JURA CH RÉPUBLIQUE ET CANTON DU JURA

STRATÉGIE DE CYBERSÉCURITÉ DE LA RÉPUBLIQUE ET CANTON DU JURA (SCJU)

31 octobre 2023

INTRODUCTION

La sécurité et la prospérité de tous les Jurassiens sont au cœur des préoccupations du Gouvernement et de la République et Canton du Jura. Comme partout ailleurs dans le monde, le Jura vit une profonde et rapide mutation numérique, une dimension désormais essentielle pour l'État, pour l'ensemble des citoyens et tout le tissu économique. En 2018, le Gouvernement en a fait l'une de ses priorités, réaffirmée dans le programme de législature 2021–2025. Il a ainsi fixé l'année 2026 comme objectif pour que la population s'adresse à l'administration cantonale principalement de manière numérique. Un guichet virtuel, interface avec la population et les entreprises, est d'ores et déjà en fonction et ses prestations se développent sans cesse pour renforcer l'accessibilité du service public et augmenter l'efficacité et l'efficience des administrations publiques.

Tout progrès technologique comporte des aspects de sécurité et la numérisation ne fait pas exception. Les institutions publiques, les entreprises et les individus sont tous confrontés à des risques qu'il s'agit d'identifier à temps et dont il s'agit de se prémunir. Trop souvent encore considérées comme quelque chose « qui n'arrive qu'aux autres », les cyberattaques sont désormais un fléau qui touche tout le monde et peut entraîner de lourdes conséquences. Les cyberrisques sont déjà considérés avec sérieux par le Canton du Jura et nombre d'organisations et d'entreprises, mais l'analyse montre que la maturité générale en matière de cybersécurité en Suisse est encore insuffisante.

Face à ce constat, la Confédération a pris aussi d'importantes mesures législatives qu'il convient également de prendre en considération dans le Canton du Jura. En raison de la nature dynamique et complexe des cyberrisques et du cadre pour les maîtriser, le Gouvernement – en plus de ses responsabilités constitutionnelles pour garantir ses prestations à la population – ne saurait laisser les communes, les entreprises et les citoyens seuls face à ces défis. En conséquence, il a décidé de définir une **stratégie de cybersécurité pour l'ensemble du canton** afin que s'établisse un continuum cohérent, de la Confédération jusqu'au citoyen.

Le Gouvernement est conscient des efforts et du temps nécessaire pour que cette stratégie déploie ses effets et que la cybersécurité devienne un réflexe et une culture chez chaque individu. Dans ce but, la stratégie établit d'abord un **suivi de situation** et une **gouvernance** qui, en soutien et en étroite collaboration avec toutes les parties prenantes, permettra de maximaliser l'effet de l'ensemble des mesures qui reposent sur **cinq piliers** :

- l'identification des intérêts et des objets à protéger;
- leur protection;
- la détection des incidents;
- la réponse à ceux-ci;
- le rétablissement après un incident.

Les progrès seront régulièrement évalués et le dispositif adapté en conséquence.

Par cette stratégie, le Gouvernement entend créer un **Jura numérique sûr, exemplaire, résilient, souverain et proactif**. Une stratégie pour tous et par tous, parce que la sécurité est l'affaire de chacune et de chacun !

La sécurité est l'affaire de chacune et de chacun !

TABLE DES MATIÈRES

STRATÉGIE EN BREF

La Stratégie de cybersécurité de la République et Canton du Jura (SCJU) s'inscrit en soutien de la volonté du Gouvernement de promouvoir un Jura qui fait un plein usage du monde numérique. Un Jura innovant, mais sûr. La mutation numérique de la société comprend en effet de nombreux défis qu'il s'agit autant que possible de comprendre et de maîtriser.

La SCJU définit un cadre pour **augmenter la confiance, la résilience et la souveraineté numériques de l'ensemble de la société jurassienne face aux défis de la numérisation, en particulier de sa sécurité**. Elle n'a pas pour but d'imposer de nouvelles obligations, mais d'accompagner les Jurassiennes et Jurassiens dans la mise en œuvre des exigences déjà existantes. Avant tout, la SCJU pose les bases pour une **collaboration de tous les acteurs concernés**, du Gouvernement aux citoyennes et citoyens, en passant par les communes et les entreprises. Elle les invite à l'échange d'informations et à la mutualisation des moyens et des actions chaque fois que cela est possible et produit un gain objectif.

UN JURA NUMÉRIQUE SÛR

EXEMPLAIRE, RÉSILIENT, SOUVERAIN ET PROACTIF

Pour atteindre cette vision, la SCJU définit **5 + 1 piliers** :

IDENTIFICATION
Chaque entité[1] doit cartographier son cyberespace et définir ce qui doit être protégé, donc comprendre ses risques.

PROTECTION
Il s'agit de mettre en place des mesures techniques et organisationnelles selon les règles de l'art et proportionnées.

DÉTECTION
Rester vigilant, tester sa sécurité, identifier et annoncer les anomalies, etc., afin d'agir le plus en amont possible.

RÉPONSE
Être préparé afin que chaque entité intervienne rapidement et efficacement pour maîtriser / minimiser les situations de crise.

RÉTABLISSEMENT
Revenir le plus rapidement possible à une situation « normale » et apprendre de la crise.

SUIVI DE SITUATION ET GOUVERNANCE
Il s'agit d'avoir la vue d'ensemble et de définir les rôles et responsabilités de chaque acteur.

[1] Ce terme comprend les services de l'État, les communes, les institutions paraétatiques, les prestataires d'importance, les entreprises privées et le grand public.

La SCJU considère six groupes de destinataires et leur attribue leurs rôles et responsabilités ou leur fait des recommandations.

1. **LES AUTORITÉS CANTONALES**
2. **LES ÉTABLISSEMENTS DE DROIT PUBLIC**
3. **LES COMMUNES**
4. **LES INSTITUTIONS PARAÉTATIQUES**
5. **LES PRESTATAIRES D'IMPORTANCE**
6. **LES TIERS ET LE GRAND PUBLIC**

La mise en œuvre de la SCJU d'ici 2026 sera confiée au **Service de l'informatique** (SDI) du Département de l'environnement (DEN). Le SDI mettra à cet effet sur pied plusieurs instances de **pilotage**. Il sera par ailleurs établi une « cellule de soutien cybersécurité » qui sera chargée d'accompagner les communes et les institutions publiques et paraétatiques. Le SDI sera également chargé de mettre en place divers **outils et services subsidiaires** pour aider les entreprises et la population.

Accompagner les communes, les institutions publiques et paraétatiques.

PORTÉE DU DOCUMENT

OBJECTIF

La SCJU a pour but d'augmenter la confiance, la résilience et la souveraineté numériques de l'ensemble de la société jurassienne face aux défis de la numérisation, en particulier de sa sécurité.

PUBLIC CIBLE

Cette stratégie s'adresse d'abord aux autorités cantonales, aux établissements de droit public, aux communes et aux institutions paraétatiques. Toutes ces entités doivent garantir que les données dont elles ont la charge et les systèmes qui les traitent sont protégés conformément aux bases légales et de manière à pallier les risques identifiés, dans l'esprit de la responsabilité collective et individuelle, ainsi que dans le respect des tâches, rôles et compétences de chacun ainsi que de l'autonomie des communes. La stratégie établit également un continuum avec les prestataires d'importance, les tiers, le grand public et les milieux économiques.

ÉVOLUTION DANS LE TEMPS

Les cyberrisques, les services et les technologies évoluent rapidement. Pour s'adapter constamment aux changements, le Gouvernement a donc décidé de mettre en place une structure agile supportée par trois instruments : un comité de pilotage pour les aspects stratégiques et le soutien politique, un groupe de travail pour les projets et questions techniques et une cellule de soutien pour appuyer directement les institutions cantonales, communales et de droit public. Le succès de la stratégie sera suivi en continu au moyen de dix indicateurs de succès. Lors de la mise en place du prochain plan de législature (fin 2025), la SCJU sera réexaminée afin de déterminer s'il y a lieu de la mettre à jour.

STRUCTURE DU DOCUMENT

Cette stratégie de cybersécurité comprend quatre chapitres :

- le premier chapitre expose les défis et ainsi les raisons justifiant l'établissement d'une stratégie cantonale;
- le second chapitre présente l'état de la cybersécurité en Suisse et dans le Canton du Jura ainsi que les dix grandes attentes exprimées par les participants lors de l'élaboration de la stratégie;
- le troisième chapitre présente la stratégie elle-même, la vision du Gouvernement, la répartition des rôles et les premières mesures concrètes;
- enfin, le quatrième chapitre expose la manière dont la stratégie sera mise en œuvre.

Augmenter la confiance, la résilience et la souveraineté numériques de l'ensemble de la société jurassienne.

1. DÉFIS DU NUMÉRIQUE

1.1 MUTATION DE LA SOCIÉTÉ

Durant les quarante dernières années, les technologies de l'information et de la communication (TIC) ont profondément transformé la société. Précédemment considérées comme de simples commodités, les TIC sont désormais à la racine d'une mutation de la société qui comprend trois grandes étapes. Les TIC ont tout d'abord permis l'**amélioration** des processus de travail. Ensuite est venue la **mise en réseau** des objets et entités. Finalement, depuis une dizaine d'années, nous sommes entrés dans l'**ère des données**. La dépendance de la société aux TIC est désormais globale et irréversible. Plus aucune activité, que ce soit dans la santé, l'éducation, les transports, la défense, etc., n'est possible sans cette couche technologique et les prestations sous-jacentes qui caractérisent le cyberespace[2]. Ces trois étapes sont par ailleurs dépendantes de l'électricité de façon critique ainsi que d'une multitude de facettes (personnel, formation, bases légales, évolution technologique, infrastructures, ressources naturelles, finances, etc.) dont il faut tenir compte dans une approche systémique pour établir une stratégie pérenne.

1.2 MENACES ET DANGERS DANS L'ESPACE NUMÉRIQUE

Maîtriser notre environnement numérique est désormais un enjeu stratégique qui exige de disposer d'un cadre clair et évolutif. Le cyberespace fait partie de défis caractérisés par leur volatilité, incertitude, complexité et ambiguïté. Certaines de ses facettes sont déjà des dangers ou des menaces, alors que d'autres le deviendront si on ne les traite pas, d'où l'importance d'en comprendre et d'en anticiper le développement.

En raison de leur complexité et de leur ubiquité, les TIC comportent malheureusement de nombreuses vulnérabilités qui peuvent être exploitées ou détournées par des personnes et des organisations malveillantes. Beaucoup de vulnérabilités sont le fruit du hasard, mais nombreuses aussi sont celles qui découlent de la négligence de leurs concepteurs, fabricants et exploitants, certaines étant même volontaires, à l'insu de tous.

[2] Espace (d'opération) dans lequel des données peuvent être saisies, enregistrées, transmises, traitées, classées, codées, visualisées et converties par voie électronique en actions physiques et informationnelles.

Avec les premiers ordinateurs sont apparus divers codes malveillants (vers, virus, etc.) qui ont initialement nécessité la mise en place d'une **sécurité informatique** pour protéger les appareils et terminaux. Avec le développement de la connectivité, il a fallu mettre en place une **sécurité des réseaux**. Avec l'ère des données et des dépendances systémiques aux TIC, ces dernières années ont mené à l'avènement de l'ère de la **cybersécurité** au sens large. Ainsi, il est désormais nécessaire de disposer de politiques de sécurité pour la maîtrise des cyberrisques. Les considérants et métiers dans ce domaine ne sont ainsi plus uniquement d'ordre technique; de nombreuses disciplines non techniques (droit, gestion des risques, gestion de crise, formation, renseignement, etc.) font désormais partie intégrante du paysage de la cybersécurité.

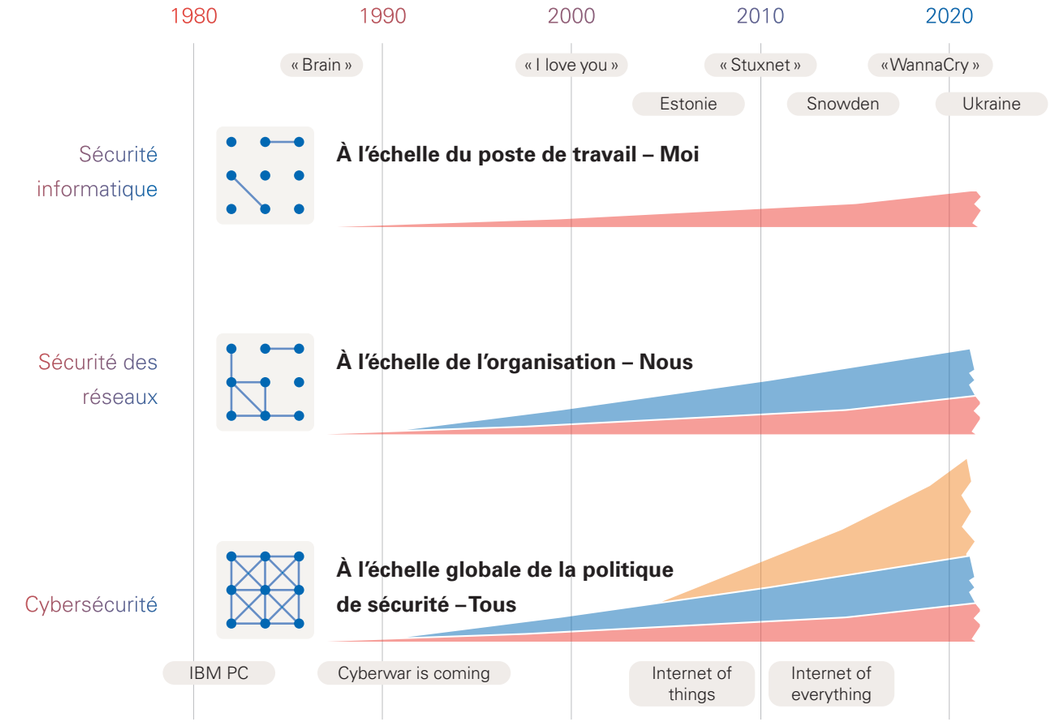


Figure 1 – L'évolution des besoins en sécurité dans le cyberespace (source digiVolution)

Du côté des acteurs malveillants, on retrouve les mêmes étapes de développement. Sont tout d'abord survenus les **hackers** animés par le jeu et le défi; ils ont un peu perdu en importance, mais ces acteurs savent se mobiliser rapidement pour une cause spécifique au sein de collectifs, comme lors des événements en lien avec Charlie Hebdo ou la guerre en Ukraine. Sont ensuite apparus les **cybercriminels** ou **pirates** attirés par l'appât du gain. Ces acteurs ont parfaitement compris la valeur des données, personnelles notamment, et l'usage qu'ils peuvent en faire. Travaillant en bandes organisées professionnelles à l'échelle internationale et dans un but d'enrichissement, ces acteurs malfaisants font des ravages.

Diverses évaluations montrent que les conséquences de la seule cybercriminalité représenteraient déjà plusieurs points de PIB (3,8% en Allemagne en 2022 selon Bitkom[3]) et la plupart des analystes s'attendent à un triplement dans les cinq à six prochaines années. Nous appellerons **cybersoldats** la troisième catégorie à s'être développée à partir des services de renseignement et des forces armées qui considèrent désormais le cyberespace comme un espace de conflictualité à part entière, au même titre que la terre, la mer, l'espace, l'espace électromagnétique et l'information. Le cyberespace devient ainsi toujours plus un lieu de guerre exploité par les États pour perturber, espionner et détruire les moyens de leurs adversaires.

[3] https://www.bitkom.org/Presse/Presseinformation/Organisierte-Kriminalitaet-greift-verstaerkt-deutsche-Wirtschaft-an#_

Pour les responsables de la cybersécurité du Canton, des communes ou des entreprises, cette distinction entre les acteurs et leurs intentions – criminelles, d'espionnage, de sabotage, de subversion, dans le cadre de conflits – importe peu.

Leur mission est d'assurer au quotidien que les données et les processus dont la population et l'économie dépendent soient protégés et ainsi que soit empêchée toute atteinte à leur confidentialité, intégrité, disponibilité et traçabilité.

1.3 FACTEUR HUMAIN

Malgré les progrès technologiques fulgurants de ces dernières années, l'humain reste au centre de l'écosystème cyber, notamment en tant que cible privilégiée des acteurs malveillants qui profitent de ses faiblesses techniques et psychologiques. Ainsi, une importante partie des attaques découle d'astuces sans cesse renouvelées d'ingénierie sociale. La rapide évolution technologique nécessite aussi une adaptation continue des compétences des personnes et des organisations. La formation continue – que peu d'entreprises et d'institutions parviennent à assurer seules – est ainsi un investissement central pour éviter la formation des décrochages et des fossés dans et entre les catégories de populations en raison de différences d'âge, de formation, d'origine, de culture, etc. Cette mesure est d'autant plus importante qu'elle s'inscrit dans un contexte de pénurie croissante de personnel spécialisé dans les TIC qui pèse toujours plus sur la capacité des entités, publiques comme privées, à assurer leurs opérations, leur sécurité et même leurs projets et développements.

Usagers, décideurs, techniciens, etc., sont une clé essentielle de l'équation et la cybersécurité est une tâche de chacun, au travail comme dans le cadre privé. À l'image de la sécurité sanitaire, qui n'est pas le seul fait des médecins, ou de la sécurité routière, qui n'est pas uniquement celui de la police, la cybersécurité n'est pas l'apanage des seuls informaticiens et doit se construire dans la société toute entière.

1.4 ÉVOLUTIONS ATTENDUES

Les TIC sont un moteur essentiel et hautement dynamique du développement de la société et il faut s'attendre à voir sans cesse émerger des évolutions disruptives, comme récemment avec les nouveaux modèles d'intelligence artificielle tels que ChatGPT.

Les prochaines années seront notamment influencées par la croissance des conflictualités et les progrès fulgurants des technologies et services existants tels que les objets connectés, l'intelligence artificielle, l'informatique quantique, les technologies spatiales ou l'informatique en nuage et il s'agira d'identifier et de suivre constamment les risques liés.

Le défi majeur pour toute entité sera donc, surtout avec des ressources limitées, d'identifier aussi tôt que possible ces changements, ainsi que leurs conséquences, et de prendre à temps les mesures requises pour éviter ou au moins réduire les risques ou de tirer avantage des opportunités. L'anticipation devient donc un élément clé qui dépasse les seules considérations techniques. Il est ainsi crucial – tant en Suisse qu'au niveau international – de suivre aussi les évolutions sociales, juridiques, financières, environnementales, énergétiques, matérielles, en matière de personnel et de formation, de chaînes d'approvisionnement, de télécommunications, etc.

2. ÉTAT DE LA CYBERSÉCURITÉ EN SUISSE

2.1 ÉCHELON FÉDÉRAL

Les cyberrisques ont une courte histoire et ils évoluent rapidement. Les facteurs qui les influencent sont nombreux, technologiques, criminels, opportunistes, géopolitiques, etc. En Suisse, ce sujet s'est imposé pour la première fois lors de l'exercice de conduite stratégique de 1997 sur le thème de la «Vulnérabilité dans notre société d'information». En 2003 a été créée la *Centrale d'enregistrement et d'analyse pour la sûreté de l'information* MELANI. En 2012, la Confédération a publié la première *Stratégie nationale de protection de la Suisse contre les cyberrisques* (SNPC), révisée en 2018. La troisième édition, nommée *Cyberstratégie nationale* (CSN) a été rendue publique le 13 avril 2023. Ces développements ont permis d'affiner et de renforcer graduellement la répartition des tâches et les responsabilités entre acteurs. La cybersécurité reste cependant une discipline jeune, aux ressources limitées et souvent en décalage avec les enjeux. Son organisation en Suisse comprend trois domaines[4]:

- la **cybersécurité**: ensemble des mesures visant à prévenir et à gérer les incidents, à améliorer la résilience face aux cyberrisques ainsi qu'à développer la coopération internationale à cet effet;
- la **cyberdéfense**: ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la défense nationale, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et de développer ses capacités et compétences afin qu'elle puisse apporter un appui subsidiaire aux autorités civiles; ce domaine inclut des mesures pour identifier les menaces et les attaquants et pour entraver leurs actions;
- la **poursuite pénale de la cybercriminalité**: ensemble des mesures prises par la police et les ministères publics de la Confédération et des cantons pour lutter contre la cybercriminalité.

[4] Voir l'article 6 de https://www.fedlex.admin.ch/eli/cc/2020/416/fr

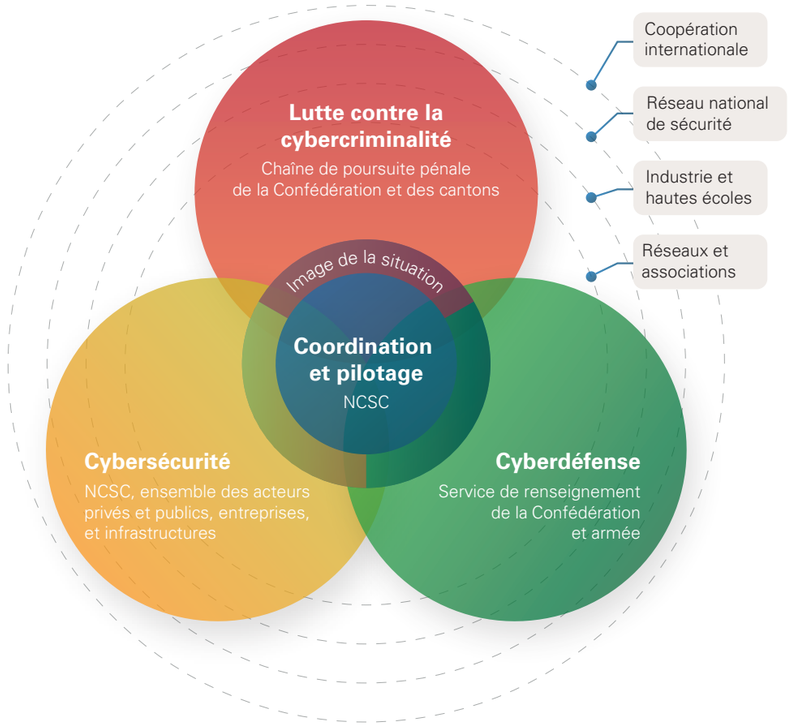


Figure 2 – Dispositif national de cybersécurité de la Suisse

Au centre de ce dispositif, pour en assurer la cohérence, la Suisse dispose depuis 2020 du Centre national de cybersécurité (NCSC: National Cyber Security Center) qui deviendra au 1er janvier 2024 un office fédéral rattaché au Département fédéral de la défense et de la protection de la population (DDPS). Comme illustré à la figure 2, ce dispositif ne saurait fonctionner sans les réseaux officiels, économiques, académiques et associatifs, tant nationaux qu'internationaux[5].

Avec la nouvelle CSN, le Conseil fédéral donne une nouvelle impulsion et une vision renouvelée:

« La Suisse saisit les chances offertes par la transformation numérique et engage des mesures de protection pour réduire les cybermenaces et leurs conséquences. Elle compte parmi les leaders mondiaux en matière de connaissances, de formation et d'innovation dans le domaine de la cybersécurité. Dans le contexte des cybermenaces, la capacité d'action et l'intégrité de sa population, de son économie, de ses autorités et des organisations internationales basées sur son territoire sont garanties. »

[5] La Suisse participe par exemple au CCDCoE, le Centre d'excellence de cyberdéfense de l'OTAN à Tallinn et, bien que perfectible, l'échange de renseignements entre les agences est établi.

La nouvelle stratégie nationale définit cinq objectifs stratégiques et leurs **M**esures :

RESPONSABILISATION

- **M1** : Formation, recherche et innovation en matière de cybersécurité;
- **M2** : Sensibilisation;
- **M3** : État de la menace;
- **M4** : Analyse des tendances, des risques et des dépendances.

FIABILITÉ ET DISPONIBILITÉ DE L'INFRASTRUCTURE ET DES SERVICES NUMÉRIQUES

- **M5** : Identifier les vulnérabilités et y remédier;
- **M6** : Résilience, normalisation et régulation;
- **M7** : Accroître la collaboration entre les autorités.

DÉTECTION, PRÉVENTION, GESTION ET DÉFENSE EFFICACES CONTRE LES CYBERATTAQUES

- **M8** : Gestion des incidents;
- **M9** : Attribution;
- **M10** : Gestion de crise;
- **M11** : Cyberdéfense.

LUTTE ET POURSUITES PÉNALES EFFICACES CONTRE LA CYBERCRIMINALITÉ

- **M12** : Collaboration accrue des autorités de poursuite pénale;
- **M13** : Vue d'ensemble des cas;
- **M14** : Formation des autorités de poursuite pénale.

RÔLE DE PREMIER PLAN DANS LA COOPÉRATION INTERNATIONALE

- **M15** : Renforcement de la Genève internationale dans le domaine numérique;
- **M16** : Règles internationales dans le cyberespace;
- **M17** : Coopération bilatérale avec des partenaires stratégiques et des centres de compétence internationaux.

En matière de **droit fédéral**, la présente stratégie devra prendre tout particulièrement en compte les textes de loi suivants :

- **Loi sur la protection des données (LPD[6]) :** établit une première compatibilité de la Suisse avec le Règlement général sur la protection des données RGPD de l'Union européenne.
- **Loi sur la sécurité de l'information (LSI) :** pose nouvellement aux opérateurs d'infrastructures critiques notamment l'obligation d'annoncer les cyberincidents.

2.2 ÉCHELON CANTONAL

La 1re version de la SNPC se focalisait sur la Confédération et ce n'est que dans sa révision pour la période 2018–2022 qu'une annexe a chargé les cantons de 4 objectifs principaux :

- élever le niveau de compétence dans leurs administrations;
- contribuer au partage de connaissance sur les cybermenaces ;
- améliorer la gestion de leur résilience informatique;
- contribuer à l'institutionnalisation de l'échange d'expérience pour la création de bases communes.

Un tour d'horizon montre que les mesures en place dans les cantons sont hétérogènes et sont le reflet de leurs moyens et du dynamisme variable de leurs responsables. La nouvelle CSN a été adoptée par le Conseil fédéral lors de sa séance du 5 avril 2023 et par les cantons lors de l'assemblée plénière de la Conférence des directrices et directeurs des départements cantonaux de justice et police du 13 avril 2023; elle est donc pleinement applicable aux cantons.

[6] Entrée en vigueur le 1er septembre 2023.

2.3 SITUATION DANS LE JURA

2.3.1 INSTITUTIONS

Bien que vingtième canton en taille nationale, le Jura est souvent pris en exemple pour l'ingéniosité et l'agilité de ses solutions innovantes qui, en plus, préservent ses finances publiques. Il dispose d'un *Schéma directeur des systèmes d'information* qui détermine les orientations stratégiques pour le développement de la société de l'information jurassienne de demain, avec pour mission d'accroître l'efficacité et l'efficience des institutions étatiques et paraétatiques dans leur fonctionnement et leurs relations avec l'extérieur, en adéquation avec la stratégie de l'administration.

Comme interface numérique sécurisée avec la population et les entreprises, le Jura dispose d'un guichet virtuel. Les modifications de la loi de 2012 qui l'encadre ont été approuvées par le Parlement le 6 septembre 2023. Ladite loi clarifie la collaboration entre le Canton et les communes avec l'objectif que celles-ci fournissent l'essentiel de leurs prestations via ce guichet virtuel.

Cette importante étape a aussi été pensée dans un contexte général des enjeux du numérique comme l'exploitation mutualisée de solutions informatiques, le renforcement de la cybersécurité ou le développement du haut débit dans le canton. La présente stratégie s'inscrit donc comme l'un des piliers pour atteindre les objectifs numériques de la législature.

S'agissant des bases légales, plusieurs lois et conventions significatives sont à considérer en lien avec la présente stratégie. En plus de la loi concernant le guichet virtuel sécurisé (LGVS)[7], on retiendra surtout la **Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâte**l (CPDT-JUNE)[8].

Dans le Canton du Jura, la sécurité fait partie intégrante des services numériques et son importance augmente sans cesse, conformément aux buts du Gouvernement. L'analyse montre toutefois la nécessité d'établir un continuum de sécurité entre l'État et les acteurs non soumis au droit public, notamment les entreprises et les citoyens.

Le Canton du Jura, un exemple pour l'ingéniosité et l'agilité de ses solutions innovantes.

[7] https://rsju.jura.ch/fr/viewdocument.html?idn=20015&id=37687

[8] https://www.lexfind.ch/fe/fr/tol/10504/versions/55770/fr / RSJU (170.41)

S'agissant des communes, un état des lieux initial a été établi au moyen d'une enquête du préposé cantonal à la protection des données et à la transparence (PPDT). Un questionnaire adressé à une sélection de communes et d'entités représentatives ainsi que des séminaires réalisés avec leurs représentants dans le cadre de la présente stratégie ont permis de coconstruire cette dernière sur la base des enseignements clés suivants :

DONNÉES

Le but de la cybersécurité est la protection des données, soit des processus et services qui en dépendent. Parmi les mesures nécessaires, il ressort un besoin de sobriété en matière de données, notamment en archivant les données non nécessaires.

CARTOGRAPHIER / INVENTORIER

La connaissance de l'état et de la solidité des propres infrastructures IT ainsi que des compétences et de la préparation du personnel (cyberhygiène, gestion des risques et de crise, etc.) s'avère insuffisante. Le Jura ne dispose donc pas d'une appréciation sur son propre degré de maturité.

INFORMATION

Chaque personne doit pouvoir accéder à tout moment et simplement à de l'information pertinente sur les menaces et dangers. En l'état, les communes, entreprises et citoyens n'ont pas d'accès simplifié à ce type d'information et aux comportements à adopter.

FOURNISSEURS

La fourniture de services est souvent déléguée à des tiers / hébergeurs dont l'investissement dans la cybersécurité ne fait pas l'objet d'appréciations formelles. Les contrats avec les prestataires externes comprennent couramment des exigences sur le plan social, financier, ou des conditions de travail, mais la cybersécurité et la protection des données font souvent défaut.

COLLABORATION

Les responsables consultés reconnaissent la faiblesse de leurs connaissances et de leurs moyens et appellent de leurs vœux une collaboration accrue entre acteurs pour mutualiser leurs ressources et compétences.

ÉDUCATION

Les cyberincidents résultent souvent de compétences individuelles et collectives insuffisantes. Dans le Canton du Jura, la formation dispensée est le plus souvent limitée à un niveau élémentaire[9] qui ne suffit pas pour corriger les faiblesses constatées. Ce domaine est ainsi vu comme une priorité à tous les échelons.

[9] La Conférence des directrices et directeurs cantonaux de justice et police (CCDJP) a mandaté le Réseau national de sécurité (RNS) pour la mise en place du programme eCyAd d'enseignement à distance (eLearning) destiné au personnel des cantons et des communes. Il sera graduellement déployé dès 2023.

GOUVERNANCE

La cybersécurité n'est plus considérée comme un simple sujet délégable au niveau opérationnel; elle est désormais reconnue comme relevant d'abord de la responsabilité du niveau exécutif et la chaîne doit comprendre une fonction de « responsable sécurité ». Les attentes sont fortes pour que soient définis des rôles clairs pour chaque entité.

GESTION DE CRISE

Les personnes consultées considèrent les situations de crise comme des défis face auxquels elles s'estiment insuffisamment préparées.

LEADERSHIP

L'engagement et l'exemplarité doivent venir d'en haut. Il est attendu des décideurs qu'ils mettent à disposition des moyens dédiés à la cybersécurité en adéquation avec les enjeux et les objectifs qu'ils ont approuvés.

COMMUNICATION

Une communication fondée sur une culture de confiance et dans un environnement positif est essentielle en toute circonstance. Il s'agit aussi d'éviter une fatigue et *in fine* une démobilisation des destinataires.

La maturité des institutions jurassiennes face aux défis de la mutation numérique et des cyberrisques montre d'importantes marges de manœuvre.

2.3.2 TISSU ÉCONOMIQUE

Les statistiques et prévisions disponibles indiquent, malgré l'importance des zones grises dans les chiffres, une croissance continue du nombre et de la sévérité des cyberattaques dont l'impact peut devenir très important lorsque sont visées des infrastructures critiques (énergie, santé, transports, etc.). Du fait de l'attractivité d'une économie globalement en bonne santé, la Suisse représentera toujours davantage un but rentable pour les cybercriminels dont les méthodes ne cessent de progresser en termes de sophistication et de professionnalisation. En matière d'investissement dans la cybersécurité, la croissance dans les entreprises suisses ne suit cependant pas la même courbe, en raison notamment du fait que 90% des entreprises suisses sont des microentreprises ne disposant ni du temps ni des ressources pour s'emparer de ce domaine. Sur la base des constats faits ailleurs, on peut estimer comme limité le degré de maturité et de résilience des entreprises jurassiennes face aux cyberrisques.

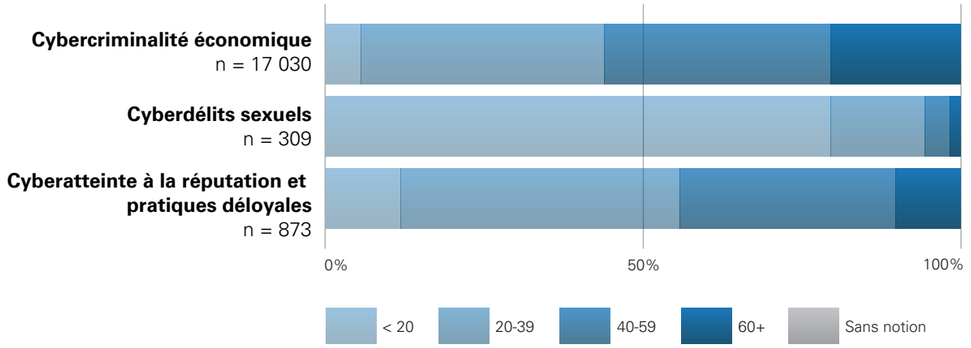
En raison de leur multiplication, les cyberattaques répondent par ailleurs de moins en moins à la définition d'événements « soudains et imprévisibles » couverts par les assurances. Les conditions pour la couverture des cyberrisques pourraient ainsi devenir plus restrictives et conduire certains acteurs modestes à y renoncer. Insuffisamment protégées, peu préparées à la gestion de crise et en plus non assurées, les entités touchées par des cyberattaques seraient plus exposées à des difficultés économiques, voire à des situations de faillites[10]. Et en bout de chaîne, des difficultés sociales et des pertes fiscales impacteraient le Canton lui-même.

[10] Différents chiffres circulent. En France, tous montrent que de nombreuses entreprises victimes de cyberattaques déposent le bilan quelques mois plus tard.

2.3.3 CITOYENS

Former les jeunes au monde de demain est une priorité et le « Plan d'action numérique pour l'école et la formation jurassienne » est une des mesures fortes du Programme gouvernemental de législature. Ce plan ne couvre toutefois qu'une partie de la population qui est elle-même toujours plus exposée aux cybercriminels. Les statistiques policières nationales sur les années 2020 et 2021 ont montré une progression de 24% des infractions numériques et toutes les statistiques et prévisions internationales vont dans le sens d'une aggravation continue.

Nous faisons face à une situation complexe et devons, sur la base des récents développements, considérer que la part de population non préparée aux cyberrisques ira croissant. Il faut donc ainsi s'attendre à ce que le nombre de victimes progresse en raison de l'augmentation de la surface d'attaque (toujours plus de systèmes et de terminaux connectés) et de la multiplication des délits. Le numérique représente une aubaine pour la criminalité qui bénéficie du rapide développement technologique. Cependant, il est important de noter que le numérique peut également représenter un obstacle pour un nombre croissant de personnes, notamment pour les seniors de plus de 65 ans. D'ici 2030, ils constitueront près de 25% de la population[11]. Ces cas viendront ainsi surcharger des autorités de poursuite pénale déjà fortement sollicitées et dont la préparation à ces phénomènes est encore lacunaire.



Source : OFS – Statistique policière de la criminalité (SPC) © OFS 2022

Figure 3 – Répartition de l'âge des personnes lésées par domaines de la criminalité numérique

[11] https://www.bfs.admin.ch/bfs/fr/home/statistiques/population/evolution-future/scenarios-suisse.assetdetail.14963222.html

3. STRATÉGIE

3.1 VISION

UN JURA NUMÉRIQUE SÛR

EXEMPLAIRE, RÉSILIENT, SOUVERAIN ET PROACTIF

Le Gouvernement jurassien a pour ambition que la numérisation profite à toute la société jurassienne et, dans la mesure du possible, que les risques accompagnant cette mutation soient maîtrisés, les données protégées, et que les services essentiels dont dépend la société soient assurés en tout temps.

Les principes d'action suivants caractérisent la stratégie du Jura :

EXEMPLAIRE

La sécurité doit être inclusive et toute la société jurassienne doit y adhérer et y contribuer activement.

RÉSILIENT

Comme tous les incidents, ceux du cyber ne sont pas toujours évitables, mais une préparation adéquate doit permettre de contenir leurs conséquences à un niveau supportable.

SOUVERAIN

La cybersécurité est désormais une tâche impérative pour la sécurité et la prospérité communes, au même titre que les autres politiques publiques. Il s'agit d'une responsabilité non délégable et dont le succès dépend de la collaboration entre les acteurs.

PROACTIF

Gouverner c'est prévoir, et la cybersécurité ne fait pas exception. Se préparer à temps est donc impératif et cela commence par une connaissance globale des défis et la parfaite connaissance des propres intérêts et actifs[12] numériques.

[12] Ensemble des éléments software (applications), hardware (matériel) et des données.

3.2 BUTS

La SCJU s'adresse à toute la société jurassienne. Elle pose un cadre, afin que tâches, compétences et responsabilités de chaque entité – de l'État à l'individu –, selon ses spécificités, contribuent à la protection des données et à la sécurité des systèmes TIC dont l'entité en question a la charge.

La SCJU considère six groupes de destinataires :

- les autorités cantonales jurassiennes[13];
- les établissements de droit public[14];
- les communes[15];
- les institutions paraétatiques[16];
- les prestataires d'importance[17];
- les tiers et le grand public.

Chacune de ces entités doit garantir que les données et systèmes TIC de traitement dont elle a la charge :

• ne sont accessibles qu'aux entités autorisées	**CONFIDENTIALITÉ**
• sont disponibles en cas de besoin	**DISPONIBILITÉ**
• ne peuvent être modifiées sans droit ou par mégarde	**INTÉGRITÉ**
• permettent d'assurer leur origine et leur suivi	**TRAÇABILITÉ**

Il s'agit donc de veiller à ce que les moyens TIC auxquels les différentes entités publiques ou privées recourent pour accomplir leurs tâches au profit de leurs bénéficiaires respectifs soient protégés contre toute forme d'utilisation malveillante, abusive ou perturbatrice.

La SCJU souhaite par ailleurs promouvoir la mutualisation de certaines tâches, comme l'exploitation d'infrastructures TIC, afin de maximaliser les effets pour la sécurité et de produire des économies d'échelle.

[13] Parlement, Gouvernement, administration et services de l'État.
[14] Hôpital du Jura, Caisse de compensation, Caisse de pensions, ECA.
[15] Législatif et exécutif, administration et services communaux.
[16] Crèches, hôpitaux et centres de soins privés, associations, fondations, EMS, accueil parascolaire, etc., auxquels l'État délègue des prestations (liste indicative sous https://www.ppdt-june.ch).
[17] Entités dont les prestations sont significatives / systémiques pour l'État (tels que fournisseurs d'électricité et télécom, transports, service postal et tout poids lourd économique) dont le défaut suite à une cyberattaque aurait un impact significatif pour le Canton du Jura.

3.3 ARCHITECTURE

En raison de leurs responsabilités respectives et des obligations légales, les entités auxquelles s'adresse la SCJU sont appelées à endosser de nombreuses tâches et à réaliser les mesures y relatives, conformément aux règles de l'art et dans le respect du principe de proportionnalité.

Ces mesures s'articulent selon les **5 piliers** du *NIST Cybersecurity Framework*[18] représentés à la figure 4. Ce cadre doit permettre de couvrir l'ensemble des besoins et de favoriser l'interopérabilité des entités entre elles et avec leurs partenaires.

À ces piliers s'ajoute le suivi de situation, permettant de toujours tenir compte de l'environnement global, et la gouvernance, qui sert à assurer la cohérence de l'ensemble ainsi que la coordination des nombreux acteurs concernés et qui définit les rôles et tâches de chacun.

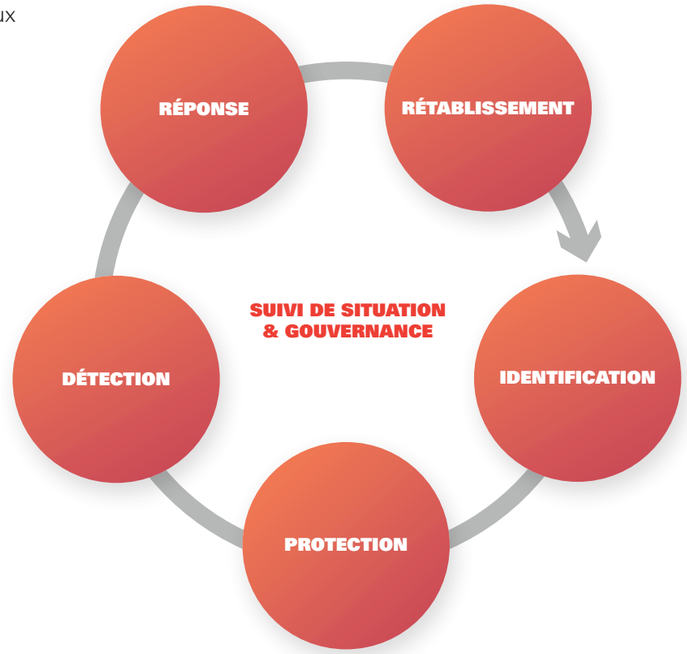


Figure 4 - Piliers de la stratégie de cybersécurité du Jura

[18] National Institute of Standards and Technology (NIST).

3.3.1 IDENTIFICATION

Les destinataires de la SCJU doivent créer, à leur niveau, les conditions favorables de leur cybersécurité par une connaissance et une gestion de leurs actifs (données, personnel, dispositifs, systèmes, installations, etc.). Ainsi, ils sont en mesure de distinguer l'important de l'accessoire, de définir leurs priorités, d'attribuer les tâches et responsabilités aux parties prenantes et d'établir une gestion dynamique de leurs cyberrisques.

3.3.2 PROTECTION

Selon leurs métiers, responsabilités, moyens et risques, les entités publiques et privées mettent en œuvre les bonnes pratiques et recommandations en vigueur. Elles comprennent notamment les mesures de contrôles d'accès, de sensibilisation, de formation et d'entraînement de leur propre personnel et des entités partenaires / clientes, ainsi que l'ensemble des mesures techniques et opérationnelles de protection des données, des systèmes et des infrastructures selon l'état de la technique du moment, le tout en étroite collaboration avec les prestataires de service impliqués.

3.3.3 DÉTECTION

Les parties doivent en tout temps rester vigilantes. Les recommandations et alertes doivent être diffusées et mises en œuvre sans délai. Les systèmes et infrastructures TIC doivent être surveillés en continu (monitoring) et les processus (y c. de détection d'incidents) régulièrement entretenus et testés. Il est attendu des utilisateurs qu'ils annoncent sans délai toute perturbation ou anomalie. Il est aussi attendu de la part de tous les acteurs, même en l'absence de bases légales formelles, qu'ils informent spontanément les autorités cantonales en cas d'incident afin qu'elles puissent, en garantissant l'anonymat et la confidentialité de ces informations, alerter tout tiers qui pourrait être impacté et augmenter sa connaissance des phénomènes et de la façon de s'en prémunir.

3.3.4 RÉPONSE

Chaque entité publique et privée doit disposer d'une cellule de gestion de crise ou au minimum d'un point de contact responsable. Ces éléments doivent être préparés et entraînés à la gestion des crises cyber. Ils doivent connaître leur cartographie / inventaire respectifs et avoir accès aux informations et alertes. Ils doivent savoir à qui s'adresser en matière d'assistance technique (p. ex. forensique pour analyser et qualifier les cyberincidents) et non technique (p. ex. communication et soutien juridique).

3.3.5 RÉTABLISSEMENT

Chaque entité doit disposer de planifications prévisionnelles (« qu'est-ce que je fais si… ? ») permettant, en cas de crise, de rapidement prendre des dispositions convenues et éprouvées et ainsi de revenir le plus rapidement possible à la normale tout en minimisant autant que possible les conséquences. Parmi les mesures clés figurent les sauvegardes régulières des données et leur vérification, ainsi que les journaux d'activités (logs). En cas de crise, il s'agit également de protocoler les actions et les observations pertinentes afin, une fois la crise passée, de se servir de ces informations et d'en tirer des enseignements pour améliorer ses propres mesures et procédures de sécurité, d'en faire profiter d'autres entités et de se prémunir de prétentions injustifiées de tiers.

3.3.6 SUIVI DE SITUATION ET GOUVERNANCE

Les 5 piliers qui précèdent permettent un suivi dynamique de l'organisation et des systèmes internes ainsi que des cyberrisques au niveau technique. Il est toutefois impératif que l'échelon stratégique dispose de la vue d'ensemble sur les domaines qui influencent ou sont influencés par la mutation numérique (voir ch. 1.1 à 1.4). C'est la fonction du suivi de situation qui doit permettre aux décideurs de toujours contextualiser le numérique dans l'écosystème global.

La gouvernance, quant à elle, également de niveau stratégique, détermine le cadre nécessaire pour synchroniser les responsabilités, les coopérations[19], les procédures, les projets, les mesures et les ressources des différentes entités. Elle définit les rôles et responsabilités de chacun afin de garantir une mise en œuvre durable, agile, homogène, efficiente et efficace de la stratégie. La figure 5 distingue :

- les entités soumises au droit public et pour lesquelles le dispositif de la SCJU est impératif et
- les entités soumises au droit privé et pour lesquelles la SCJU ne représente que des recommandations.

[19] Personne n'est en mesure d'affronter seul et de façon prolongée l'ensemble des cyberrisques et de leurs conséquences. Il s'agit donc, partout où cela est possible, d'établir des partenariats permettant de gagner en profondeur, largeur et endurance dans chacun des piliers. Ces partenariats comprennent notamment le Centre national de cybersécurité (NCSC), les fournisseurs de services, les entreprises spécialisées dans la cybersécurité, les cantons voisins, les organisations régionales telles que le Regional Cyber Competence Center (RC3) et le domaine académique.

Aucune entité ne peut déléguer ses responsabilités.
En revanche, certaines tâches peuvent être déléguées selon les principes généraux exposés à la figure 5.

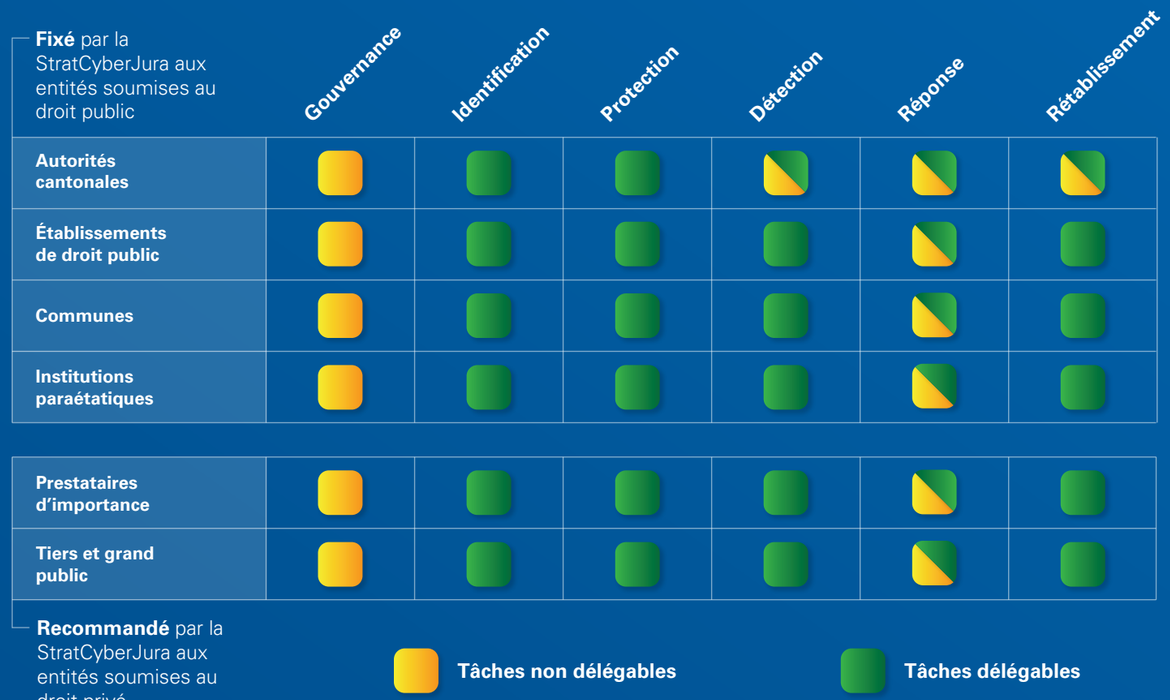


Figure 5 – Responsabilités et tâches des différentes entités en matière de cybersécurité

3.4 RÔLES

Afin d'atteindre les objectifs de la SCJU, la clarification des rôles est essentielle pour assurer les flux d'information, des prises de décisions rapides, une grande agilité et un emploi parcimonieux des ressources. La figure 6 explicite les relations entre les différentes entités.

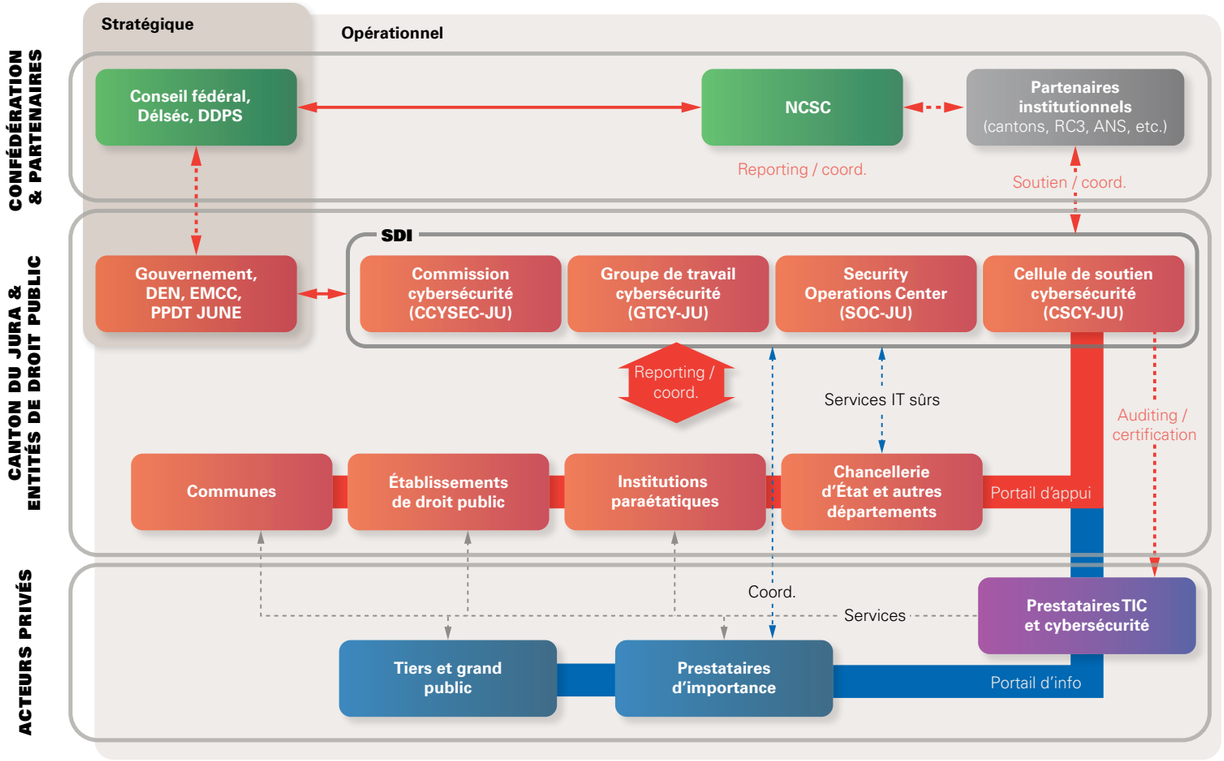


Figure 6 – Répartition des rôles en matière de cybersécurité

Le **SDI**, chargé de l'exploitation sûre des infrastructures et systèmes IT du Canton, est le **centre de compétence cantonal en matière de cybersécurité**. Pour remplir sa mission, il dispose de quatre organes de pilotage et d'appui :

LA COMMISSION CYBERSÉCURITÉ (CCYSEC-JU)

Nommée par le chef du DEN, elle est dirigée par le chef de service du SDI et comprend des représentants de la Chancellerie d'État, des autres départements ainsi que des communes ou de leurs syndicats.

Sa mission est d'assurer l'accompagnement stratégique et politique de la stratégie.

LE GROUPE DE TRAVAIL CYBERSÉCURITÉ (GTCY-JU)

Conduit par le responsable de la cybersécurité du SDI, il est composé de représentants du SDI, des communes, des établissements de droit public et des institutions paraétatiques. Les prestataires d'importance et les représentants des prestataires TIC et de cybersécurité pourront y être invités selon les besoins.

Sa mission est de coordonner les mesures, moyens et actions de la SCJU.

LE SECURITY OPERATIONS CENTER (SOC-JU)

Conduit par le responsable de la cybersécurité du SDI.

Sa mission est le monitoring permanent des infrastructures TIC de l'État, la détection d'anomalies et la prise de mesures immédiates en cas d'incident.

Selon la gravité de la crise, le chef de service adjoint du SDI[20] prend la tête de la **cellule de gestion de crise cyber** cantonale, un instrument qui peut aussi apporter un soutien spécialisé aux structures de conduite de l'État en cas de crise.

CELLULE DE SOUTIEN CYBERSÉCURITÉ (CSCY-JU)

Cette cellule, placée sous la direction du SDI, livre conseils et soutiens pratiques.

Sa mission est d'aider les entités de droit public à mettre en œuvre la stratégie et à augmenter leur maturité.

Elle intervient notamment en matière de relations avec les prestataires, d'audits, de tests de pénétration et de sensibilisation / formation. La cellule peut être renforcée par des spécialistes du SDI et faire appel à des mandataires externes. Ses prestations seront étoffées au cours du temps.

[20] Ce dispositif permet au chef de service du SDI de ne pas être submergé par les considérants opérationnels et au chef de la cybersécurité du SDI de rester concentré sur les tâches techniques.

3.5 MESURES POUR LA MISE EN ŒUVRE DE LA STRATÉGIE POUR LE CANTON ET LES ENTITÉS DE DROIT PUBLIC

Le tableau ci-dessous énumère les mesures dévolues aux entités en titre et qui seront graduellement réalisées et complétées d'ici 2026 (voir chiffre 4.5).

	GOUVERNANCE	IDENTIFICATION	PROTECTION	DÉTECTION	RÉPONSE	RÉTABLISSEMENT
AUTORITÉS CANTONALES (SDI)	**Création et conduite** • Commission cybersécurité CCYSEC-JU • Groupe de travail cybersécurité GTCY-JU • Cellule de soutien cybersécurité CSCY-JU **En continu** • Mesure de la maturité de la cybersécurité du canton • Reporting au Gouvernement • Communication • Contribution au développement et actions de la Confédération	• Inventaire des actifs[21] • Identification des menaces et vulnérabilités • Gestion des risques • Établissement et diffusion de la situation et des alertes aux autres entités publiques	• Mesures techniques et non techniques de cybersécurité (selon catalogue SDI) • Plan de sensibilisation, formation et entraînement du personnel de l'État • Contribution à la sensibilisation de la population (aussi dans les écoles) et des entreprises aux cyberrisques	• Testing / auditing du propre dispositif et des tiers • Création et exploitation du Security Operations Center SOC-JU • Analyse d'impact des événements (déclenchement de la réponse si significatif)	• Établissement et maintien en condition de la cellule cantonale de gestion de crise cyber • Gestion de crise en cas d'incident • Assistance subsidiaire aux entités de droit public en cas d'incident	• Développement / actualisation des planifications prévisionnelles; communication / coordination avec les parties prenantes • Établissement et test de plans de restauration • Pilotage du retour sur expérience
ÉTABLISSEMENTS DE DROIT PUBLIC **COMMUNES** **INSTITUTIONS PARAÉTATIQUES**	• Planification et mise en œuvre de la stratégie cantonale au propre échelon • Désignation d'un responsable / SPOC cybersécurité • Pilotage des fournisseurs (adaptation des bases contractuelles) • Participation à la CCYSEC-JU et GTCY-JU (selon clé de répartition) • Reporting à la propre direction et au GTCY-JU	• Inventaire des actifs[21] • Gestion des risques (actualisation selon la situation et les alertes)	• Mesures techniques et non techniques de cybersécurité* • Formation et entraînement du personnel* * selon standards métier et recommandations de la CSCY-JU	• Testing / auditing du dispositif (y c. des tiers avec soutien de la CSCY-JU) • Monitoring de la propre infrastructure • Analyse d'impact en cas d'événement significatif	• Établissement et maintien en condition de la cellule / point de contact cyber • Engagement et coordination des acteurs lors d'événements	• Développement / actualisation des planifications prévisionnelles; communication / coordination avec les parties prenantes • Établissement et test de plans de restauration

[21] Ensemble des éléments software (applications), hardware (matériel) et des données représentant de la valeur pour une organisation.

Figure 7 – Tâches des entités cantonales et de droit public

4. MISE EN ŒUVRE

4.1 PILOTAGE

La SCJU sera pilotée stratégiquement par la **Commission cybersécurité** (CCYSEC-JU[22]) présidée par le chef du SDI. La Commission sera appuyée opérationnellement par le **Groupe de travail cybersécurité** (GTCY-JU) conduit par le responsable de la cybersécurité du SDI.

Une planification détaillée de la mise en œuvre de la stratégie, notamment pour les mesures techniques, sera réalisée par le SDI dès l'approbation par le Gouvernement.

L'avancement des travaux sera rapporté trimestriellement au chef du DEN et annuellement au Gouvernement jurassien au moyen d'un tableau de bord comprenant les points de mesure de succès (KPI[23]) et le résultat d'un sondage annuel effectué auprès des différentes entités.

[22] Il est recommandé de désigner un employé de la commune dans la durée.

[23] Key Performance Indicators.

4.2 MESURES DE SUCCÈS (KPI)

Les indicateurs suivants (en % du nombre d'entités de droit public[24]) seront mesurés.

a. Entités ayant mis en place un **responsable cybersécurité**.
b. Réalisation de l'**inventorisation** des actifs.
c. Plan de **gestion des risques** établi.
d. Entités en conformité avec la **CPDT-JUNE**.
e. Entités ayant déterminé leurs **relations contractuelles** avec leurs fournisseurs IT, en particulier en matière d'exigences de cybersécurité.
f. Entités ayant atteint le niveau 3/5 **de maturité**[25] en matière de cybersécurité / ou accédé à des labels reconnus tels que Cyber Safe.
g. **Points de contact** et remplaçants formés à la gestion de crise (formation de base + répétition annuelle).
h. Entités dont les collaborateurs sont **sensibilisés** aux cyberrisques (yc. maintien périodique du niveau avec p.ex. eCyAd).
i. Entités dont les fournisseurs sont certifiés selon un cadre de référence qui sera élaboré sous la direction du SDI en collaboration avec les partenaires impliqués.
j. Entités disposant de **planifications prévisionnelles** (les «what if») en cas d'incident.

[24] Cette liste sera établie au début de la mise en œuvre de la SCJU.

[25] Selon CMMC (Cybersecurity Maturity Model Certification) du NIST.

1) **Appliqué** Les actions nécessaires sont mises en œuvre mais ne sont pas documentées ou spécifiquement pilotées.

2) **Documenté** Les actions menées et les règles en vigueur sont documentées, par domaine.

3) **Suivi** La politique de cybersécurité est concrètement pilotée : ressources identifiées, plan d'action et de formation défini, etc.

4) **Revues** Un mécanisme d'évaluation est mis en place pour analyser la politique cyber et permettre sa réévaluation régulière.

5) **Optimisé** L'approche est standardisée et optimisée pour l'ensemble de la structure, par domaine.

4.3 RESSOURCES

Définir une enveloppe globale n'est pas possible en l'état. Chaque projet devra faire l'objet d'une planification dédiée et répondre à la **règle PPQITR**:

PRIORITÉ
Justifier l'importance et l'urgence

PRODUIT
Définir l'objet et l'effet recherché

QUALITÉ
Définir le niveau d'ambition

INTENTION
Définir le « comment », l'idée de manœuvre pour atteindre le but

TEMPS
Définir le point de départ et la durée

RESSOURCES
Décliner les coûts financiers et en personnel

Les projets seront établis en principe par le Groupe de travail cybersécurité (simple ou élargi selon les sujets) puis soumis à la Commission cybersécurité qui, le cas échéant, les fera ensuite approuver par les autorités compétentes.

4.4 COMMUNICATION

Un plan de communication sera élaboré en parallèle du plan de réalisation de la stratégie. Le but est de démystifier la cybersécurité et de la rendre intéressante pour la population jurassienne afin que celle-ci devienne activement partie prenante du résultat. La Commission cybersécurité sera systématiquement consultée avec la tâche spécifique d'assurer dans la durée la cohérence de l'ensemble.

4.5 FEUILLE DE ROUTE

Le plan suivant pose les balises principales de la mise en œuvre de la stratégie qui devra atteindre ses objectifs à la fin de la législature, soit à fin 2025. Ce plan ne considère pas les mesures techniques qui feront l'objet de plans internes spécifiques à chaque entité.

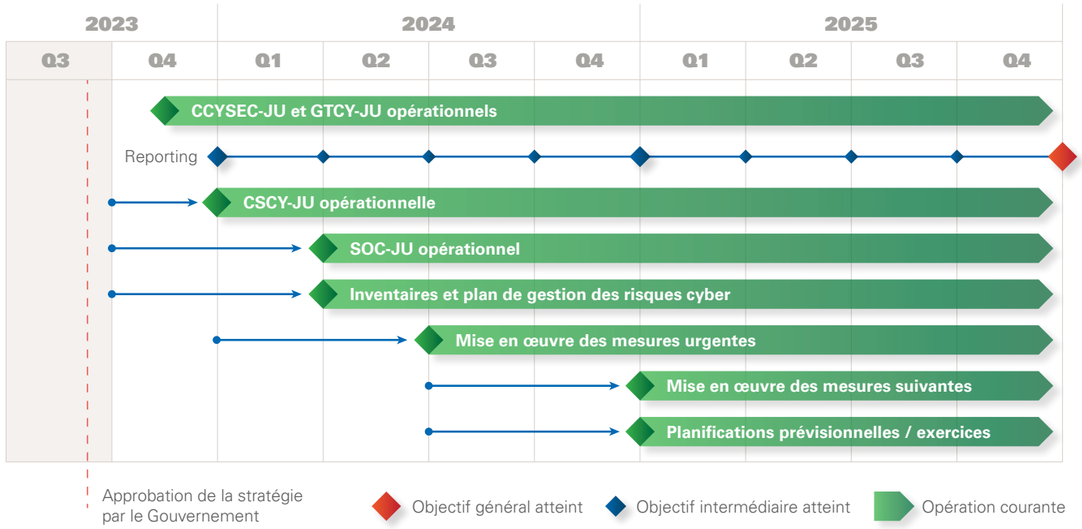


Figure 8 – Feuille de route

4.6 RÉVISION

Compte tenu de l'accélération du développement technologique (notamment en matière d'intelligence artificielle et d'informatique quantique, dont les progrès vont rapidement menacer les processus basés sur de la cryptographie « non quantum resistant »), des tensions géopolitiques et de l'augmentation continue de la cybercriminalité, un suivi permanent de situation sera nécessaire. L'impact de la stratégie sera suivi en continu au moyen de dix indicateurs de succès. La Commission cybersécurité émettra fréquemment ses recommandations et le Gouvernement décidera sur ces bases d'une mise à jour éventuelle de la stratégie en relation avec le prochain plan de législature.

ABRÉVIATIONS

CCYSEC-JU	Commission cybersécurité
CPDT-JUNE	Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel
CSCY-JU	Cellule de soutien cybersécurité
CSN	Cyberstratégie nationale
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DélSéc	Délégation de sécurité du Conseil fédéral
GTCY-JU	Groupe de travail cybersécurité
KPI	Key Performance Indicators
LGVS	Loi concernant le guichet virtuel sécurisé
LPD	Loi sur la protection des données
LSI	Loi sur la sécurité de l'information
PPDT	Préposé cantonal à la protection des données et à la transparence
PPQITR	Priorité, Produit, Qualité, Intention, Temps, Ressources
NCSC	National Cyber Security Center
NIST	National Institute of Standards and Technology
RC3	Regional Cyber Competence Center
RGPD	Règlement général de l'UE sur la protection des données
SCJU	Stratégie de cybersécurité de la République et Canton du Jura
SDI	Service de l'informatique
SOC-JU	Security Operations Center
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
TIC	Technologies de l'information et de la communication

IMPRESSUM

Stratégie de cybersécurité de la République et Canton du Jura

ÉDITEUR

Gouvernement de la République et Canton du Jura

CONCEPTION

Service de l'informatique

PHOTOGRAPHIES

République et Canton du Jura

JURA CH RÉPUBLIQUE ET CANTON DU JURA