_swissprivacy.law

Nouvelle cyberstratégie nationale : objectif de protection contre les cybermenaces

Pauline Meyer, le 22 mai 2023

Le Conseil fédéral et les cantons ont adopté la nouvelle cyberstratégie nationale le 5 avril 2023 pour protéger la Suisse contre les cybermenaces. La stratégie et son plan de mise en œuvre seront en vigueur jusqu'à leur examen dans cinq ans.

La nouvelle cyberstratégie nationale (CSN), qui remplace la stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC) de 2018, est adoptée en avril 2023 et pose les grandes lignes des mesures à prendre pour faire face aux principales cybermenaces en Suisse.

La CSN fait état des principales cybermenaces, au premier rang desquelles figurent les menaces liées aux cyberattaques liées à la cybercriminalité (notamment à visée patrimoniale), au cyberespionnage, au cybersabotage, à la cybersubversion et aux cyberopérations dans des contextes de conflits armés. Viennent ensuite les cybermenaces liées aux erreurs humaines et aux défaillances techniques et finalement les facteurs généraux ayant un impact sur les cybermenaces, à l'instar des développement technologiques (en lien notamment avec l'intelligence artificielle ou l'Internet des objets) ou des tensions géopolitiques.

Après avoir rappelé le contexte dans lequel la CSN est adoptée, cette dernière pose la vision, les objectifs stratégiques et les principes gouvernant celle-ci. La stratégie met un accent sur la responsabilisation de la Suisse et des différentes parties prenantes, sur la fiabilité des services numériques, sur la gestion de cyberincidents, la poursuite de la cybercriminalité et enfin le rôle de la Suisse sur le plan international.

La protection de la Suisse contre les cybermenaces préconise une approche fondée sur les risques, permettant de s'adapter et d'être cohérente avec la réalité selon laquelle tous les risques ne peuvent être évités. Un accent est maintenu sur la responsabilité et la coopération de toutes les parties prenantes, avec une limitation du rôle de l'État à une intervention subsidiaire et partenariale.

Le premier lot de mesures de la CSN vise la responsabilisation de toutes les parties prenantes, qui est un objectif. Il s'agit de mesures relatives à la formation, la sensibilisation et l'analyse et l'état de la situation, en impliquant différentes entités et mécanismes de coopération.

Ensuite, des mesures visent la réalisation de l'objectif de la CSN cherchant à garantir la fiabilité et la disponibilité de l'infrastructure et des services numériques. Ces mesures doivent servir à l'identification des vulnérabilités et leur gestion, à la coopération entre autorités pour accroître la cybersécurité et à une réglementation efficace. Cette dernière mesure comprend des analyses des besoins sectoriels en termes de réglementations et d'incitations au respect de ces dernières.

L'objectif de détection, prévention, gestion et défense efficaces contre les cyberattaques mobilise notamment des compétences privées (équipes de gestion de cyberincidents) et étatiques (Centre national pour la cybersécurité) dans la gestion technique des cyberincidents, les compétences du Service de renseignement (SRC) et des autorités de poursuite pénale pour l'attribution de cyberattaques, les compétences de l'armée (et du SRC) pour la cyberdéfense et un ensemble de compétence pour la gestion de crise.

La CSN prévoit que, pour améliorer la poursuite pénale de la cybercriminalité, il convient d'accroître la collaboration entre autorités de poursuite pénale, améliorer la vue d'ensemble des cas et former les autorités compétentes.

Finalement, l'objectif de renforcement du rôle de la Suisse sur le plan international passe par la « Genève internationale » et plus largement par l'implication de la Suisse dans la réglementation internationale du cyberespace et par la coopération bilatérale.

Cette nouvelle stratégie devrait permettre à la Suisse de continuer ses progrès dans sa cyberrésilience, notamment par la création et la réorganisation de structures disposant de compétences dans le domaine de la cybersécurité. Parmi ces nouveautés, la transformation du NCSC devrait permettre plusieurs améliorations, notamment en termes de compétences et de ressources, bien qu'elle apporte vraisemblablement plusieurs défis. En outre, la création de nouvelles structures, telles que l'Institut national de test pour la cybersécurité (NTC) détenant des compétences en lien avec l'appréhension des attaques contre les produits informatiques, devrait être à l'origine de progrès.

De manière générale, la nouvelle CSN consacre des priorités aujourd'hui essentielles dans la gestion de différentes cybermenaces. La stratégie ayant une portée générale et devant être

détaillée par un plan de mise en œuvre, l'adoption de ce dernier permettra en principe de mieux appréhender chaque étape concrète permettant de protéger la Suisse des cybermenaces.

Proposition de citation : Pauline MEYER, Nouvelle cyberstratégie nationale : objectif de protection contre les cybermenaces, 22 mai 2023 *in* www.swissprivacy.law/228