Programme initiatives en cybersécurité
Ensemble pour sécuriser le milieu canadien de la recherche et de l'éducation

Kevin Parent | Webinaire de CICan | Le 31 mars 2021

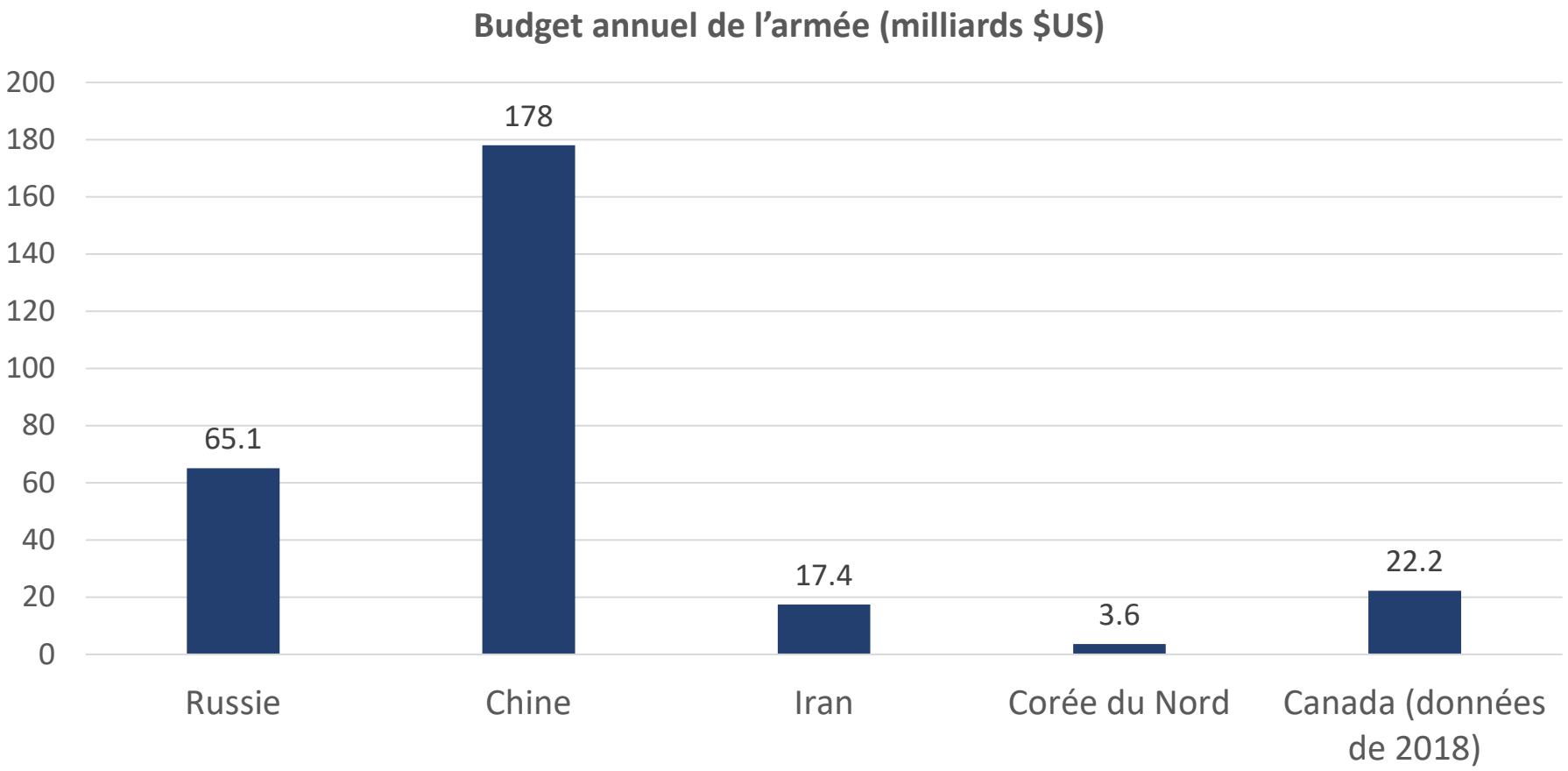
Énoncé du problème

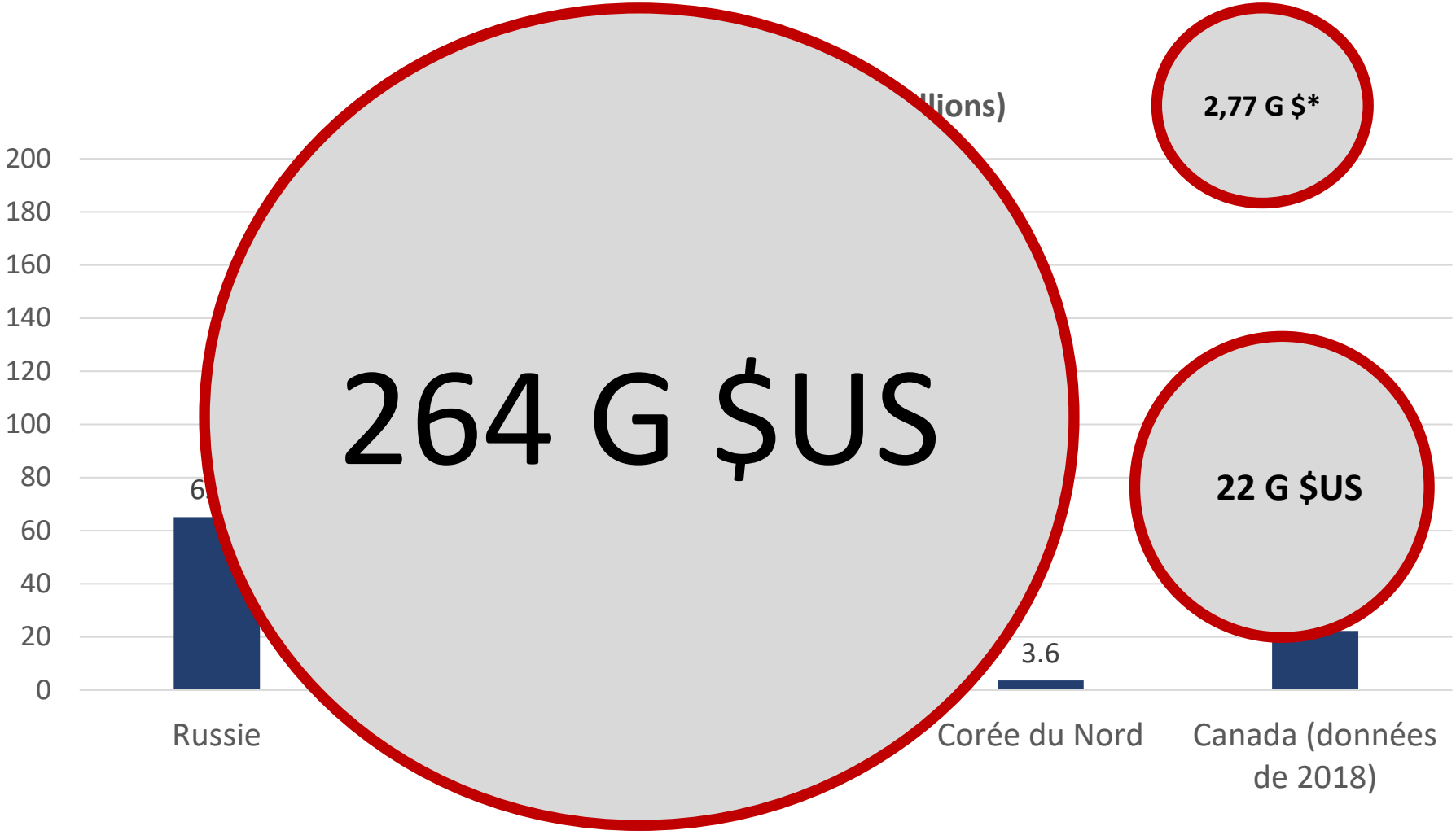
« …les activités hostiles des acteurs étatiques, peu importe leur forme, **font peser une lourde menace sur la prospérité et la souveraineté du Canada.**

Depuis de nombreuses années, le SCRS observe la tenue incessante d'**activités liées à la menace parrainées par des États**, activités qui sont aujourd'hui de plus en plus fréquentes et sophistiquées… Les nouvelles technologies [en] biopharmaceutique, [en] santé, [en] intelligence artificielle, les technologies quantiques, les technologies marines et l'aérospatiale sont plus visées que d'autres **parce qu'elles sont en grande partie créées dans les universités** et les petites entreprises… »

David Vigneault
Directeur, SCRS
9 février 2021

La menace, remise en contexte





*Budget d'exploitation annuel de la plus grande université canadienne en 2019-2020

Une réalité collective

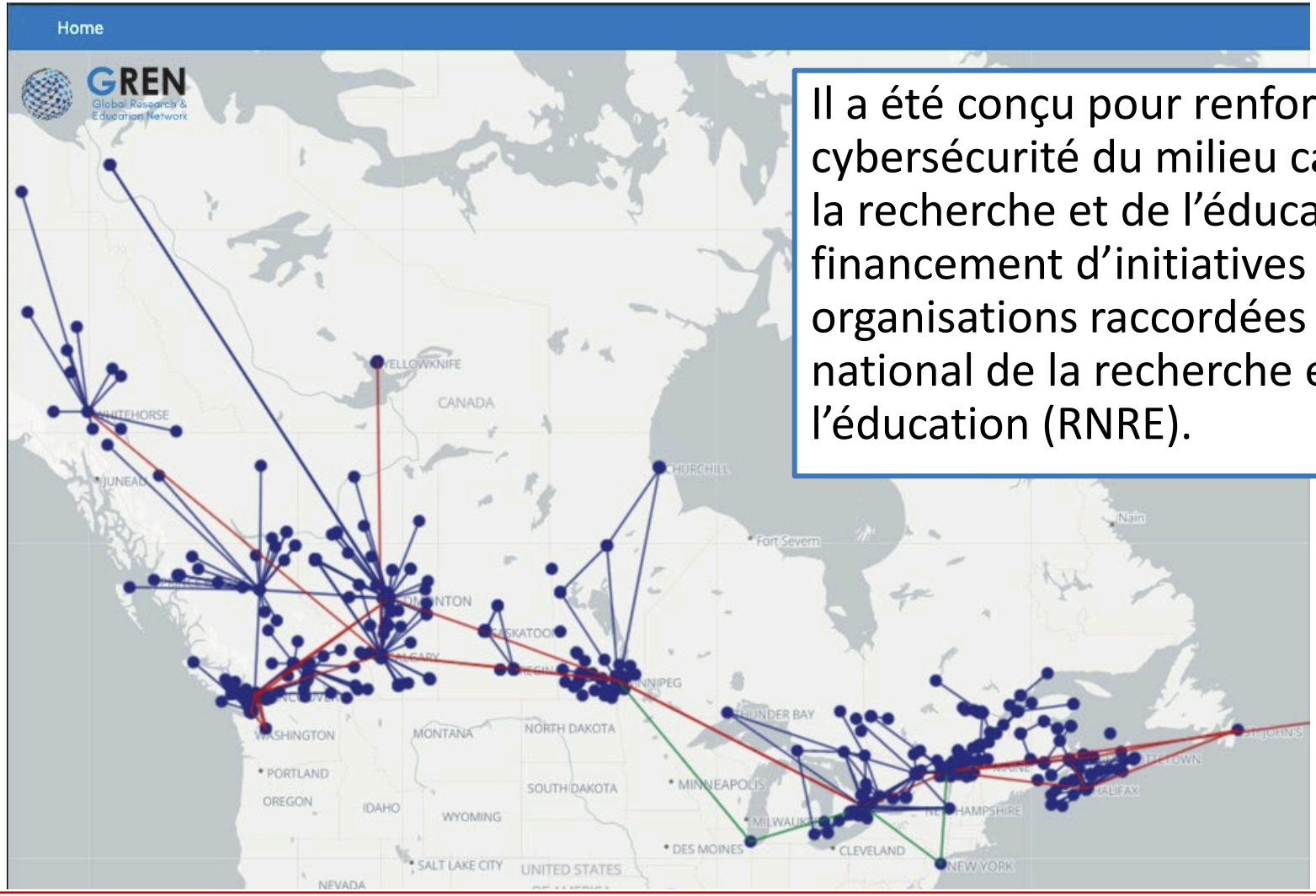
- Nous sommes tous connectés, que ce soit physiquement ou par la collaboration.
- Chaque organisation, chaque dispositif connecté est susceptible d'être piraté.
- Cette connectivité fait en sorte que la chaîne est aussi solide que son maillon le plus faible.
- La cybersécurité n'est pas qu'un problème IT : c'est une priorité de l'organisation.
- Une approche nationale en cybersécurité n'est réalisable que si le secteur entier s'harmonise et coordonne ses efforts.

Une fois sécurisé, le secteur sera plus solide que la somme de ses parties.

Une brèche en cybersécurité

- Il n’y a aucune honte à se faire pirater!
- Une cyberattaque est une activité illicite perpétrée par des criminels.
- Si on vous pirate, signalez-le. NE VERSEZ aucune rançon!
- Céder au chantage, c’est encourager plus d’attaques. Le pirate a déjà accès à vos systèmes. Rien ne dit qu’il tiendra parole une fois la rançon payée.
- Faites appel aux forces de l’ordre : à votre partenaire du RNRE, CCCS, CanSSOC. Les ressources pour vous venir en aide ne manquent pas. Vous n’êtes pas seul.

Le programme Initiatives en cybersécurité (PIC)



Il a été conçu pour renforcer la cybersécurité du milieu canadien de la recherche et de l'éducation par le financement d'initiatives dans les organisations raccordées au Réseau national de la recherche et de l'éducation (RNRE).

La vision : un Canada plus sûr

La collaboration de nos partenaires est indissociable de l'approche et de la stratégie élaborées pour le programme.

Avantages pour l'organisation admissible

- Élargir l'infrastructure de cybersécurité
- Jauger l'impact des initiatives en cybersécurité sur l'organisation
- Collaborer avec un bassin national de spécialistes en sécurité du secteur R-E
- Renforcer les compétences et l'expertise de l'équipe de sécurité de l'organisation : le programme comprend un volet formation et soutien technique

Sécuriser l'organisation davantage

Sans coûts directs

Les trois premières initiatives

cira

D-ZONE DNS FIREWALL

Financement de la mise en œuvre, du soutien et de la formation dans plus de 200 organisations admissibles

CANSSOC Threat Feed

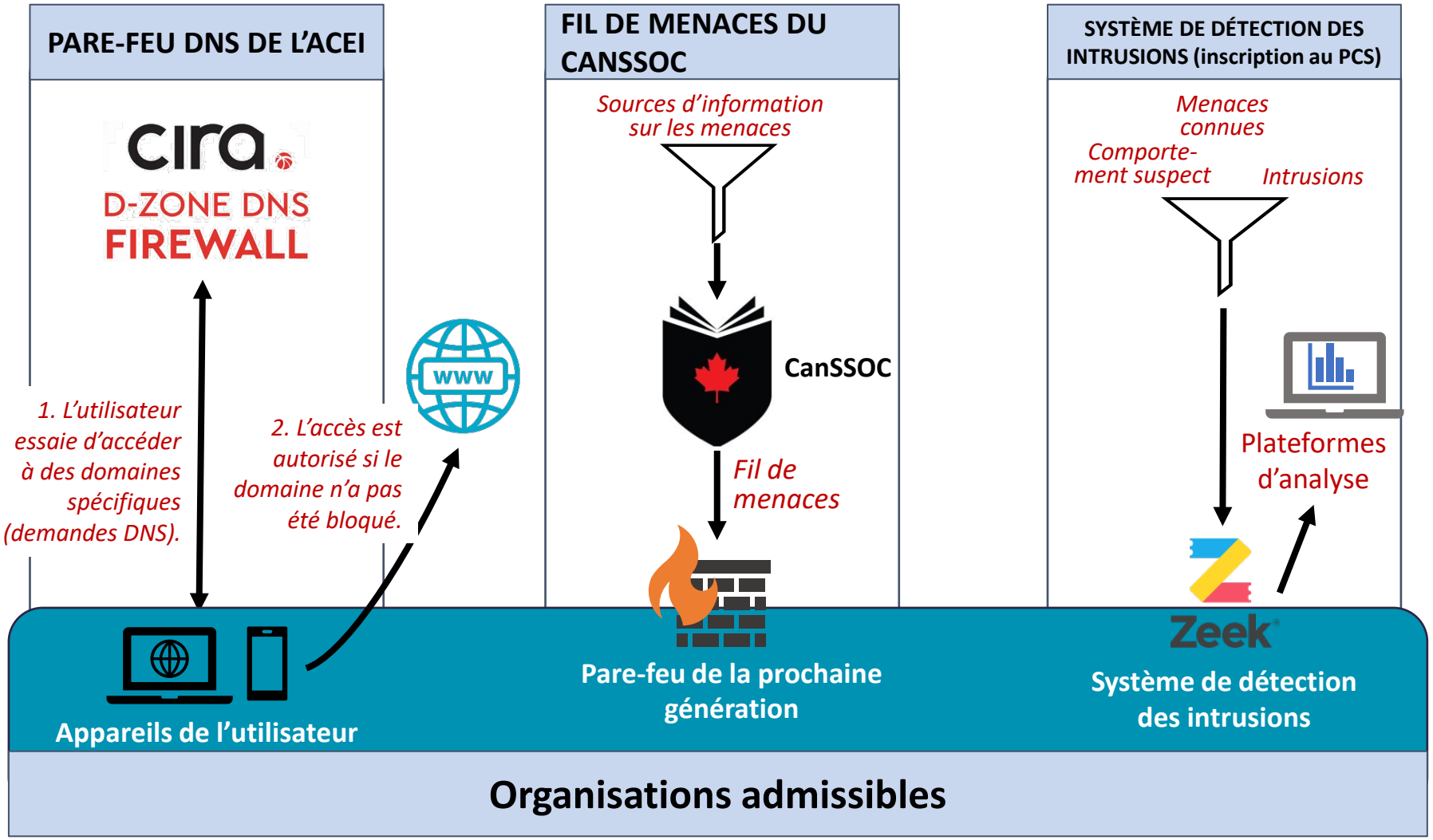
Financement de la mise en œuvre, du soutien et de la formation dans plus de 200 entreprises admissibles

Intrusion Detection System *(Join the JSP)*

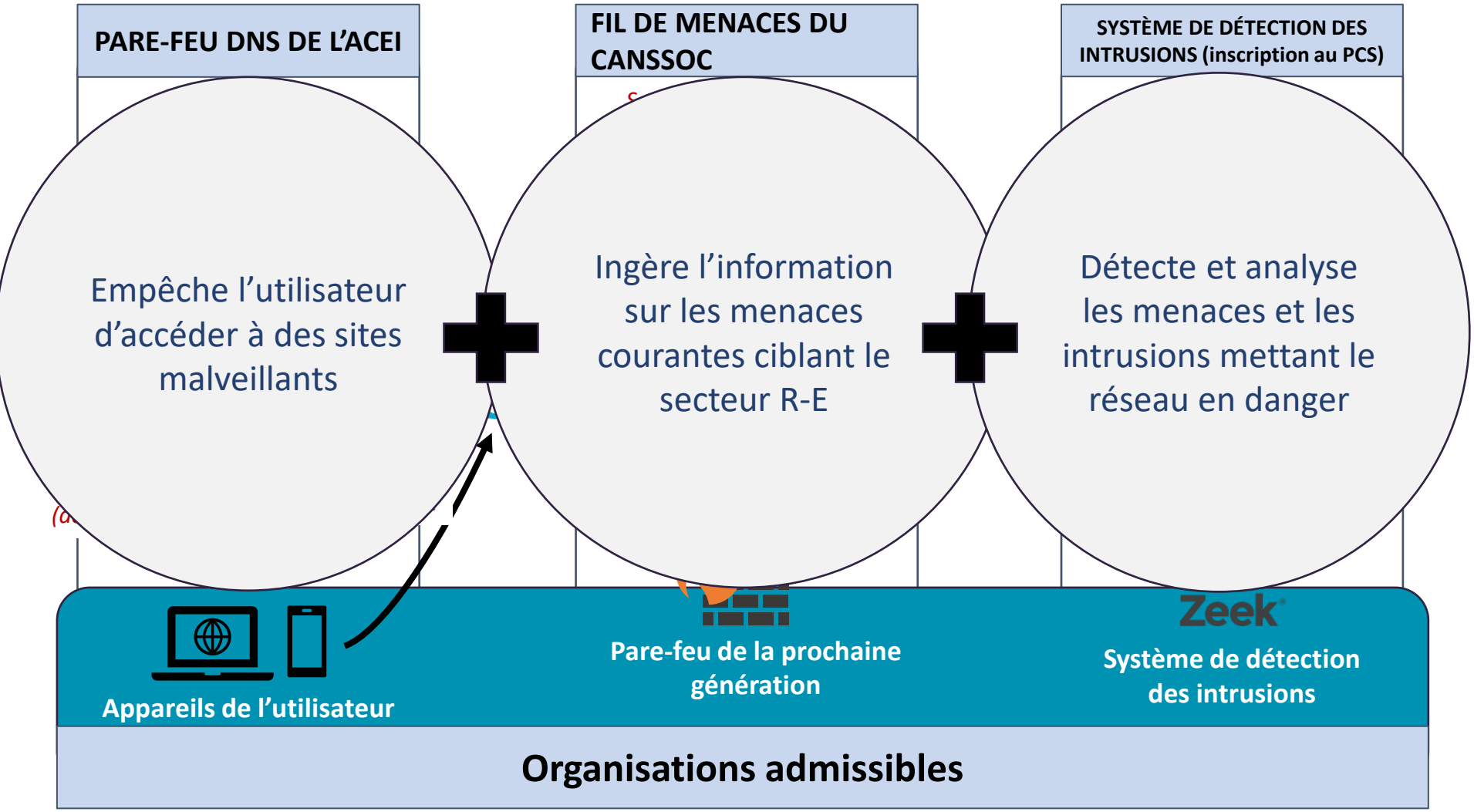
Financement de la mise en œuvre, du soutien et de la formation dans les organisations admissibles non inscrites au Projet conjoint en sécurité (PCS)

Les initiatives subventionnées sont conçues pour s'intégrer et renforcer la cybersécurité localement, ce qui rendra l'ensemble du secteur plus sûr.

Comment les initiatives s'harmonisent



Comment les initiatives s'harmonisent



Qui choisit les initiatives qui seront financées?

Commission consultative en cybersésurité

Elle se compose de chefs de file des universités, collèges, écoles polytechniques, cégeps, organismes sans but lucratif et organisations privées du Canada.

Rôle

- Prôner une approche nationale coordonnée à la cybersésurité dans le secteur R-E
- Orienter les initiatives financées dans le cadre du programme

Gouvernance du programme

Commission consultative en cybersécurité

- Elle oriente les collaborations nationales en cybersécurité.
- Elle dispense des conseils sur la stratégie, l'évolution et les résultats du programme.

Comité de la fiabilité et des identités

Il oriente l'évolution des services sectoriels de gestion des identités, y compris la Fédération canadienne d'accès.

Comité technique en cybersécurité

Il dispense des conseils et formule des recommandations sur les aspects techniques de la cybersécurité qui ont un impact sur les initiatives de CANARIE.

Comité de déploiement des initiatives en cybersécurité

Il recueille les commentaires et fournit de l'information sur les activités des institutions afin de faciliter la conception, l'exécution et l'adoption du programme.

La Commission consultative en cybersécurité et ses comités permanents

Commission consultative en cybersécurité

- Elle oriente les collaborations nationales en cybersécurité.
- Elle dispense des conseils sur la stratégie, l'évolution et les résultats du programme.

Comité de la fiabilité et des identités

Il oriente l'évolution des identités du secteur, y Fédération canadienne d'accès.

Comité technique en cybersécurité

Il dispense des conseils et impact sur les initiatives de CANARIE.

Comité de déploiement des initiatives en cybersécurité

Il recueille les commentaires sur les activités des conception, l'exécution et l'adoption du programme.

Groupe de travail sur la quantification de la cybersécurité

Cadre d'investissement dans la cybersécurité

La participation des membres de CICan en un clin d'œil

> 102 organisations admissibles

- Elles sont connectées au Réseau national de la recherche et de l'éducation (RNRE) du Canada.
- Elles font partie des organisations membres d'un partenaire du RNRE ET sont connectées à son réseau grâce à un réseau autonome.
- Établissement d'enseignement postsecondaire, installation de recherche non fédérale ou centre d'excellence

> 85 sont déjà inscrites au PIC et prêtes à profiter des initiatives subventionnées

- 73 organisations utilisent déjà le pare-feu DNS de l'ACEI

Comment participer

Terminologie

RNRE

- Réseau national de la recherche et de l'éducation – réseau pancanadien exploité par CANARIE et ses partenaires des provinces et des territoires

Partenaire du RNRE

- Un des 13 partenaires provinciaux et territoriaux du RNRE ou CANARIE

Organisation admissible (OA)

- Organisation pouvant accéder aux initiatives financées dans le cadre du programme Initiatives en cybersécurité

Obligations du participant

> Habituellement, accorder du temps à son personnel pour qu'il prête main-forte au déploiement et au fonctionnement de l'initiative

> Fournir des données sur les initiatives déployées par l'organisation jusqu'en mars 2024

> Remettre un bref rapport après le déploiement de chaque initiative

Comment participer

1. Des représentants des partenaires provinciaux et territoriaux du RNRE inviteront les organisations admissibles à participer au programme.
   - Veuillez prendre contact avec le partenaire du RNRE de votre province ou territoire pour vérifier votre admissibilité.
   - https://www.canarie.ca/fr/cybersecurite/pic/soutien/

2. Organisation admissible
   - Elle soumet un court formulaire d'inscription à CANARIE.
   - Elle signe l'Entente de collaboration en cybersécurité avec une organisation (ECCO).

3. Après ratification de l'ECCO, votre partenaire du RNRE vous indiquera comment accéder à l'initiative subventionnée.
   - L'ECCO est valable pour toutes les initiatives.

Questions que vous pourriez vous poser

Doit-on adopter toutes les initiatives financées?

> Non. Vous choisissez celles qui conviennent le mieux à l'organisation. Veuillez toutefois nous dire pourquoi vous écartez telle ou telle initiative afin que nous puissions mieux en planifier de nouvelles.

Ces initiatives doivent-elles remplacer celles qui existent déjà?

> Non. L'idée est que toutes les organisations admissibles connectées au RNRE jouissent des mêmes technologies, méthodes et compétences de base en cybersécurité.

> Les initiatives du PIC comblent les lacunes qui pourraient exister et complètent les outils et les processus en place.

Questions que vous pourriez vous poser

Y a-t-il une date limite pour participer?

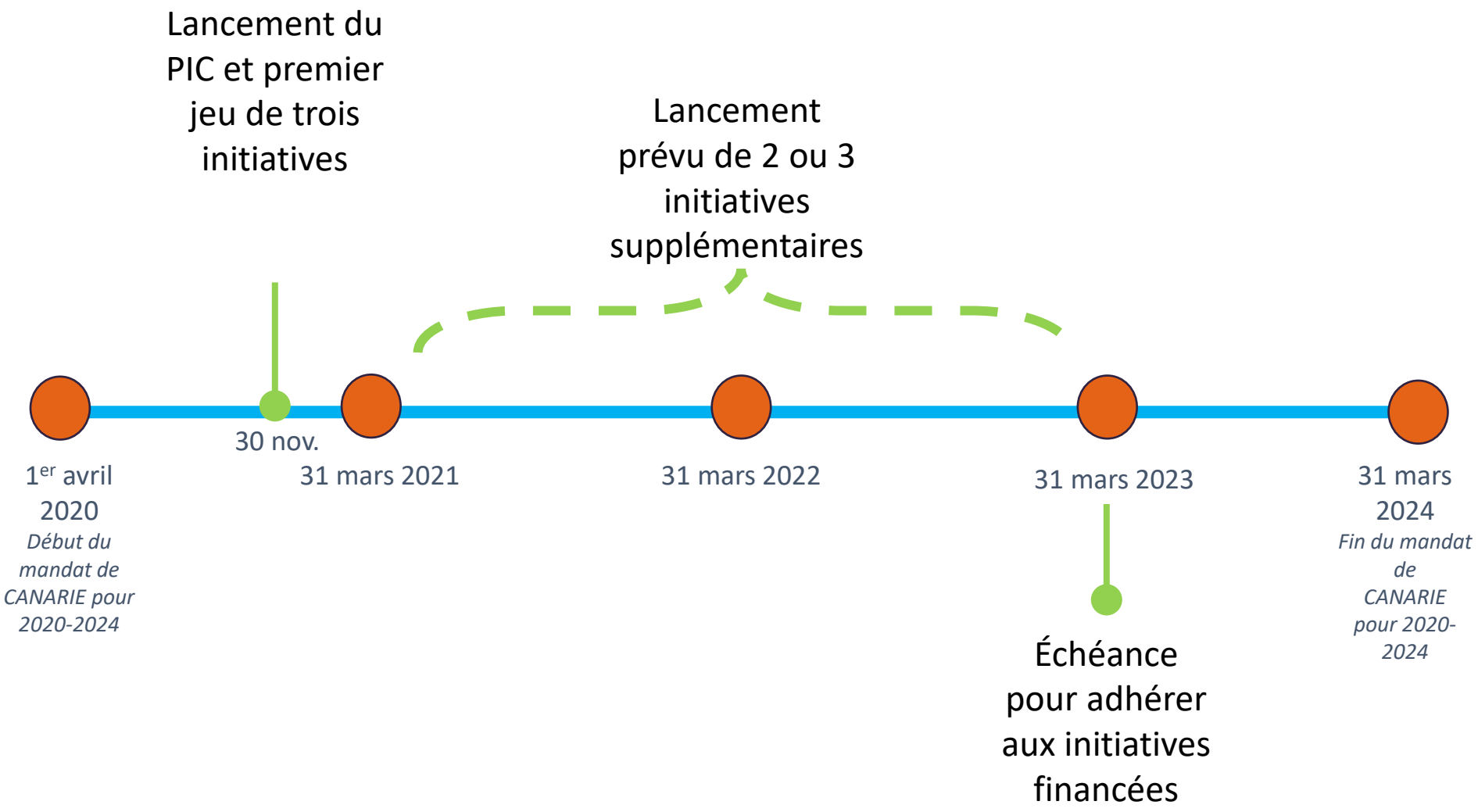
> L'organisation admissible peut participer en tout temps, mais elle n'aura accès aux initiatives subventionnées qu'après avoir signé l'ECCO.

> Plus tôt l'organisation participera, plus longtemps elle profitera des initiatives subventionnées.

> L'échéance pour participer aux initiatives subventionnées a été fixée au 31 mars 2023.

> Le financement du PIC se poursuivra jusqu'au 31 mars 2024.

Déroulement du programme



Et ensuite?

> Lancement du fil de menaces du CanSSOC – prochaines semaines

> Achèvement du système de détection des intrusions (auparavant Projet conjoint en sécurité) – été 2021

> Activités de la CCC et de ses comités

- Architecture de référence pour un cadre national en cybersécurité
- Prochain jeu d'initiatives prioritaires
- Poursuite des travaux sur la quantification de la cybersécurité

Le succès d'un plan national bien orchestré et articulé sur la collaboration en cybersécurité repose entièrement sur votre participation.

Quelles sont vos priorités/difficultés en cybersécurité?

canarie

canarie.ca | @canarie_inc