrer les attaques puis l'organisation elle-même. Les attaques diminuent ensuite très rapidement.
Phase de rétablissement	Les sites Internet des autorités, des établissements financiers et des médias peuvent être rétablis au fur et à mesure et fonctionnent à nouveau normalement. Une semaine après la fin des attaques, les principaux sites Internet visés sont à nouveau utilisables. Pour les fournisseurs mal protégés, la remise en service prend un peu plus de temps. À peu près un mois après la cessation des attaques, tous les sites internet fonctionnent à nouveau comme auparavant. 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	La phase de l'événement dure environ cinq mois et se déroule en trois vagues : 1 : Compromission des sites Internet des médias. 2 : Attaques menées contre l'infrastructure informatique de la Confédération. 3 : Attaques menées 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

Aucun décès n'est à déplorer.

Les querelles devant les distributeurs automatiques d'argent causent quelques blessés. Certaines personnes subissent une forte charge psychique et doivent également être prises en charge. La défense et la maîtrise immédiate de l'attaque créent une forte charge de travail pour le personnel spécialisé des organisations touchées. Cela crée des états d'épuisement chez certaines collaboratrices et certains collaborateurs du service informatique. Les attaques contre l'État et le système financier ainsi que la désinformation suscitent en outre des craintes pour l'avenir chez de nombreuses personnes. Au total, on estime à 100 le nombre de blessés légers.

Quelque 20 000 bénéficiaires de l'aide sociale sont également touchés par la panne des services financiers. Ils n'ont quasiment pas de réserves financières et doivent donc bénéficier d'une aide supplémentaire pendant dix jours.

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.

Le trafic des paiements de plusieurs commerçants de détail est perturbé temporairement dans toute la Suisse. Une grande partie des distributeurs automatiques d'argent dans toute la Suisse n'est pas disponible, ce qui crée des pénuries sur les distributeurs qui fonctionnent encore.

De moins en moins de guichets permettant de retirer de l'argent liquide sont disponibles. Le retrait d'argent liquide est donc restreint.

Une fois les perturbations résolues, on constate une forte augmentation de la demande en denrées alimentaires, en biens de consommation courante et en espèces, ce qui entraîne à son tour des pénuries à court terme.

Les services en ligne des établissements financiers concernés sont fortement limités et sont éventuellement corrompus ou indisponibles. Comme les transactions correspondantes comme les ordres de paiement et de bourse ne peuvent pas être réalisées au guichet, on enregistre des retards de paiement. Les clients perdent donc confiance, certains résilient leurs contrats, dont certains gros clients internationaux. Plusieurs plaintes et demandes de dédommagement sont également déposées.

Les organisations concernées subissent d'autres dommages financiers car elles doivent consentir des efforts supplémentaires en ressources techniques et humaines pour juguler et contrer les attaques, évaluer le flux de données transférées et identifier leurs auteurs. Par ailleurs, elles doivent prendre des mesures de sécurité supplémentaires.

La douane suisse est également restreinte en raison des pannes.

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 1,7 milliard de francs en raison de la réduction des activités économiques qu'il a entraînée.

Société

On constate les pénuries et interruptions d'approvisionnement suivantes :

- Services financiers : l'événement provoque des interruptions des services financiers (argent liquide et transactions en ligne) ; environ 4 millions de personnes sont concernées pendant 3 jours. Toutefois, la paralysie des établissements financiers concernés n'entraîne pas de rupture importante d'approvisionnement.
- Denrées alimentaires : les restrictions de retrait d'argent liquide et des transactions financières empêchent les personnes de faire leurs courses alimentaires comme à l'accoutumée. Environ 400 000 personnes sont touchées.
- Approvisionnement en pétrole : faire le plein de carburant n'est possible qu'en payant en liquide dans la plupart des stations en raison de la panne des terminaux de paiement. Environ 100 000 personnes sont touchées.
- Médias : l'attaque visant les médias entraîne une réduction de l'offre des services de médias. Environ 500 000 personnes sont touchées pendant dix jours.

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

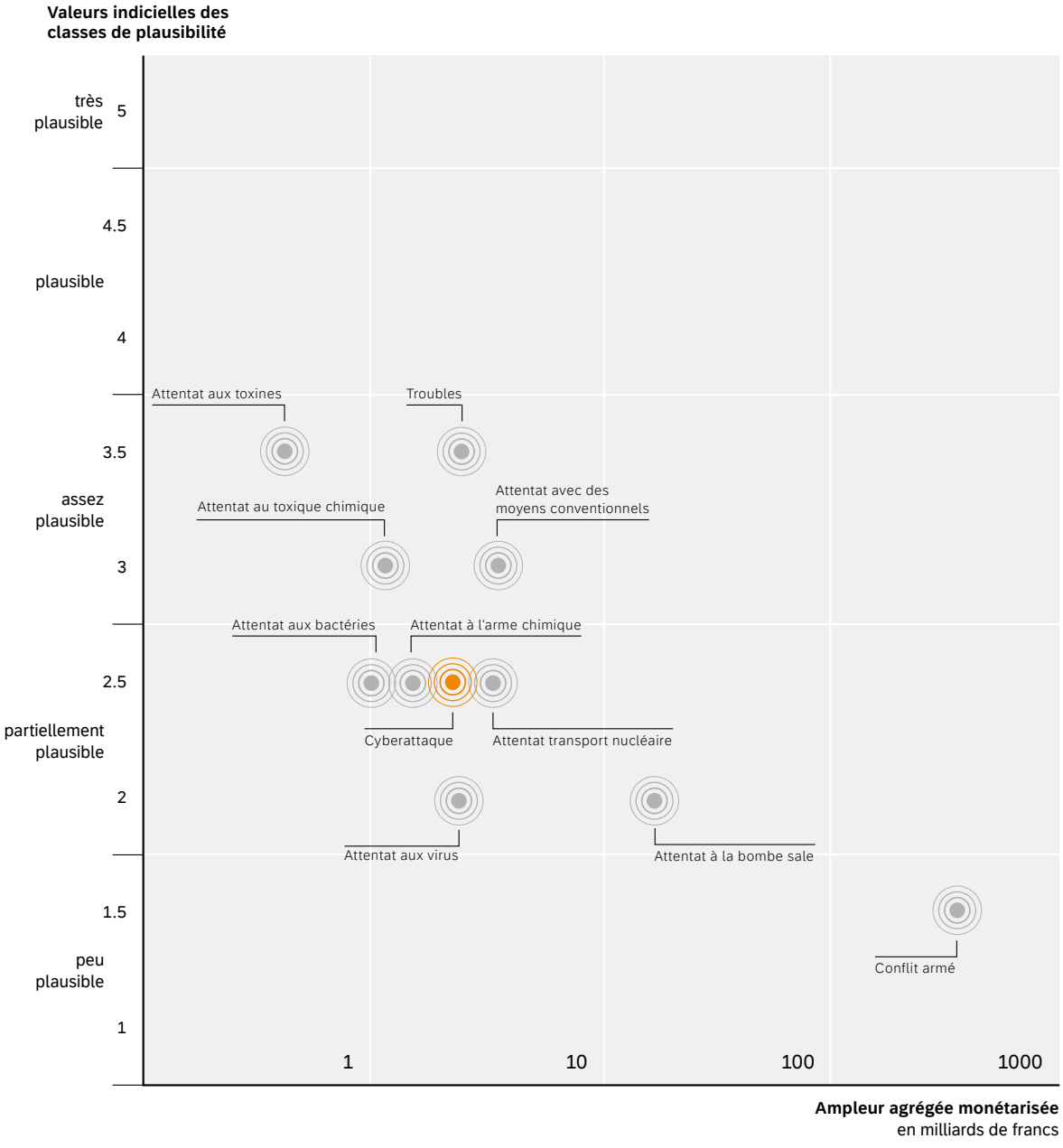
Les biens culturels (numériques) ne sont quasiment pas en danger. Les grandes archives notamment sont toutefois connectées aux systèmes informatiques cantonaux. Des cyberattaques contre des systèmes cantonaux peuvent donc entraver et réduire la disponibilité des fonds d'archives. En outre, une destruction irréversible, un vol ou une publication d'informations sensibles contenues dans les archives sont également possibles.

Les médias internationaux parlent de manière répétée des diverses vagues de cyberattaques. L'attaque contre des institutions financières et la fermeture de la bourse pendant deux jours suscitent une grande attention internationale.

Suite aux attaques, les médias suisses se montrent également critiques pendant plusieurs semaines (« Une Suisse si vulnérable ! »), et la polémique ne reste pas sans effet 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. 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 18 décembre 2020 sur la sécurité de l'information (LSI) ; RS 128 – Loi fédérale du 30 mars 1911 complétant le Code civil suisse (Livre cinquième : Droit des obligations) ; RS 220. – Loi fédérale du 25 septembre 2020 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 (Loi sur l'approvisionnement 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 8 novembre 2023 sur la sécurité de l'information dans l'administration fédérale et l'armée (Ordonnance sur la sécurité de l'information, OSI) ; RS 128.1. – Ordonnance du 7 mars 2025 sur la cybersécurité (OCyS) ; RS 128.51. – Ordonnance du 20 décembre 2024 sur l'organisation de crise de l'administration fédérale (OCAF) ; RS 172.010.8. – Ordonnance du 31 août 2022 sur la protection des données (OPDo) ; RS 235.11.
Autres bases juridiques	– Conseil de l'Europe (2001) : Convention européenne sur la cybercriminalité.

Informations complémentaires

Au sujet du danger en question

- Agence de l'Union européenne pour la cybersécurité (ENISA) (2019) : Rapport de l'ENISA sur le paysage des menaces 2018. Les 15 principales menaces. EU, Heraklion.
- 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.
- Le Conseil fédéral (2023) : Cyberstratégie nationale (CSN). Office fédéral de la cybersécurité (OFCS), Berne.
- Le Conseil fédéral (2023) : Stratégie nationale de protection des infrastructures critiques. OFPP, Berne.
- Ministère des affaires économiques et des communications : département des systèmes d'information d'État (2008) : Information Technology in Public Administration of Estonia. Yearbook 2007. Tallinn.
- Office fédéral de la cybersécurité (OFCS) (diverses années de parution) : Sûreté de l'information : situation en Suisse et sur le plan international. Rapport semestriel. DFF et DDPS, Berne.

Au sujet de l'analyse nationale des risques

- Office fédéral de la protection de la population (OFPP) (2026) : Dossiers sur les dangers. Catastrophes et situations d'urgence en Suisse 2025. OFPP, Berne.
- Office fédéral de la protection de la population (OFPP) (2026) : À quels risques la Suisse est-elle exposée ? Catastrophes et situations d'urgence en Suisse 2025. OFPP, Berne.
- Office fédéral de la protection de la population (OFPP) (2026) : Méthode d'analyse nationale des risques. Catastrophes et situations d'urgence en Suisse 2025. Version 3.0. OFPP, Berne.
- Office fédéral de la protection de la population (OFPP) (2026) : Rapport sur l'analyse nationale des risques. Catastrophes et situations d'urgence en Suisse 2025. OFPP, Berne.
- Office fédéral de la protection de la population (OFPP) (2023) : Liste des dangers. Catastrophes et situations d'urgence en Suisse 2025. 3e édition. OFPP, Berne.

Impressum

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

88.128.14.f