Groupe des 5 Partenaires

Adaptation à l'évolution des menaces :

Résumé des approches en matière de sécurité et de résilience des infrastructures essentielles du Groupe des 5 Partenaires

En partenariat avec les gouvernements de : l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis.

Cette publication peut être consultée en ligne à l'adresse suivante :
www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2024-dptng-vlvng-thrts/index-fr.aspx

Ce résumé fait le point sur l'évolution des risques pour les infrastructures essentielles et explique comment les pays du Groupe des 5 Partenaires ont modernisé leurs approches en matière de protection des infrastructures essentielles. Il met également de l'avant des moyens communs pour renforcer la sécurité et la résilience des infrastructures essentielles dans chacun des pays, tout en reconnaissant l'importance d'une approche concertée et coordonnée au sein de la communauté internationale compte tenu de la nature interreliée des infrastructures essentielles.

Also available in English under the title: Adapting to Evolving Threats: A Summary of Critical 5 Approaches to Critical Infrastructure Security and Resilience

Sécurité publique Canada (Communications)
269, avenue Laurier Ouest
Ottawa (Ontario) K1A 0P8

Communications@ps-sp.gc.ca
www.securitepublique.gc.ca

Date de publication : 2024-06
Numéro de catalogue : PS9-35/2024F-PDF
ISBN : 978-0-660-71372-4

Table des matières

Introduction

En 2014, le Groupe des 5 Partenaires a publié un exposé commun intitulé : Forger une compréhension commune des infrastructures essentielles. Cette publication établissait une interprétation collective des concepts et des définitions des infrastructures essentielles et visait à faciliter la coordination des approches en matière de protection de ces infrastructures. Au cours de la décennie suivante, le contexte géopolitique a évolué et les effets des changements climatiques ont été ressentis plus rapidement que prévu. Les pays du Groupe des 5 Partenaires remanient donc leurs approches en fonction des nouveaux risques et des menaces émergentes, d'où l'importance de revoir et de mettre à jour leur exposé commun.

Ce résumé fait le point sur l'évolution des risques pour les infrastructures essentielles et explique comment les pays du Groupe des 5 Partenaires ont modernisé leurs approches en matière de protection des infrastructures essentielles. Il met également de l'avant des moyens communs pour renforcer la sécurité et la résilience des infrastructures essentielles dans chacun des pays, tout en reconnaissant l'importance d'une approche concertée et coordonnée au sein de la communauté internationale compte tenu de la nature interreliée des infrastructures essentielles.

La résilience au cœur de la sécurité des infrastructures essentielles

Les sociétés modernes dépendent de systèmes d'infrastructures essentielles pour fournir des services essentiels à la vie des canadiens et à leurs moyens de subsistance. La défaillance d'une infrastructure essentielle peut être catastrophique. Notons d'ailleurs que les dommages causés aux infrastructures essentielles et l'interruption des services sont parmi les principales causes des pertes économiques dues aux catastrophes[1]. Conscients de ce fait, les pays du Groupe des 5 Partenaires s'efforcent d'assurer la sécurité, la protection et la résilience des

[1] Nations Unies – Département des affaires économiques et sociales. « UN DESA Policy Brief No. 139: Strengthening Disaster Risk Reduction and Resilience for Climate Action through Risk-Informed Governance » | Département des affaires économiques et sociales, Nations Unies, 6 octobre 2022, www.un.org/development/desa/dpad/publication/un-desa-policy-brief-no-139-strengthening-disaster-risk-reduction-and-resilience-for-climate-action-through-risk-informed-governance.

biens et systèmes de leurs infrastructures essentielles afin de minimiser et de prévenir les perturbations en cas d'incident.

La nécessité de telles interventions est plus pressante que jamais. Les systèmes d'infrastructures essentielles sont de plus en plus interdépendants et interreliés. Les défaillances d'une organisation risquent de créer des pannes en cascades importantes. Parallèlement, les risques et les menaces qui pèsent sur nos systèmes d'infrastructures ne cessent d'augmenter.

Nous savons également que nombre de nos infrastructures essentielles ne sont pas préparées à ce nouvel avenir. La pandémie de COVID-19, par exemple, a révélé des lacunes dans la planification de la continuité des activités des infrastructures essentielles, notamment des stocks inadéquats d'équipements de protection individuelle et des difficultés à établir des priorités et à protéger les actifs clés. Les gouvernements ont dû intervenir pour donner la priorité aux activités essentielles afin de minimiser les perturbations économiques et d'assurer la continuité de la prestation des services essentiels.

Dans ce contexte, nous savons que l'absence d'investissements adéquats dans la résilience des infrastructures essentielles aura les conséquences suivantes :

- Des effets négatifs sur le bien-être des personnes, des entreprises et des communautés touchées par des perturbations qui, dans de nombreux cas, auraient pu être évitées;
- Des coûts importants pour l'économie, car les frais de rétablissement et de reprise des services dépassant généralement ce qui est nécessaire pour prévenir les pannes avant tout événement.

Investir de le renforcement de la résilience aujourd'hui est un pas vers l'avenir qui apporte un certain nombre d'avantages positifs :

- Sauver des vies et préserver les moyens de subsistance;
- Maintenir la cohésion sociale;

- Réduire les chocs économiques sur les chaînes d'approvisionnement;
- Promouvoir des solutions et des technologies innovantes pour minimiser les dommages causés aux communautés.

Évolution du contexte des menaces et des risques

Depuis 2014, le contexte géopolitique s'est complexifié. Les infrastructures essentielles sont désormais confrontées à un éventail plus large de menaces et de risques, qu'il s'agisse d'événements d'origine naturelle ou de perturbations d'origine humaine, qu'elles soient accidentelles ou malveillantes. De plus, les biens et les systèmes des infrastructures essentielles sont davantage intégrés qu'en 2014, car les progrès technologiques de la dernière décennie ont encouragé les propriétaires et les exploitants d'infrastructures essentielles à rationaliser la prestation de services en adoptant des systèmes numériques.

Par conséquent, le risque qu'un événement déclenche des défaillances en cascade dans plusieurs secteurs interdépendants et ait des répercussions nationales et internationales étendues s'est considérablement accru.

L'évolution du contexte géopolitique au cours de la dernière décennie a intensifié les préoccupations en matière de sécurité nationale. Les conflits récents ont montré comment les infrastructures essentielles peuvent être ciblées par des moyens cybernétiques ou physiques afin d'affaiblir la capacité d'un pays à se protéger et à protéger ses citoyens. En deçà du seuil du conflit armé, les auteurs de menace hostiles déploient des méthodes telles que les campagnes d'ingérence étrangère, le vol de propriété intellectuelle et les perturbations opérationnelles pour exploiter les infrastructures essentielles, ce qui entraîne des pertes financières considérables, notamment des dépenses d'entretien et de réparation, des pertes de revenus et une augmentation des coûts de sécurité.

L'adoption de technologies numériques et téléopérées pour les systèmes d'infrastructures essentielles a également rendu ces derniers de plus en plus vulnérables à l'exploitation par des cybercriminels et des acteurs parrainés par un État. Les cyberincidents peuvent avoir des conséquences, notamment des pannes d'électricité, la contamination de l'eau potable, la perturbation des réseaux de transport, allant jusqu'à la perte de vies humaines. De telles

perturbations peuvent causer d'importants dommages financiers et entacher la réputation de diverses organisations, et réduire la confiance envers les institutions.

Les risques liés aux changements climatiques augmentent avec la fréquence, l'intensité et l'imprévisibilité des phénomènes météorologiques extrêmes, lesquels exercent une pression considérable sur les infrastructures matérielles essentielles telles que les réseaux de transport, les systèmes de télécommunication et les infrastructures énergétiques. En l'absence d'efforts appropriés pour atténuer les effets des changements climatiques afin de s'y adapter, ces biens sont confrontés à un risque croissant de perturbations plus fréquentes et de défaillances catastrophiques.

Adaptation au contexte des menaces en évolution pesant sur les infrastructures essentielles

Afin de relever les défis posés par les menaces actuelles et futures, les pays du Groupe des 5 Partenaires ont dû adapter leur approche pour assurer la sécurité et la résilience des infrastructures essentielles en misant sur les mesures suivantes :

- Modernisation des politiques;
- Révision de la définition des infrastructures essentielles et de la composition des secteurs;
- Élaboration d'outils de mise en commun de l'information et de mécanismes de partenariat plus solides.

Modernisation des politiques

Depuis 2014, les pays du Groupe des 5 Partenaires ont réalisé des avancées notables en matière de politiques et de programmes afin de protéger et de sécuriser leurs infrastructures essentielles.

Australie

En 2018, l'Australie a mis en œuvre sa principale loi en matière de sécurité des infrastructures essentielles, la *Security of Critical Infrastructure Act 2018* - SOCI Act. Depuis lors, des modifications y ont été apportées pour tenir compte des nouvelles menaces. La SOCI Act vise à renforcer la sécurité et la résilience des infrastructures essentielles en s'intéressant aux secteurs et aux catégories d'actifs essentiels de l'Australie. Elle fournit un niveau de sécurité de base dans 11 secteurs d'infrastructures essentielles et impose plusieurs obligations aux entités qui en sont responsables, dont :

- La possibilité d'imposer des obligations renforcées en matière de cybersécurité aux infrastructures essentielles les plus importantes de l'Australie en tant que systèmes d'importance nationale. Il s'agit d'infrastructures qui, si elles étaient perturbées, pourraient avoir des effets en cascade importants sur la société australienne et sur la sécurité nationale;

- La communication d'information sur les opérations et la propriété au registre des infrastructures essentielles, qui est géré par le ministère de l'Intérieur;

- La mise en place d'un programme de gestion des risques liés aux infrastructures essentielles qui exige des entités qu'elles identifient et atténuent les risques internes, physiques ou naturels, les cyberrisques et les risques liés à la chaîne d'approvisionnement qui pèsent sur les actifs infrastructures essentielles;

- L'obligation de signaler les incidents de cybersécurité au portail ReportCyber de l'Australian Cyber Security Centre;

- Des mesures d'assistance gouvernementale réactives pour permettre au gouvernement d'aider l'industrie à intervenir en cas de cyberincident grave.

Le Réseau d'échange d'information de confiance (Trusted Information Sharing Network – TISN), créé en 2003, est le principal mécanisme de mobilisation du gouvernement australien avec l'industrie en ce qui concerne les infrastructures essentielles. Il réunit des intervenants de toute la communauté des infrastructures essentielles, notamment des propriétaires et des exploitants d'infrastructures essentielles, des entités de la chaîne d'approvisionnement, des experts en la matière et tous les ordres de gouvernement. Les membres se réunissent

régulièrement entre eux et au sein de groupes sectoriels dans le but d'améliorer la sécurité et la résilience des infrastructures essentielles. L'Australie a également élaboré une plateforme virtuelle de mobilisation TISN, offrant un environnement plus flexible pour soutenir les activités de mobilisation TISN.

La Stratégie de résilience des infrastructures essentielles (Critical Infrastructure Resilience Strategy) de 2023 fournit un cadre national pour guider l'Australie vers une sécurité et une résilience accrues des infrastructures essentielles. Élaborée en consultation avec la communauté des infrastructures essentielles et soutenue par le Plan de résilience des infrastructures essentielles de 2023 (*2023 Critical Infrastructure Resilience Plan*), la Stratégie guidera les intérêts de l'Australie en matière d'infrastructures essentielles de 2023 à 2028.

En novembre 2023, l'Australie a publié la Stratégie australienne de cybersécurité 2023-2030 (2023-2030 Australian Cyber Security Strategy). Dans le cadre du quatrième bouclier de cette stratégie, le gouvernement s'est engagé à protéger les infrastructures essentielles et les systèmes gouvernementaux essentiels de l'Australie afin que le pays puisse résister aux cyberattaques et se rétablir. Il doit pour ce faire :

- Préciser l'application de la SOCI Act afin de s'assurer que les infrastructures essentielles protègent leurs systèmes de stockage de données et que leurs fournisseurs de services améliorent leurs paramètres de sécurité;

- Fournir des orientations sur les pratiques exemplaires, des exercices et des conseils sur les cadres réglementaires en travaillant avec l'industrie pour concevoir conjointement des obligations de sécurité pour les fournisseurs de services de télécommunications et en explorant les possibilités d'intégrer la réglementation en matière de cybersécurité à des exigences élargies pour les secteurs de l'aviation et de la marine;

- Établir un cadre pour assurer le respect des obligations en matière de sécurité et évaluer les conséquences secondaires des cyberincidents en explorant les pouvoirs permettant d'ordonner à une entité de prendre des mesures précises pour gérer les conséquences d'un incident d'importance nationale;

- Accélérer la mise en œuvre des infrastructures essentielles les plus interdépendantes et les plus importantes d'Australie afin de soutenir l'établissement d'un partenariat sur mesure et axé sur les résultats entre le gouvernement et les entités responsables des systèmes d'importance nationale;

- Renforcer la cybersécurité du gouvernement en permettant au coordonnateur national de la cybersécurité de superviser la mise en œuvre de mesures de cybersécurité et l'établissement de rapports connexes dans l'ensemble du gouvernement et de procéder à des examens de la cybermaturité des agences gouvernementales afin de positionner le gouvernement australien en tant que gouvernement numérique de confiance de classe mondiale;

- Mettre les défenses nationales à l'épreuve en élargissant le programme national d'exercices de cybersécurité dirigé par le coordonnateur national de la cybersécurité afin de déceler les lacunes dans les cyberdéfenses et d'élaborer des manuels d'intervention en cas d'incident.

Canada

Le Canada s'emploie à moderniser son approche en matière d'infrastructures essentielles. En 2022, le Canada a lancé une consultation publique sur la *Stratégie nationale sur les infrastructures essentielles de 2009* afin d'éclairer la prise de décisions pour assurer leur sécurité et leur protection. Alors que les travaux se poursuivent pour définir une approche politique révisée de la protection des infrastructures essentielles, le gouvernement du Canada a également déposé des textes législatifs et mis en œuvre des politiques visant à répondre aux menaces qui pèsent sur elles.

Le Canada a pris des mesures pour améliorer sa cybersécurité, y compris celle de ses infrastructures essentielles. En 2018, le Canada a lancé sa *Stratégie nationale de cybersécurité* (SNC), qui vise à faire progresser la cybersécurité et la résilience, à soutenir la cyberinnovation et à favoriser la collaboration entre les intervenants. La SNC a entraîné la création du Centre canadien pour la cybersécurité, qui travaille en étroite collaboration avec des partenaires nationaux et internationaux et constitue une ressource de confiance en matière de cybersécurité. Elle a également mené à la création du Groupe national de coordination contre la cybercriminalité de la Gendarmerie royale du Canada (GRC), qui vise

à accroître la capacité de la GRC à enquêter sur la cybercriminalité. En raison des progrès rapides de l'infrastructure numérique, le Canada met actuellement à jour sa SNC.

En 2022, le Canada a présenté le projet de loi C-26 qui, au moment de la rédaction du présent document, était en comité à la Chambre des communes pour examen. Le projet de loi C-26 édicte la *Loi sur la protection des cybersystèmes essentiels*, qui désignerait les entités sous réglementation fédérale de quatre secteurs prioritaires (à savoir l'énergie, les finances, les télécommunications et les transports) pour protéger leurs cybersystèmes essentiels. Si elle est adoptée, cette loi créera un registre des exploitants désignés des infrastructures essentielles qui seront soumis à des obligations en matière de cybersécurité.

Pour faire face aux menaces qui pèsent sur la sécurité économique, le Canada propose des modifications à la Loi sur Investissement Canada qui renforceront la visibilité du Canada en matière d'investissements, amélioreront la transparence, favoriseront une plus grande certitude pour les investisseurs et garantiront que le Canada dispose de pouvoirs solides pour prendre rapidement les mesures qui s'imposent. Les principales modifications comprennent de nouvelles exigences de dépôt avant la mise en œuvre d'investissements dans des secteurs commerciaux prescrits, un meilleur échange de renseignements avec les homologues internationaux et un pouvoir ministériel élargi de façon à étendre l'examen de la sécurité nationale des investissements, imposer des conditions au cours d'un examen de la sécurité nationale et accepter des engagements pour atténuer le risque pour la sécurité nationale.

Parallèlement, le Canada se penche sur les possibilités de moderniser ses outils de lutte contre l'ingérence étrangère, compte tenu de l'évolution rapide de cette menace. Dans le cadre d'une consultation publique lancée en novembre 2023, des avis ont été sollicités concernant des modifications potentielles à plusieurs lois canadiennes, dont les suivantes :

- Nouvelles infractions d'ingérence étrangère dans la *Loi sur la protection de l'information*;
- Mise à jour de l'infraction de sabotage dans le *Code criminel* pour renforcer la dissuasion des dommages intentionnels aux infrastructures essentielles;
- Introduction d'un mécanisme de révision dans la *Loi sur la preuve au Canada* pour les cas où il y a des renseignements de nature délicate;

- Modification de la *Loi sur le Service canadien du renseignement de sécurité* pour permettre à cet organisme de divulguer des renseignements de nature délicate à des personnes qui ne font pas partie du gouvernement du Canada.

En 2023, le Canada a également publié le premier rapport public du Profil national des risques, sa première évaluation stratégique des risques au niveau national. Ce rapport s'appuie sur les observations et les données recueillies auprès d'intervenants de l'ensemble de la société canadienne et jette les bases d'une compréhension des risques de catastrophes liés aux trois dangers les plus coûteux auxquels les Canadiens sont confrontés : les tremblements de terre, les feux de forêt et les inondations. Il vise à mieux sensibiliser le public aux risques de catastrophes, à déceler les lacunes du système canadien de gestion des urgences à l'échelle nationale et à fournir des données probantes à l'appui des efforts fédéraux actuels en matière d'évaluation des risques et d'adaptation aux changements climatiques.

Des efforts ont également été déployés pour réduire stratégiquement les risques liés aux effets des changements climatiques. En 2022, le Canada a lancé sa première Stratégie nationale d'adaptation. L'un des principaux objectifs de cette stratégie est de veiller à ce que tous les systèmes d'infrastructure au Canada soient résilients aux changements climatiques et fassent l'objet d'une adaptation continue en fonction des répercussions futures, ceci afin de fournir des services fiables, équitables et durables à l'ensemble de la société canadienne. La Stratégie nationale d'adaptation vise à intégrer la résilience aux changements climatiques dans tous les nouveaux programmes fédéraux de financement des infrastructures et à garantir la publication d'orientations, de codes et de normes solides qui couvrent les principaux risques liés aux changements climatiques pour les principaux systèmes d'infrastructure publique.

Nouvelle-Zélande

L'engagement de la Nouvelle-Zélande envers l'amélioration de la résilience des infrastructures essentielles se reflète dans une série de stratégies et de politiques, notamment :

- la Stratégie Rautaki Hanganga o Aotearoa de 2022, soit la première stratégie d'infrastructure de la Nouvelle-Zélande, qui recommande d'adopter une approche coordonnée pour la gestion des risques en vue d'assurer la résilience des infrastructures;

- le premier Plan national d'adaptation de 2022 de la Nouvelle-Zélande, qui établit une série d'actions visant à permettre aux propriétaires d'infrastructures essentielles de prendre les mesures nécessaires pour assurer la résilience aux effets des changements climatiques et s'y adapter;

- la Stratégie nationale de sécurité de 2023, qui nomme la résilience des infrastructures essentielles comme un objectif clé relatif à la sécurité économique;

- la Stratégie nationale de cybersécurité, qui accorde la priorité aux efforts visant à aider les responsables d'infrastructures essentielles à renforcer la cyberrésilience et à assurer la sécurité de leurs systèmes.

Conformément aux orientations fournies dans ces stratégies nationales, la Nouvelle-Zélande s'efforce de réviser ses paramètres afin de mettre en place un système d'infrastructures essentielles plus résilient, notamment en :

- améliorant l'accès aux fonds et au financement pour les investissements dans les infrastructures;

- peaufinant l'approche du secteur des infrastructures en matière de gestion des biens pour améliorer la prestation de services;

- élaborant un cadre d'adaptation aux changements climatiques afin d'appuyer les décisions d'investissement, de faciliter le partage des coûts et de simplifier la gestion des risques climatiques;

- simplifiant les processus de gestion des ressources;

- élaborant une approche normalisée plus solide qui prend en compte les risques naturels dans l'aménagement du territoire.

La Nouvelle-Zélande envisage notamment d'adopter une nouvelle approche réglementaire axée sur les systèmes qui compléterait le régime réglementaire sectoriel existant en y ajoutant un ensemble complet d'exigences en matière de résilience pour toutes les infrastructures essentielles. L'objectif de cette réforme réglementaire est de mieux permettre aux systèmes d'infrastructures essentielles de gérer l'ensemble des risques et des menaces (y compris les

risques naturels de longue date, les effets des changements climatiques et le vaste éventail de menaces à la sécurité nationale). Les caractéristiques potentielles d'une nouvelle approche réglementaire qui ont fait l'objet d'une consultation en 2023 sont les suivantes :

- l'amélioration de l'échange d'information entre le gouvernement et les propriétaires d'infrastructures essentielles sur les risques, les menaces et les vulnérabilités, pour permettre aux responsables d'infrastructures de prendre des décisions éclairées en ce qui concerne les investissements;

- la collecte d'information par le gouvernement sur des questions telles que la propriété et le contrôle ainsi que les cyberincidents, pour accroître la sensibilisation du gouvernement aux vulnérabilités et aux menaces auxquelles sont exposées les responsables d'infrastructures essentielles;

- l'application de normes minimales de résilience en vue de réduire la probabilité d'événements défavorables qui pourraient perturber la prestation de services essentiels dans l'ensemble du système d'infrastructures essentielles et d'en minimiser les répercussions;

- en dernier recours, la mise en place de pouvoirs d'intervention accordés au gouvernement afin d'aider les responsables d'infrastructures essentielles à gérer les menaces importantes à la sécurité nationale (comme les cyberincidents).

De manière générale, en 2021, la *Overseas Investment Act* a été modifiée afin de renforcer la capacité du gouvernement de la Nouvelle-Zélande à gérer les risques pour la sécurité nationale et la sécurité publique posés par les investissements à l'étranger dans les infrastructures essentielles. Cela comprend la capacité de filtrer les investissements dans un certain nombre de secteurs d'infrastructures essentielles indépendamment de la valeur monétaire de l'investissement, ou du montant de la valeur nette obtenue.

Royaume-Uni

Depuis 2014, le Royaume-Uni a adapté et développé son approche en matière d'infrastructures essentielles nationales, à laquelle il avait ajouté en 2015 deux nouveaux secteurs, l'espace et la défense.

En 2018, le Royaume-Uni a élaboré une méthodologie de pensée systémique – le processus des criticités – pour identifier et catégoriser les infrastructures essentielles et leurs systèmes de soutien. Cette nouvelle approche normalisée permet une compréhension cohérente et commune des infrastructures les plus essentielles du Royaume-Uni.

Le Royaume-Uni s'est appuyé sur le processus des criticités en créant un nouvel outil numérique, la base de connaissances des infrastructures essentielles nationales (Critical National Infrastructure – CNI). Cette base de connaissances reprend les renseignements sur les criticités et permet aux responsables des risques de voir les infrastructures essentielles nationales sur une carte ou sous la forme d'un graphique en réseau et de visualiser les interdépendances et les relations entre les infrastructures afin de comprendre les risques et les impacts en cascade potentiels. Ces deux outils sont devenus essentiels, car ils aident le gouvernement du Royaume-Uni à fournir des conseils ciblés et pratiques afin de prendre des décisions plus éclairées en matière de gestion des risques.

En outre, le gouvernement a publié en décembre 2022 son cadre de résilience, qui a marqué la première définition de l'approche stratégique du gouvernement du Royaume-Uni en matière de résilience. Mettant l'accent sur les éléments fondamentaux de la résilience, ce cadre permet au gouvernement du Royaume-Uni de mieux prévenir et atténuer les risques auxquels la nation est confrontée, d'intervenir et de se rétablir. Dans ce cadre, le gouvernement s'est engagé à mettre en place des normes relatives aux infrastructures essentielles nationales d'ici 2030. La mise à jour du cadre de résilience de 2023 (publiée le 4 décembre 2023) met en évidence les progrès réalisés sur le plan de différents engagements en matière de résilience.

De plus, le Royaume-Uni a adopté la *Telecommunications (Security) Act 2021*, qui impose au secteur des télécommunications des obligations et des responsabilités plus strictes en matière de sécurité. Cette loi exige des fournisseurs de services de télécommunications qu'ils mettent en place des mesures pour identifier et défendre leurs réseaux contre les cybermenaces, ainsi que pour se préparer à tout risque futur. La même année, le Royaume-Uni a également adopté

la *National Security and Investment Act*, qui lui permet de déceler et de gérer les risques d'investissement pour la sécurité nationale, y compris en ce qui concerne les infrastructures essentielles.

Reconnaissant l'importance que les développements dans le domaine de la cybersécurité auront sur ses infrastructures essentielles nationales, le Royaume-Uni a mis en œuvre, en 2022, une stratégie nationale de cybersécurité (National Cyber Strategy 2022). Cette stratégie renforce la cybersécurité du Royaume-Uni afin que ce dernier puisse soutenir et promouvoir ses intérêts en toute confiance. En particulier, cette stratégie nationale fixe des objectifs pour les infrastructures essentielles nationales (dans les secteurs privé et public) afin de mieux comprendre et gérer les cyberrisques, tout en minimisant l'impact des cyberincidents.

En 2023, le Royaume-Uni a également dévoilé un nouveau cadre, le *New Position, Navigation and Timing*, qui comprend un plan d'intervention en cas d'indisponibilité des services actuels de positionnement, de navigation et de synchronisation (PNS), ainsi que la création d'un groupe gouvernemental spécialisé devant s'assurer que les services essentiels puissent être fournis sans interruption.

Finalement, deux nouvelles autorités techniques ont été créées pour soutenir et améliorer la sécurité et la résilience des infrastructures essentielles nationales. En 2016, le Royaume-Uni a créé le Centre national de cybersécurité (National Cyber Security Centre – NCSC) afin d'apporter une réponse nationale unifiée aux cybermenaces. En 2023, le Royaume-Uni a créé l'Autorité nationale de sûreté (National Protective Security Authority – NPSA), qui est chargée de fournir des conseils d'experts, fondés sur le renseignement, aux secteurs sensibles, y compris aux intervenants des infrastructures critiques.

États-Unis

Depuis 2014, la doctrine des États-Unis en matière de sécurité et de résilience des infrastructures essentielles a évolué vers une centralisation du département de la Sécurité intérieure et de l'Agence de cybersécurité et de sécurité des infrastructures (DHS/CISA) afin de gérer la coordination conjointe et intersectorielle au sein du gouvernement fédéral, d'établir des objectifs mesurables en matière de réduction des risques et de faire face aux menaces stratégiques urgentes.

En 2015, les États-Unis ont commencé à publier des plans sectoriels qui fixent des objectifs et des priorités pour chaque secteur en tenant compte de l'environnement de risque actuel, comme le lien entre la cybersécurité et la sécurité physique, l'interdépendance entre les différents secteurs, les risques associés aux changements climatiques, le vieillissement et l'obsolescence des infrastructures, et la nécessité d'assurer la continuité d'un effectif qui approche rapidement de la retraite[2].

En reconnaissance de la convergence des mondes physique et cybernétique, les États-Unis ont adopté en novembre 2018 la *Cybersecurity and Infrastructure Security Agency Act.* Cette dernière a désigné la National Protection and Programs Directorate (Direction de la protection nationale et des programmes – NPPD) du Department of Homeland Security (DHS) en tant que la Cybersecurity and Infrastructure Security Agency (CISA). La CISA emprunte une approche intégrée envers la sécurité en ciblant la collaboration avec les entreprises, les communautés et tous les ordres de gouvernement dans le but d'accroître la résilience des infrastructures essentielles américaines face aux menaces physiques et cybernétiques. La CISA, en tant qu'Agence de coordination nationale pour la sécurité et la résilience des infrastructures essentielles, coordonne les efforts nationaux de gestion des risques physiques envers les infrastructures essentielles et collabore avec les intervenants des secteurs public et privé qui possèdent et exploitent la majorité des infrastructures essentielles du pays.

La *Fiscal Year 2021 National Defense Authorization Act* a codifié les agences sectorielles (Sector-Specific Agencies), précédemment définies dans la Presidential Policy Directive 21 (PPD-21), en tant qu'Agences de gestion des risques sectoriels (Sector Risk Management Agencies – SRMA). Elle a aussi autorisé la collaboration entre le DHS et les SRMA pour protéger les infrastructures essentielles.

Le 30 avril 2024, la Maison Blanche a publié le National Security Memorandum (mémorandum de sécurité nationale – NSM-22) sur la sécurité et la résilience des infrastructures essentielles. Ce mémorandum s'appuie sur le travail important que le DHS/CISA et les agences du gouvernement fédéral ont entrepris en partenariat avec les communautés des infrastructures essentielles américaines depuis plus d'une décennie. Il remplace également la Presidential Policy Directive 21 (directive présidentielle – PPD-21) sur la sécurité et la résilience des infrastructures essentielles, cette dernière ayant été publiée il y a plus de dix ans et ayant pour

[2] Agence de cybersécurité et de sécurité des infrastructures – CISA, « 2015 Sector-Specific Plans: CISA », 15 décembre 2015, www.cisa.gov/2015-sector-specific-plans.

but de définir la politique nationale en matière de sécurité et de résilience des infrastructures essentielles. Le contexte de la menace a considérablement évolué depuis la publication de la PPD-21, passant de la lutte contre le terrorisme à la concurrence stratégique, aux progrès technologiques tels que l'intelligence artificielle, à la cyberactivité malveillante d'acteurs étatiques et à la nécessité d'une coordination internationale accrue. L'évolution des menaces et l'augmentation des investissements fédéraux dans les infrastructures essentielles des États-Unis ont rendu nécessaire la mise à jour de la PPD-21 et la publication du mémorandum.

Le NSM-22 œuvre à assurer que les infrastructures essentielles puissent contribuer à une économie forte et innovante, protéger les familles américaines et améliorer la résilience collective aux sinistres, renforçant ainsi la nation pour les générations à venir. Ce NSM prévoit en particulier :

- Attribuer à la DHS l'autorité de coordonner l'effort pangouvernemental visant la sécurisation des infrastructures essentielles aux États-Unis avec la CISA dans son rôle d'agence Coordonatrice nationale pour la sécurité et la résilience des infrastructures essentielles des États-Unis.. Le Secretary of Homeland Security devra soumettre au Président un Plan national de gestion des risques biennal résumant les efforts entrepris par le gouvernement américain afin d'atténuer les risques aux infrastructures essentielles du pays.

- Réaffirmer la désignation des 16 secteurs d'infrastructures essentielles et établir un département ou une agence fédéral responsable de la gestion des risques dans chacun de ces secteurs.

- Souligner l'importance des obligations de base en matière de sécurité et de résilience au-travers des secteurs des infrastructures essentielles, conformément à la National Cyber Strategy (stratégie nationale sur le cyberespace), soulignant les limites d'une approche de la gestion des risques volontaire dans le contexte des menaces actuel.

Définition des infrastructures essentielles et composition des secteurs

Si les définitions des infrastructures essentielles peuvent varier légèrement d'un pays du Groupe des 5 Partenaires à l'autre, les principaux points communs sous-jacents n'ont pas beaucoup changé depuis la publication de l'exposé commun en 2014.

> « Les infrastructures essentielles, qui sont également désignées par le terme 'infrastructures d'importance nationale', peuvent être définies de manière générale comme les systèmes, les biens, les installations et les réseaux qui fournissent des services essentiels et qui sont nécessaires à la sécurité nationale, à la sécurité économique, à la prospérité, à la santé et à la sécurité de leur pays. »

Cette définition continue de soutenir un cadre commun pour façonner l'engagement international en matière d'infrastructures essentielles.

Tous les pays du Groupe des 5 Partenaires continuent d'utiliser une approche sectorielle. Celle-ci facilite la collaboration sectorielle et intersectorielle entre les intervenants et peut être utilisée comme cadre analytique de haut niveau pour identifier les services et fonctions essentiels ainsi que les biens et les systèmes sur lesquels ils reposent. Certains pays identifient également des sous-secteurs d'infrastructures essentielles ou donnent la priorité à des biens et systèmes vitaux précis qui requièrent une plus grande protection.

L'émergence de menaces pour la sécurité nationale et économique et les progrès technologiques rapides ont incité les pays du Groupe des 5 Partenaires à élargir leur compréhension de ce qui constitue une infrastructure essentielle. Les domaines dans lesquels certains pays du Groupe des 5 Partenaires se sont concentrés et ont déployé des efforts supplémentaires sont notamment les suivants :

- Enseignement supérieur et recherche : Ce domaine joue un rôle primordial dans le développement d'un effectif qualifié, l'innovation technologique et la croissance économique. Il permet également de faire progresser les nouvelles technologies qui

sont indispensables aux infrastructures essentielles, telles que les soins de santé et les technologies de l'information;

- Stockage de données : Il s'agit d'un service primordial pour les particuliers, les entreprises et les administrations. Il permet également aux intervenants des infrastructures essentielles d'accéder aux renseignements indispensables, dont une grande partie est stockée dans le nuage;

- L'espace : La dépendance à l'égard des données et des services provenant des biens spatiaux (p. ex. les services de positionnement, de navigation et de synchronisation fournis par les systèmes mondiaux de navigation par satellite) et l'environnement de menace unique auquel sont confrontés ces biens ont incité certains membres du Groupe des 5 Partenaires à envisager de reconnaître l'espace comme un secteur à part entière.

La composition du secteur continuera d'évoluer en fonction des changements technologiques et des menaces, afin de garantir que les services les plus essentiels soient soumis aux exigences réglementaires appropriées et à d'autres mesures de protection.

Élaboration d'outils de d'échange d'information et de mécanismes de partenariat plus solides

Les pays du Groupe des 5 Partenaires accordent une grande importance aux partenariats et à l'échange de renseignements avec les propriétaires et les exploitants d'infrastructures essentielles, ainsi qu'avec leurs homologues nationaux, régionaux et locaux. L'utilisation de différents formats, tels que les forums de mobilisation et les plateformes d'échange de renseignements en ligne, permet aux intervenants de l'industrie et des gouvernements de collaborer sur des sujets tels que l'évaluation et la détermination de la criticité des infrastructures, l'établissement des dépendances intersectorielles et l'élaboration de pratiques exemplaires pour gérer les vulnérabilités face à des risques communs.

Les forums de mobilisation de l'industrie et des gouvernements favorisent l'établissement de partenariats et la mise en commun de l'information au sein de la communauté des infrastructures essentielles. Entre autres exemples, la Nouvelle-Zélande s'engage par

l'intermédiaire du groupe national Lifelines Council (New Zealand Lifelines Council – NZLC) et de ses groupes régionaux, ainsi que par des échanges de renseignements sectoriels facilités par le Centre national de cybersécurité (CNSC), tandis que le Royaume-Uni organise des forums sectoriels dirigés par les ministères responsables des infrastructures et systèmes nationaux essentiels ainsi que par la National Protective Security Authority – NPSA.

Les campagnes de sensibilisation et d'information, telles que le Mois de la sécurité des infrastructures aux États-Unis et en Australie, le Conseil consultatif des partenariats des infrastructures essentielles (Critical Infrastructure Partnership Advisory Council – CIPAC), le Comité consultatif de la cybersécurité (Cybersecurity Advisory Committee – CAC) et le Conseil consultatif sur l'infrastructure nationale (National Infrastructure Advisory Council – NIAC) des États-Unis, sont mises à profit pour promouvoir les ressources et les outils susceptibles d'aider les propriétaires et les exploitants d'infrastructures essentielles à renforcer la sécurité et la résilience de leurs infrastructures. Dans les années à venir, les pays du Groupe des 5 Partenaires entendent organiser collectivement un mois officiel de réflexion et d'action sur la sécurité des infrastructures essentielles.

Enfin, certains des pays du Groupe des 5 Partenaires utilisent des plateformes Web de mise en commun de l'information pour permettre à l'industrie et aux gouvernements de partager des renseignements opportuns dans un environnement sécurisé, comme la plateforme d'engagement TISN de l'Australie et la Passerelle des infrastructures essentielles du Canada.

Conclusion

Au cours de la dernière décennie, les pays du Groupe des 5 Partenaires ont dû adapter leurs approches politiques face à l'évolution rapide de l'environnement des risques et des menaces. Les changements climatiques, les cybermenaces et les risques grandissants pour la sécurité nationale ont conduit tous les pays du Groupe des 5 Partenaires à introduire ou à envisager des changements dans la définition des infrastructures essentielles ainsi que dans les outils réglementaires et non réglementaires mis à la disposition des fournisseurs d'infrastructures essentielles en vue d'accroître leur résilience. On a ainsi reconnu qu'il est essentiel d'investir collectivement dans la résilience des infrastructures essentielles, faute de quoi l'interruption ou la perte de services pourrait s'avérer inutilement coûteuse.

Les pays du Groupe des 5 Partenaires continuent de partager leurs connaissances, leur expérience et leur expertise sur des questions d'intérêt commun, ce qui permettra à la communauté de mieux répondre aux risques croissants et évolutifs. La solidité des relations entre les membres du Groupe des 5 Partenaires s'est avérée précieuse, car elle permet de continuer d'apprendre les uns des autres sur des questions clés d'intérêt mutuel.

Annexe A : Fiche d'information sur les infrastructures essentielles des pays du Groupe des 5 Partenaires

Australie

Définition des infrastructures essentielles

Les infrastructures essentielles sont définies comme étant les installations physiques, les systèmes, les biens, les chaînes d'approvisionnement, les technologies de l'information et les réseaux de communication qui, s'ils étaient détruits, dégradés, compromis ou rendus inaccessibles pour une période prolongée, auraient une incidence importante sur le bien-être social ou économique du pays, de ses États ou de ses territoires, ou affecteraient la capacité de l'Australie d'assurer sa défense ou sa sécurité nationale[3].

Liste des secteurs

Alimentation et épicerie

Énergie

Enseignement supérieur et recherche

Communications

Industrie de la défense

Services d'eau et d'égout

Services financiers et marchés

Soins de santé et médecine

Stockage ou traitement des données

Technologie spatiale

Transports

[3] « Critical Infrastructure Resilience Strategy ». Site Web du Cyber and Infrastructure Security Centre, ministère de l'Intérieur et gouvernement australien, 2023, www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/critical-infrastructure-resilience-strategy.

Approche politique de la gestion de la sécurité et de la résilience des infrastructures essentielles

En Australie, la sécurité des infrastructures essentielles est régie par la loi. Les politiques et les cadres relatifs aux infrastructures essentielles sont gérés par le ministère de l'Intérieur, certains aspects de la réglementation relevant d'autres agences gouvernementales australiennes.

Le ministère de l'Intérieur est responsable de la *Security of Critical Infrastructure Act 2018 - SOCI Act*), qui est la principale loi relative à la sécurité des infrastructures essentielles. D'autres cadres de sécurité des infrastructures essentielles ont été mises en place. Notons :

- *Aviation Transport Security Act 2004 (Loi de 2004 sur la sécurité du transport aérien)*, qui protège l'infrastructure de l'aviation civile australienne contre les actes d'ingérence illicite (principalement le terrorisme);

- la *Maritime Transport and Offshore Facilities Security Act 2003 (loi de 2003 sur la sécurité des transports maritimes et des installations hauturières)*, qui protège les transports maritimes civils et les installations hauturières de l'Australie contre les actes d'ingérence illicite (principalement le terrorisme);

- la partie 14 de la *Telecommunications Act 1997 (loi de 1997 sur les télécommunications)*, qui formalise les accords d'échange de renseignements entre le gouvernement et l'industrie afin de mieux protéger les réseaux australiens contre les actes de sabotage, d'espionnage et d'ingérence étrangère.

Programme de mobilisation des intervenants et mesures de soutien

L'engagement avec l'industrie est au cœur du modèle australien de sécurité et de résilience des infrastructures essentielles. Depuis la fin de l'année 2022, l'Australie a entrepris de développer considérablement ses relations avec les propriétaires et les exploitants afin de les aider à gérer les risques et à mieux se conformer à la réglementation. Elle a notamment accueilli la première conférence australienne sur la cybersécurité et la sécurité des infrastructures, ainsi que le Mois de la sécurité des infrastructures essentielles, mis à l'essai de nouveaux supports et formats tels que des webinaires, des assemblées générales et des balados, mis en place une présence dédiée aux médias sociaux pour les propriétaires et les

exploitants, tenu des événements en personne dans le cadre d'une communauté des pratiques exemplaires, et planifié un programme d'engagement avec les dirigeants d'entreprise, les administrateurs de société et les membres de divers conseils d'administration.

Le réseau TISN est une plateforme permettant à tous les niveaux de l'industrie et du gouvernement australiens de discuter et d'améliorer la sécurité et la résilience des infrastructures essentielles. En plus d'être une plateforme en ligne sécurisée, le réseau TISN comprend des groupes sectoriels qui permettent aux propriétaires et aux exploitants d'infrastructures essentielles d'échanger des renseignements sur les menaces et les vulnérabilités et de collaborer en vue de prendre des mesures appropriées pour atténuer les risques et renforcer la résilience. Le nombre de membres du réseau TISN a doublé en 2023.

L'Australie publie régulièrement une série de documents d'évaluation des risques afin d'aider les propriétaires et les exploitants à comprendre l'environnement des menaces et de les encourager à réfléchir de manière critique à leur exposition aux risques.

Le programme d'exercices de l'Office national australien de la cybersécurité (National Office of Cyber Security – NOCS) organise des exercices en priorité avec les secteurs essentiels. Ces exercices sont conçus pour mettre à l'épreuve les processus établis en cas d'incident de cybersécurité ayant un impact sur l'industrie et nécessitant une interaction avec le gouvernement pour gérer les conséquences qui en découlent. Il s'agit d'exercices de collaboration et de discussion qui démontrent les possibilités d'amélioration et d'harmonisation en cas d'incident.

Canada

Définition des infrastructures essentielles

La Stratégie nationale sur les infrastructures essentielles du Canada définit les infrastructures essentielles comme l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sécurité, la sûreté ou le bien-être économique des Canadiens ainsi que l'efficacité du gouvernement. Il peut s'agir d'infrastructures autonomes ou caractérisées par des interdépendances au sein d'une province ou d'un territoire, entre eux ou au-delà des frontières du pays.

Liste des secteurs

Alimentation
Eau
Énergie et services publics
Finances
Gouvernement
Santé
Secteur manufacturier
Sécurité
Technologies de l'information et des communications
Transports

Approche politique de la gestion de la sécurité et de la résilience des infrastructures essentielles

L'approche actuelle du Canada repose sur la *Stratégie nationale sur les infrastructures essentielles* et sur les plans d'action triennaux qui l'accompagnent. Publiée en 2009, la Stratégie nationale a défini les infrastructures essentielles et créé dix secteurs. Sécurité publique Canada assure une fonction centrale de gouvernance et de coordination des politiques, tandis que les réseaux sectoriels individuels – un groupe d'acteurs publics et privés au sein d'un secteur donné – sont organisés par les ministères et organismes fédéraux responsables. L'approche du Canada en matière de sécurité et de résilience des

infrastructures essentielles repose sur des actions et une participation volontaires et collaboratives, allant de l'échange d'information aux outils et aux programmes.

Programme de mobilisation des intervenants et mesures de soutien

Le Canada dispose de divers programmes de mobilisation et de soutien à l'intention des intervenants des infrastructures essentielles. Le Canada travaille notamment en étroite collaboration avec des partenaires internes et externes pour améliorer la résilience des infrastructures essentielles. En voici quelques exemples :

- Collaboration entre les secteurs public et privé au moyen de divers mécanismes de mobilisation tels que le Forum national intersectoriel qui favorise la mise en commun de l'information entre les réseaux sectoriels;
- Collaboration sur des questions multirisques et intersectorielles entre les membres de groupes de travail des ministères fédéraux responsables et des gouvernements fédéral, provinciaux et territoriaux;
- Communication d'information aux intervenants pour soutenir les mesures de gestion des risques, notamment par l'intermédiaire de la Passerelle des infrastructures essentielles du Canada, une plateforme sécurisée d'échange de renseignements avec des partenaires internes et externes en vue de renforcer la sécurité des infrastructures essentielles, entre autres au moyen d'une formation et d'exposés sur les menaces;
- Exercices visant à soutenir les efforts de planification et d'intervention en matière d'infrastructures essentielles;
- Évaluations en ligne et sur place pour déterminer et corriger les vulnérabilités et pour aider les propriétaires et les exploitants à améliorer la sécurité et la résilience de leur organisation dans une perspective tous risques.

Nouvelle-Zélande

Définition des infrastructures essentielles

En janvier 2024, la Nouvelle-Zélande n'avait aucune définition légale des infrastructures essentielles. Une proposition de définition est incluse dans la liste des entités actuellement considérées comme des services publics de base (« lifeline utilities ») à l'annexe 1 de la *(Civil Defence Emergency Management Act 2022 (Loi de 2002 sur la gestion des urgences en matière de protection civile)*.

Compte tenu de l'évolution du contexte technologique et des risques, le gouvernement néo-zélandais envisage d'adopter une nouvelle définition des infrastructures essentielles fondée sur des principes dans le cadre de travaux plus larges visant à renforcer la résilience du système d'infrastructures essentielles du pays.

Liste des secteurs

Eau (eau douce, eaux usées et eaux pluviales)
Énergie
Radiodiffusion
Télécommunications
Transports

Approche politique de la gestion de la sécurité et de la résilience des infrastructures essentielles

La Nouvelle-Zélande réglemente les responsables d'infrastructures critiques, secteur par secteur. Ces régimes réglementaires sectoriels ont tendance à mettre l'accent sur la sûreté, la sécurité et l'accessibilité financière, qui se recoupent souvent avec la résilience.

Il existe des exceptions limitées à cette approche sectorielle, notamment en ce qui concerne les mesures et interventions en cas d'urgence. La *Civil Defence Emergency Management Act 2022 (loi de 2002 sur la gestion des urgences en matière de protection civile*[4]*)* exige que les entreprises de services publics de base [traduction] « veillent à ce qu'elles soient en mesure de

[4] Ministère de l'Intérieur. *Civil Defence Emergency Management Act 2002* – Lois de la Nouvelle-Zélande, ministère de l'Intérieur, 2002, www.legislation.govt.nz/act/public/2002/0033/51.0/DLM149789.html.

fonctionner dans toute la mesure du possible, même si c'est à un niveau réduit, pendant et après une situation d'urgence ». Cette obligation est toutefois vague, non mesurable et inapplicable.

Programme de mobilisation des intervenants et mesures de soutien

Les agences gouvernementales néo-zélandaises aident les propriétaires et les exploitants d'infrastructures essentielles à se préparer aux risques et aux menaces potentiels et à en atténuer les conséquences en les sensibilisant et en renforçant leurs capacités. En voici quelques exemples :

- L'Agence nationale de gestion des urgences (National Emergency Management Agency – NEMA) joue un rôle de premier plan dans la réduction des risques. Elle aide notamment les entreprises de services publics à gérer les mesures d'urgence, d'intervention et de rétablissement;

- L'Institut national de recherche sur l'eau et l'atmosphère (National Institute of Water and Atmospheric Research) et la Commission des tremblements de terre (Earthquake Commission), Toka Tū Ake EQ, fournissent des renseignements sur l'exposition aux risques naturels, y compris des données géotechniques et des données en temps réel sur les risques naturels;

- Le Centre national de cybersécurité (National Cyber Security Centre - NCSC), qui fait partie du Bureau de la sécurité des communications du gouvernement néo-zélandais, collabore directement avec les propriétaires et les exploitants d'infrastructures essentielles, en leur fournissant des conseils, des alertes sur les menaces et des capacités techniques spécialisées afin d'améliorer leur cyberrésilience. Le NCSC aide également les propriétaires et les exploitants d'infrastructures essentielles à intervenir en cas d'incident de cybersécurité important et à se rétablir.

Outre le soutien apporté par les agences gouvernementales, le New Zealand Lifelines (Utilities) Council – NZLC (Conseil néo-zélandais des lignes de vie en services publics), composé de représentants du gouvernement et du secteur privé, se concentre à mettre en relation les propriétaires et les exploitants d'infrastructures essentielles dans tous les secteurs et à faciliter leur engagement avec une série d'intervenants qui œuvrent déjà à l'amélioration de la résilience des infrastructures néo-zélandaises.

Royaume-Uni

Définition des infrastructures essentielles

Infrastructures essentielles nationales : La définition officielle adoptée par le gouvernement du Royaume-Uni est la suivante : [traduction] « Les éléments essentiels de l'infrastructure (à savoir les biens, les installations, les systèmes, les réseaux ou les processus et les travailleurs essentiels qui les exploitent et y contribuent), dont la perte ou la compromission pourrait entraîner :

- un impact préjudiciable majeur sur la disponibilité, l'intégrité ou la prestation de services essentiels – y compris les services dont l'intégrité, si elle était compromise, pourrait causer de lourdes pertes de vies humaines ou des blessures – en tenant compte des répercussions économiques ou sociales considérables;

- un impact significatif sur la sécurité nationale, la défense nationale ou le fonctionnement de l'État. »

Liste des secteurs

Alimentation
Communications
Défense
Eau
Énergie
Énergie nucléaire civile
Espace
Finances
Gouvernement
Santé
Services d'urgence
Substances chimiques
Transports

Approche politique de la gestion de la sécurité et de la résilience des infrastructures essentielles

Le Bureau du Cabinet (Cabinet Office) du Royaume-Uni et les administrations décentralisées respectives sont chargés de fournir une gouvernance globale et des orientations stratégiques intersectorielles pour leur pays. En ce qui concerne la surveillance des infrastructures essentielles nationales au Royaume-Uni, le gouvernement supervise un modèle décentralisé et dirigé selon le cas par l'un ou l'autre des secteurs. Chaque secteur est supervisé par le ministère responsable compétent, tandis que différents intervenants, tels que le Bureau du Cabinet, les autorités techniques nationales, les organismes de réglementation, les propriétaires et les exploitants, ainsi que les administrations décentralisées, jouent tous un rôle précis dans le fonctionnement des infrastructures essentielles nationales du Royaume-Uni.

Étant donné que les ministères responsables sont responsables de leur secteur, ce sont eux qui élaborent leurs propres orientations, réglementations et législations afin de contribuer à la protection et au renforcement de la sécurité et de la résilience. Le Bureau du Cabinet conduit également la mise en œuvre de projets de loi, de législations, de stratégies et de cadres globaux visant à soutenir l'ensemble des secteurs des infrastructures essentielles nationales et à assurer leur cohérence et leur homogénéité.

Considérant que le Royaume-Uni est composé de quatre corps législatifs et exécutifs, chacun disposant d'un éventail de pouvoirs différent, l'approche en matière d'infrastructures essentielles nationales peut varier entre les administrations décentralisées et le gouvernement du Royaume-Uni. Toutefois, les quatre administrations de l'Écosse, du Pays de Galles, de l'Irlande du Nord et de l'Angleterre travaillent en partenariat pour garantir la complémentarité des approches politiques et de la législation. L'approche politique des infrastructures essentielles nationales est nuancée, dans la mesure où certains domaines sont partiellement réservés (au gouvernement du Royaume-Uni), et où certains aspects et secteurs sont dévolus (aux administrations de l'Écosse, du Pays de Galles et de l'Irlande du Nord).

Programme de mobilisation des intervenants et mesures de soutien

La mobilisation des secteurs des infrastructures essentielles nationales est menée par les ministères responsables et les administrations décentralisées. Les ministères responsables peuvent adopter des approches différentes selon les secteurs, mais comprennent des forums industriels, des engagements individuels ou des orientations d'une personne à plusieurs autres. Les autorités techniques (telles que le Centre national de cybersécurité et l'Autorité nationale de sûreté) fournissent des orientations et des conseils sur les pratiques exemplaires en matière de sécurité aux propriétaires et aux exploitants de systèmes d'infrastructures essentielles nationales, notamment en organisant des forums d'échange de renseignements avec l'industrie.

En juin 2023, le gouvernement du Royaume-Uni a publié le registre national des risques le plus transparent qui soit, lequel comprend tous les renseignements contenus dans l'évaluation des risques pour la sécurité nationale, à moins qu'ils ne puissent être divulgués pour des raisons de sécurité nationale ou des motifs commerciaux. Ce document vise à fournir des renseignements détaillés aux personnes ayant des responsabilités formelles en matière de planification d'urgence aux niveaux national et local. Cette transparence en matière de risques signifie que tout un chacun, des spécialistes de la gestion du risque aux universitaires, peut maintenant voir directement comment le gouvernement du Royaume-Uni identifie et évalue les risques.

Dans sa déclaration annuelle de 2023, le gouvernement du Royaume-Uni a également annoncé la création d'une nouvelle académie de la résilience (United Kingdom Resiliency Academy – UKRA). Celle-ci assurera la formation et jouera un rôle de premier plan dans l'établissement de normes pour l'apprentissage de la résilience. Elle élaborera et mettra de l'avant des documents d'orientation sur les bonnes pratiques et réunira régulièrement les praticiens de la résilience pour encourager la collaboration.

États-Unis

Définition des infrastructures essentielles

En vertu de la *USA Patriot Act of 2001 (Loi américaine sur le patriotisme de 2001)*, les États-Unis définissent les infrastructures essentielles comme étant [traduction] « les systèmes et les biens, physiques ou virtuels, cruciaux pour les États-Unis au point que l'incapacité ou la destruction de ces systèmes et biens auraient un effet dévastateur sur la sécurité du pays et de l'économie nationale, sur la santé ou la sécurité publiques nationales ou sur toute combinaison de ces éléments[5] ».

Liste des secteurs

Alimentation et agriculture
Barrages
Base industrielle de la défense
Communications
Eau potable et eaux usées
Énergie
Fabrication de produits essentiels
Installations commerciales
Installations et services gouvernementales
Produits chimiques
Réacteurs, matières et déchets nucléaires
Services d'urgence
Services financiers
Soins de santé et santé publique
Systèmes de transport
Technologies de l'information

[5] « Analysis of the USA PATRIOT Act ». USA PATRIOT ACT – Titre 10, article 1016, 2004, www.seattlewebcrafters.com/usapatriotact/t10sec1016.php.

Approche politique de la gestion de la sécurité et de la résilience des infrastructures essentielles

Aux États-Unis, la sécurité des infrastructures essentielles repose sur un partenariat entre le gouvernement et le secteur privé qui combine la mise en œuvre de mesures politiques, réglementaires et volontaires pour gérer les risques. Des entités publiques et privées possèdent et exploitent les infrastructures essentielles du pays. Les efforts de protection des infrastructures essentielles nationales requièrent une approche pangouvernementale ainsi qu'une coordination et une collaboration entre de multiples intervenants intergouvernementaux et industriels. La *Cybersecurity and Infrastructure Security Agency Act of 2018 (Loi de 2018 sur l'agence de cybersécurité et de sécurité des infrastructures)* exige du directeur de l'Agence de la cybersécurité et de la sécurité des infrastructures (Cybersecurity and Infrastructure Security Agency – CISA) qu'il coordonne un effort national de protection contre les risques liés aux infrastructures essentielles, conformément à un plan national global (actuellement le National Infrastructure Protection Plan 2013).

La responsabilité de la réalisation des objectifs politiques est répartie entre plusieurs agences fédérales dotées d'une responsabilité statutaire en tant qu'agences de gestion des risques sectoriels. Chacun des 16 secteurs d'infrastructures essentielles est doté d'une agence sectorielle de gestion des risques dont les pouvoirs, l'expertise et les capacités sont adaptés au secteur qu'elle représente.

Ce cadre de sécurité des infrastructures essentielles fournit un modèle de partenariat collaboratif pour consolider l'information et l'expertise du gouvernement et de l'industrie. En collaboration avec les divers secteurs d'infrastructures essentielles, le gouvernement fédéral assure la sécurité et la résilience des infrastructures nationales en utilisant des outils et des ressources tels que l'échange bidirectionnel de renseignements sur les menaces, les exercices en conditions réelles, la formation et les orientations en matière d'intervention en cas d'incident, les évaluations et les analyses des risques menées par le gouvernement fédéral et l'expertise en la matière. La mobilisation active des partenaires des secteurs public et privé est à l'origine de ce cadre national et des outils et ressources qui y sont associés, sur lesquels ces partenaires s'appuient pour assurer la sécurité de leurs systèmes et de leurs biens.

Programme de mobilisation des intervenants et mesures de soutien

Les États-Unis ont élaboré et mis en œuvre de nombreux programmes d'échange de renseignements afin de promouvoir les ressources et les outils qui aident ses partenaires à renforcer la sécurité et la résilience. Au nombre de ces programmes, citons des campagnes de sensibilisation et d'information telles que le Cybersecurity Awareness Month (Mois de la sensibilisation à la cybersécurité) annuel, le Critical Infrastructure Security and Resilience Month (Mois de la sécurité et résilience des infrastructures essentielles) annuel et des programmes de sensibilisation nationaux plus vastes qui proposent des outils aux partenaires. Ces programmes permettent l'échange de renseignements importants entre le secteur privé, les gouvernements des États et les administrations locales, tribales et territoriales.

Les États-Unis, par l'intermédiaire de la CISA, entretiennent des relations avec des partenaires internationaux afin de promouvoir la mise en commun de l'information, les pratiques exemplaires en matière de cybersécurité et les modèles de partenariat à l'échelle planétaire, car chacun sait que les auteurs de menace en matière de cybersécurité ne se limitent pas aux frontières géographiques. En outre, l'initiative Cyber Innovation Fellows permet à des experts techniques de haut niveau issus du secteur privé de poser leur candidature pour faire partie des équipes de la CISA chargées de la cybersécurité, dans l'intérêt de leur développement professionnel et de l'espace de mission grandissant de la CISA[6]. Les États-Unis disposent également de divers conseils et comités de partenariat public-privé qui travaillent à l'amélioration de la sécurité et de la résilience des infrastructures essentielles du pays.

[6] CISA. « Cyber Innovation Fellows Initiative ». CISA, 2023, www.cisa.gov/topics/partnerships-and-collaboration/cyber-innovation-fellows-initiative.