# Le partage d'information en cybersécurité

satw it's all about technology

# Enjeux pour la Suisse

## Contexte

La culture du numérique et de la cybersécurité repose sur le partage d'information et la mise à disposition des connaissances nécessaires à la construction des compétences dans les disciplines relatives à la politique, à l'économie, au management, à la sociologie, au droit et à la technologie (figure 1). Les centres de partage et d'analyse d'information (ISAC – Information Sharing & Analysis Center) concernent principalement des informations d'ordre technique. Ils constituent un type de plateforme d'échange d'information lié à la cybersécurité sachant que d'autres peuvent exister (Plateforme IE – Information Exchanges).

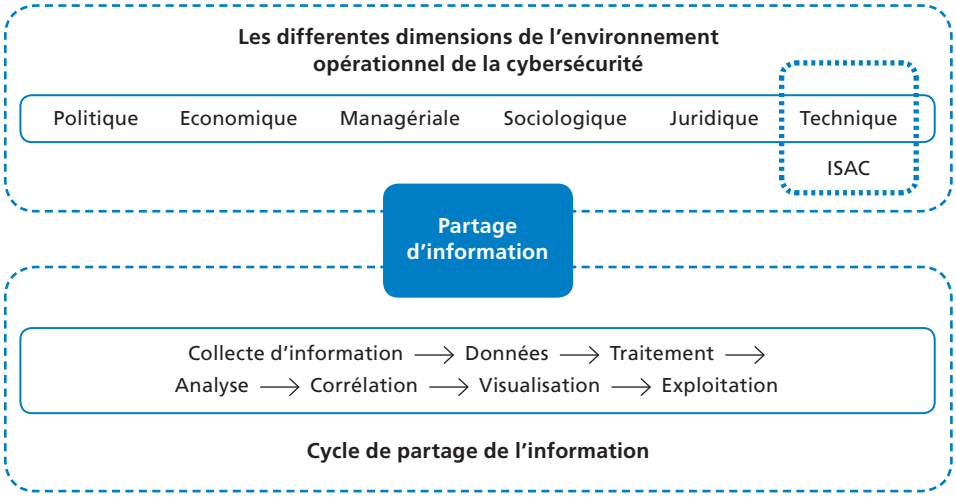


**Figure 1**
Partage d'information et dimension transdisciplinaire de la cybersécurité.

Parmi les cyberattaques pouvant nuire aux intérêts économiques d'une organisation, il ne faut pas sous-estimer les impacts dus à :

- des pertes d'actifs intangibles (réputation, propriété intellectuelle), des pertes d'opportunités ;
- des actions relevant de l'ingérence économique (surveillance, espionnage, sabotage, terrorisme, chantage, extorsion).

Une bonne connaissance des mécanismes de l'ingérence économique au regard des facilités offertes par le monde numérique, contribue au maintien des avantages concurrentiels des organisations. Ce qui contribue à une protection adaptée du capital scientifique, technique, économique et industriel du pays et à la bonne santé de la place économique. Dans tous ces domaines, un partage pertinent de l'information est nécessaire et doit être accompagné par des dispositifs de prévention des risques et de protections des actifs.

**Au niveau national**

Les individus, les organisations et l'Etat sont confrontés à des cyberrisques et aux besoins de renforcer leurs postures de sécurité et de résilience. Désormais, la souveraineté de la nation passe par la maitrise des cyberrisques et par sa capacité à prévenir et à réagir à des cyberattaques, dont toute la société peut être victime, cela comprend les infrastructures vitales à son bon fonctionnement.

Les grandes fonctions de l'Etat peuvent être perturbées par une mauvaise maitrise des enjeux du numérique et de la cybersécurité, notamment dans les domaines de la défense du pays, de la diplomatie, du maintien de l'ordre, de la sûreté publique, de la démocratie, de la protection des infrastructures critiques, de l'économie et de la place financière de la Suisse. Aujourd'hui, la performance économique de la Suisse dépend dans une large mesure du bon fonctionnement de l'écosystème numérique et de sa cybersécurité.

Certains acteurs, selon des motivations et des circonstances particulières, savent exploiter les capacités offertes par le monde Cyber pour nuire, déstabiliser, influencer, contrôler, espionner, voler, s'enrichir illégitimement, projeter du pouvoir, soutenir des actions terroristes et conflictuelles.

Protéger, prévenir et défendre des valeurs, détecter et gérer des incidents et des crises, corriger des défauts de sécurité, optimiser des mesures de sécurité et de défense afin qu'elles soient efficaces et efficientes est un exercice complexe et difficile pour lequel le partage d'information apporte un des éléments de réponse.

Le cadre de la cybersécurité s'inscrit dans un contexte de compétitivité économique et de tensions géopolitiques. En Suisse, l'échange d'information, pour produire de la stabilité économique et politique, intervient à plusieurs niveaux : celui de la société civile, des organisations privées, de la Confédération et des cantons, dans des logiques de coopération nationale et internationale. Celles-ci sont, en 2018, au cœur de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) qui repose sur une approche décentralisée basée sur la responsabilité personnelle de tous les acteurs.

Cela nécessite des dispositifs organisationnels, techniques, procéduraux et humains ainsi que des incitations pour que les propriétaires de « l'information utile » soient convaincus de participer à cette chaine du partage et puissent en récolter des avantages.

**Au niveau international**

La sécurité durable des infrastructures numériques nationales ne peut être renforcée que si les États coopèrent au niveau international et définissent conjointement les règles du jeu qui sont généralement acceptées dans le cyberespace. Dans sa stratégie de protection de la Suisse contre les cyberrisques (NCS) 2018–2022[1], le Conseil fédéral reconnaît que la Suisse doit se positionner activement sur le plan international afin de contrer les cyberrisques de manière préventive, réactive, efficace et cohérente. Le Conseil fédéral envoie ainsi un signal fort, parce qu'il reconnaît que le cyberespace a créé une nouvelle dimension de la politique étrangère de sécurité.

Les tâches de politique étrangère et de sécurité se concentrent sur l'utilisation de l'espace Cyber à des fins pacifiques. Pour cela, « l'élaboration d'un ensemble de règles pour une utilisation responsable des TIC » est primordiale. Cela est basé sur l'application du droit international, des processus de dialogue internationaux et régionaux (ONU, l'OSCE, etc.), des plates-formes internationales et régionales de dialogue sur la cybersécurité dans lesquelles la Suisse est activement impliquée. L'échange d'information entre les parties prenantes contribue à adresser des questions comme par exemple : Où sont les limites de l'utilisation du cyberespace pour la résolution des conflits ? Comment les États peuvent-ils prévenir les activités illégales menées par des acteurs non étatiques à partir de leur territoire ?

Un « Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace » a été créé par le Département fédéral des affaires étrangères afin d'institutionnaliser la participation de la Suisse au processus de dialogue et d'échange d'information à l'international[2].

[1] Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022 https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

[2] https://www.staatskalender.admin.ch/navigate.html?dn=ou=Cyber-Aussen-%20und%20-Sicherheitspolitik,ou=Abteilung%20Sicherheitspolitik,ou=Politische%20Direktion,ou=Staatssekretariat,ou=Eidg.%20Dep.%20fuer%20auswaertige%20Angelegenheiten,ou=bundesrat&localeString=Fran%E7ais

# Cinq applications du partage d'information en cybersécurité

**Sensibiliser et former**

Sensibiliser les acteurs de l'écosystème numérique aux menaces et aux risques, leur donner des pistes pour adopter des comportements responsables et des mesures de précaution, de protection et de défense, fait partie du partage d'information. Cela contribue globalement à une meilleure cybersécurité, à renforcer la résilience et à lutter contre les cybermenaces.

Des mesures d'information au public sont possibles lorsqu'il s'agit de communiquer des informations relatives à la sûreté, à la sécurité publique et à la protection de la population notamment lors de situations de gestion de crises ayant une dimension Cyber. Dans certains cas, les médias sociaux peuvent servir de plateforme d'échange d'informations notamment lorsqu'il s'agit de pouvoir interagir rapidement avec la population. Ils contribuent à la sensibilisation, la diffusion d'alertes ou de consignes de sécurité.

L'éducation des écoliers, des futurs professionnels (ingénieurs, techniciens, juristes, policiers, administrateurs, dirigeants et acteurs des secteurs public et privé), des personnes en activité ou non ainsi que des séniors, est importante pour la cybersécurité. Ainsi, l'éducation est considérée comme le premier socle du partage d'information. Elle est un levier pour contribuer à réaliser une cybersécurité par conception (« by design ») pour ce qui concerne la sécurité informatique, des réseaux de télécommunication, des systèmes d'information et des objets connectés.

**Participer à une culture de la cybersécurité**

Certaines organisations privées actives en cybersécurité partagent des informations au sein de la société, selon des modèles gratuits ou payants, de manière ponctuelle ou régulière, sous forme d'abonnement gratuits ou payants. Tous contribuent à la diffusion d'une culture de la cybersécurité participant à augmenter le seuil de connaissances des acteurs que cela soit sous la forme de lettres d'information, de rapports, de services de veilles stratégique ou opérationnelle, de veille technique ou juridique par exemple.

A ces approches s'ajoutent les actions portées notamment par le tissus associatif, les hautes écoles, les fournisseurs de solutions, le monde de l'assurance ou encore des acteurs de l'évènementiel, les médias ou les chambres de commerce. Ils organisent des rencontres, des conférences, des forums, des expositions et diffusent des supports informatifs concernant la cybersécurité. Cela contribue au partage d'information, au développement de la prise de conscience de la nécessité d'agir pour faire face aux cyberrisques, et d'autre part à élever le seuil de connaissances et de compétences permettant de construire les capacités humaines nécessaires au développement économique du pays.

## Lutter contre la cybercriminalité

En Suisse[3], le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI), financé conjointement par la Confédération et les cantons, est opérationnel depuis 2003[4] .

Le formulaire d'annonce mis à disposition des victimes pour rapporter des délits, des escroqueries, des crimes ou des contenus suspects à l'Office fédéral de la police (Fedpol) constitue un outil du partage d'information[5] et un canal de communication privilégiée pour la prise en compte des victimes, dont le nombre ne cesse de s'accroitre. Pour autant, ces plateformes de communication ne constituent pas des plateformes d'assistance aux victimes de cybermalveillance.

La Suisse dispose d'une Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)[6] qui contribue au partage d'information dans le domaine de la sécurité des systèmes d'information et de l'Internet. Cela notamment au travers de diverses documentations, lettres d'information, une présentation des cas fréquemment annoncés ou des formulaires d'annonce d'incidents par exemple. La mission de MELANI ne peut se réaliser sans un échange d'information entre diverses entités privées et publiques mais aussi avec des partenaires privilégiés.

Lutter efficacement contre la cybercriminalité passe par une approche préventive qui consiste à rendre le cyberespace moins favorable à l'expression de la criminalité et à réduire les opportunités criminelles. Par conséquent, il faut élever le seuil de difficulté de réalisation des cyberattaques (augmenter les coûts en termes de compétences et de ressources pour le malveillant et diminuer les profits attendus) et accroître les risques pris par les criminels d'être identifiés, localisés, arrêtés et poursuivis[7]. Toutes ces mesures ne peuvent être conçues et mises en œuvre que s'il existe, à la base, un partage d'information efficace entre tous les acteurs de l'écosystème numérique.

## Produire de la cybersécurité

Les normes internationales issues de l'ISO[8] (Organisation Internationale de Standardisation) ou de l'UIT[9] (Union Internationale des Télécommunications) contribuent au développement des capacités en matière de cybersécurité. Elles sont à considérer comme des mécanismes et des leviers du partage d'information, comme par exemple la famille des normes ISO/IEC 27000 qui traite des différents domaines du management de la sécurité des systèmes d'information.

Le secteur privé et associatif est également un vecteur de diffusion de recommandations et de bonnes pratiques, cela peut avoir éventuellement une envergure sectorielle, nationale ou internationale, concerner des domaines techniques ou managériaux. Qu'il s'agisse des normes ou de référentiels issus du secteur privé, ces documents sont conçus généralement sur la base d'une participation de divers représentants du monde professionnel et de la société civile. Cela a nécessité la mise en place préalable d'un mécanisme de consultation, de collecte, de transmission de l'information selon un format adapté, d'échange de l'information et de restitution des résultats du partage.

**Maitriser les vulnérabilités et les incidents de sécurité**

Tout élément constitutif d'un système d'information peut comporter des vulnérabilités et constituer des failles exploitables pour mettre à mal sa sécurité. De manière régulière, de nouvelles failles de sécurité et des vulnérabilités sont annoncées et partagées afin de pouvoir les corriger.

L'organisation privée américaine à but non lucratif MITRE[10], active depuis 1958 en recherche et développement de technologies avancées liées à des domaines stratégiques et vitaux (défense, sécurité, cyberespace, etc.), tient à jour depuis 1999, le registre des vulnérabilités de sécurité – CVE (Common Vulnerabilities and Exposures)[11]. L'US-CERTs (United States Computer Emergency Response Team, National Cyber Awareness System – Homeland Security) en fait une synthèse hebdomadaire, les classifie en quatre catégories (haute, moyenne, faible et en niveau de sévérité non encore assigné), les décrit et identifie le correctif de sécurité (patch) à appliquer. La majorité des pays possède des entités de type CERT (Computer Emergency Response Team), parfois dénommés CSIRT pour « Computer Security Incident Response Team »[12]. Les CERTs peuvent être privés ou publics et dédiés à des secteurs d'activités particuliers (académique, militaire, administration publique, etc.). Organisés en réseau, ils collaborent au partage de certaines informations selon des règles, des rôles, des responsabilités, des canaux et des formats de communication préalablement définis.

**Un centre de partage et d'analyse d'information (ISAC)** répond généralement au besoin de pouvoir faire collaborer des acteurs privés et publics pour favoriser le partage d'information et celui des bonnes pratiques, via une entité de confiance (figure 2). Une collaboration efficace des secteurs privé et public, qui détiennent une partie de l'information utile (incidents, menaces, vulnérabilités, mesures de sécurité, de gestion des incidents, métriques, tendances, etc.) est nécessaire pour réduire les impacts des cyberrisques, dans le monde virtuel ou physique et pour assurer une meilleure anticipation des menaces.

---

[3] https://www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/internet/lutte-contre-la-cybercriminalite.html

[4] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-23881.html.

[5] https://www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/cybercrime/meldeformular.html

[6] https://www.melani.admin.ch/melani/fr/home.html

[7] S. Ghernaouti, « La cybercriminalité, les nouvelles armes de pouvoir ». Le savoir suisse, PPUR 2017.

[8] https://www.iso.org/fr/home.html

[9] https://www.itu.int/fr/Pages/default.aspx

[10] https://www.mitre.org/

[11] https://cve.mitre.org/

[12] CERT est une marque déposée aux Etats-Unis par l'Université Carnégie-Mellon. L'usage de ce nom est soumis à autorisation préalable, ce qui n'est pas le cas pour le terme CSIRT.

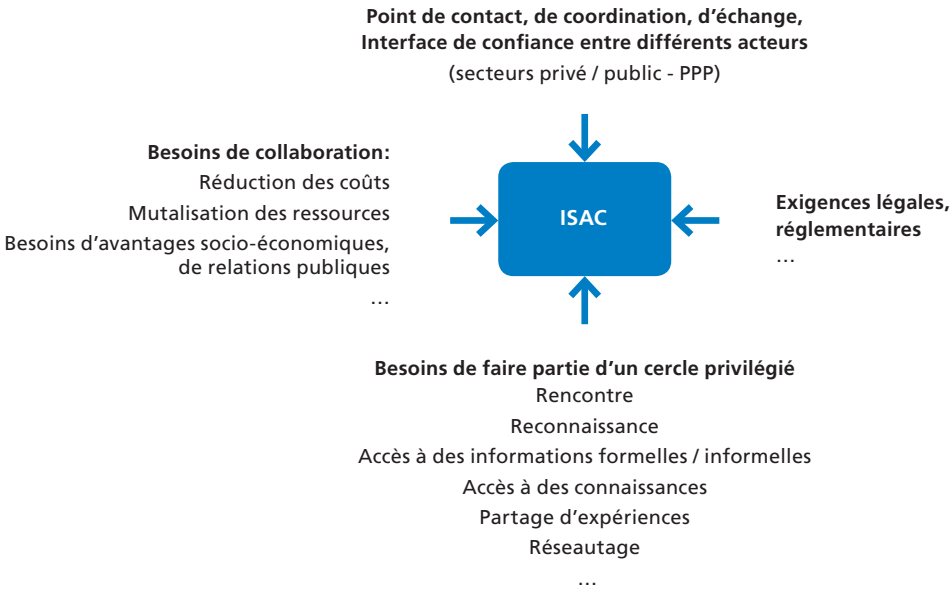


**Figure 2**
Exemples de justifications pour la création d'un ISAC (Information Sharing & Analysis Center).

Il peut exister des ISACs sectoriels dans les domaines de la finance, de l'énergie, de l'aviation, du transport ou encore de la santé. Il y a partage d'informations utiles lorsque la temporalité, la nature de l'information, l'analyse et les actions de sécurité qui en d'écoulent sont adaptées aux besoins de sécurité à satisfaire.

De manière analogue aux CERT et CSIRT, la plus-value d'un ISAC réside dans sa capacité à collecter, traiter et restituer de l'information utile au renforcement de la sécurité, notamment en termes de connaissance, de détection et de réponse aux incidents. Ces processus d'amélioration de la sécurité peuvent être plus ou moins efficaces en fonction de l'origine, de la pertinence, de la rapidité de la collecte et du traitement des données. Du fait de la couverture mondiale des cyberattaques et de l'interconnexion des cibles, une coopération des ISACs est nécessaire pour obtenir un bon niveau de réactivité et faire face aux cyberattaques qui sont transnationales et transsectorielles. Cela permet d'optimiser les démarches d'identification des victimes, des vecteurs de compromission et de propagation, de la finalité des attaques et d'adaptation des mesures de protection et de défense. Une architecture en réseaux des ISACs contribue à constituer un centre de vigilance global pour la sécurité des infrastructures numériques. Cela peut permettre par exemple des alertes précoces, pour les pays et systèmes éloignés du premier point d'impact des cyberattaques épidémiques et donc une meilleure réactivité. Faire face à des cyberépidémies, à la dimension massive de certaines cyberattaques, comme celles par exemple de Wannacry et de NotPetya survenues en 2017, pouvoir les éradiquer au plus vite tout en étant en mesure de limiter la propagation de codes malveillants, demandent une organisation et une réactivité rapide. Les ISACs peuvent répondre à ce besoin à condition qu'ils soient bien conçus, gérés, mis en œuvre et utilisés. L'Agence Européenne chargée de la sécurité des réseaux et de l'information (ENISA) considère la collaboration entre les secteurs privés et publics (Public Private Partnerships (PPP)) comme un enjeu majeur de la mise opérationnelle d'un ISAC[13].

[13] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

# Conclusion et recommandations

**Favoriser une démarche de partage d'information**

Le problème du partage est avant tout lié à la conviction des acteurs qui détiennent tout ou partie de l'information de vouloir la partager avec d'autres, y compris avec des concurrents potentiels. Les gains attendus du partage doivent être proportionnels aux coûts directs et indirects occasionnés. S'il s'agit de partager de l'information à forte valeur ajoutée (et non de répéter des informations largement diffusées et accessibles par divers canaux), il est nécessaire de motiver les participants à jouer un jeu collectif avec des incitations et des récompenses et éventuellement résoudre des questions de conflits d'intérêt. Ainsi est-il nécessaire non seulement de sensibiliser et de convaincre les acteurs de l'intérêt de partager des informations, mais aussi de démontrer la plus-value du partage par des gains tangibles en matière de renforcement de leurs postures de cybersécurité et de cyberrésilience (avantages en termes de performances mais aussi de qualité, de coût, de confort, de connaissance, d'influence ou de réputation par exemple).

**Convaincre ou contraindre**

La tendance de vouloir résoudre des problèmes de cybersécurité par des logiciels d'intelligence artificielle développés à partir de la collecte massive de données (big data, deep learning, etc.) n'incitent pas forcément, les acteurs privés à partager leurs informations. Ces dernières peuvent servir à renforcer la posture sécuritaire de la collectivité, mais aussi à développer une offre commerciale. Ce qui procure ou permet de maintenir un avantage concurrentiel aux acteurs qui savent exploiter la bonne information au bon moment. En effet, les données sur les incidents compromettant la sécurité doivent être collectées, enregistrées, corrélées avec celles relatives aux incidents préalablement survenus et analysées afin d'enrichir la base de connaissance relative aux facteurs d'insécurité (incidents, vulnérabilités, attaques, concept et termes généralement identifiés avec la notion d'intelligence des cyberattaques). Cela permet d'adapter les solutions de sécurité et d'améliorer les architectures de sécurité en conséquence.

A défaut de pouvoir convaincre pour une démarche volontaire du partage de l'information, il est parfois nécessaire de contraindre juridiquement des acteurs à communiquer un certain type d'information (obligation légale à annoncer les cyberattaques par exemple). Pour cela, un cadre légal adapté et applicable ainsi qu'une structure organisationnelle doivent exister.

**Solidarité et réciprocité**

Partager quelque chose avec quelqu'un, c'est donner à un tiers une part de ce que l'on possède, de ce que l'on acquiert, de ce que l'on reçoit. C'est mettre en commun, mais c'est aussi prendre part à quelque chose en même temps que d'autres, c'est alors participer de manière responsable. Cela suppose une solidarité entre acteurs, une certaine réciprocité, du respect et de la confiance. Il s'agit de développer et de réaliser une intelligence informationnelle collective soutenue par une politique de sécurité adaptée. Le tableau de la figure 3 présente une synthèse des recommandations pour la création d'un centre de partage d'information en cybersécurité.

## Recommandations d'ordre stratégique

- Identifier les acteurs, finalités et bénéfices du partage d'information à court, moyen et long terme (fournisseurs d'infrastructures, de services, groupes d'utilisateurs, mutualisation des ressources, ...Cf. figure2).
- Spécifier les moyens d'évaluation des gains attendus, définir les indicateurs d'évaluation de la performance (indicateurs de performance et de pilotage).
- Définir le périmètre du partage (intra organisation, inter organisations, organisations sectorielles, niveau national, international).
- Effectuer les partenariats à mettre en place en définissant les mesures qui permettent de les faire vivre, tout en tenant compte des contraintes légales, réglementaires et budgétaires.
- Identifier et adapter les structures organisationnelles existantes qui peuvent contribuer au partage d'information ou mettre en place de nouvelles structures et infrastructures informatiques pour un partage d'information efficace et efficient.
- Déterminer à qui appartient la plateforme d'échange et de partage, comment elle est sécurisée, exploitée et maintenue.
- Définir les responsabilités, les droits et devoirs de chaque partie prenante.
- Accompagner la démarche et l'infrastructure du partage par des mesures stratégiques et opérationnelles de sécurité et de défense.

**Figure 3**
Synthèse des recommandations pour la création d'un centre de partage d'information en cybersécurité

## Recommandations d'ordre technologique

- Identifier le type d'information à partager (nature, origine, format, qualité, fiabilité, véracité, durée de vie).
- Définir la manière dont l'information est collectée, stockée, traitée, présentée, restituée, sécurisée.
- Définir l'infrastructure informatique nécessaire à la plateforme d'échange (matériel, logiciel, réseaux de télécommunication).

## Recommandations d'ordre humain, managérial et économique

- Mettre en place les compétences nécessaires (capacités humaines dans les domaine du droit, de la gestion, de l'organisation, de la communication, de la technique, de l'analyse et de la visualisation des données, ...).
- Allouer les moyens et les ressources nécessaires (capacités financières, organisationnelles, procédurales et techniques).
- Identifier et communiquer les incitations qui favorisent le partage d'information (bénéfices, récompenses, ...).

# Résumé

Cette fiche d'information apporte un éclairage sur les pratiques d'échange d'information dans le domaine de la cybersécurité. Elle résume et analyse le contexte, les besoins, les contraintes du partage d'information pour produire de la sécurité, de la résilience et pour lutter contre la cybercriminalité. Elle identifie les différents types d'information partageable ainsi que les principaux vecteurs de support au partage d'information en Suisse et au niveau international. Elle propose cinq applications du partage d'information en cybersécurité en insistant sur les avantages et inconvénients d'un centre de partage et d'analyse d'information (ISAC) ainsi que sur les facteurs clés de succès d'un tel dispositif.

Des recommandations de haut niveau sont proposées en conclusion pour la mise en place d'une d'une plateforme de partage et d'analyse de l'information.

**Impressum**

Auteurs : Solange Ghernaouti, Laura Crespo,
Bastien Wanner – Université de Lausanne,
Swiss Cybersecurity Advisory & Research Group
(www.scarg.org)

satw it's all about technology

Académie suisse des sciences techniques SATW
St. Annagasse 18 | 8001 Zurich | 044 226 50 11 | info@satw.ch | www.satw.ch