INSTITUT QUANTIQUE UdS

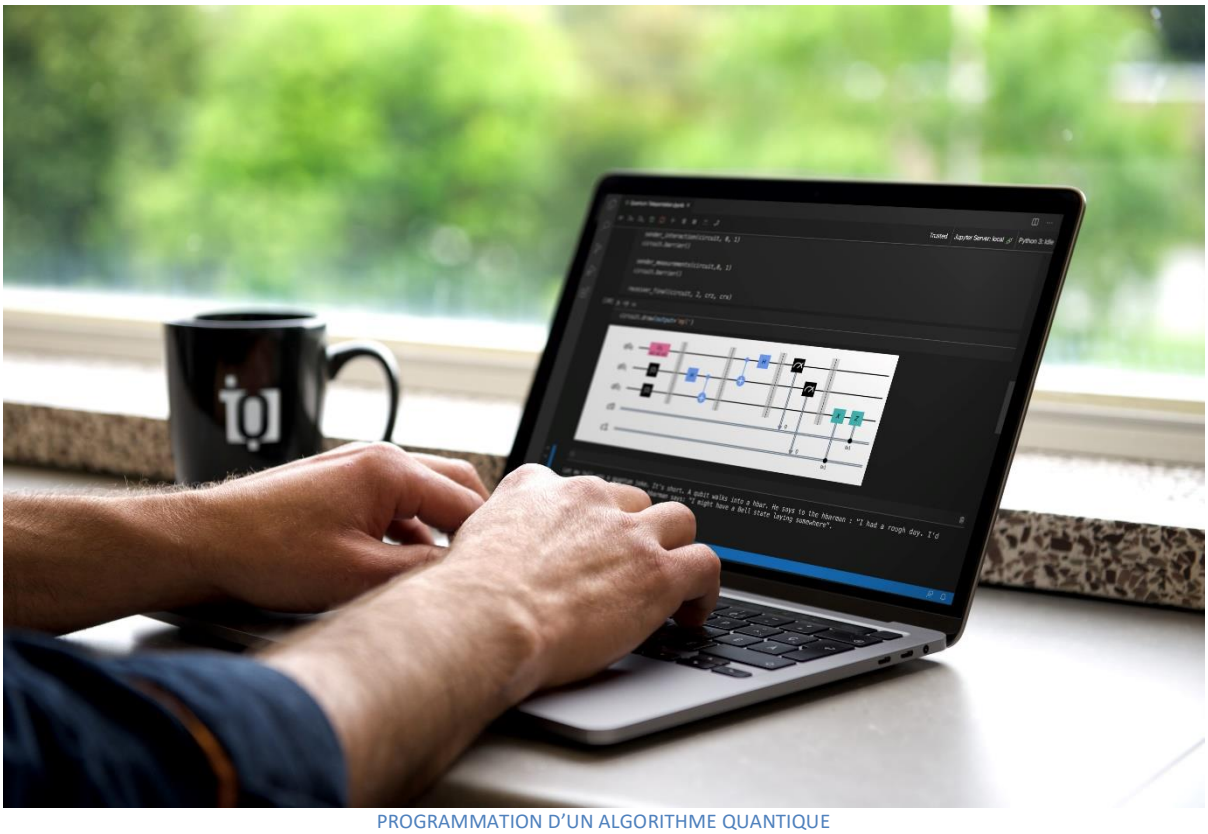
International Network for Governmental Science Advice

ÉTUDE DE CAS INGSA

SARATERRA

La cybersécurité à l'ère de l'ordinateur quantique

Rédaction : Karl Thibault, Jessica Baril et Christian Sarra-Bournet



PROGRAMMATION D'UN ALGORITHME QUANTIQUE

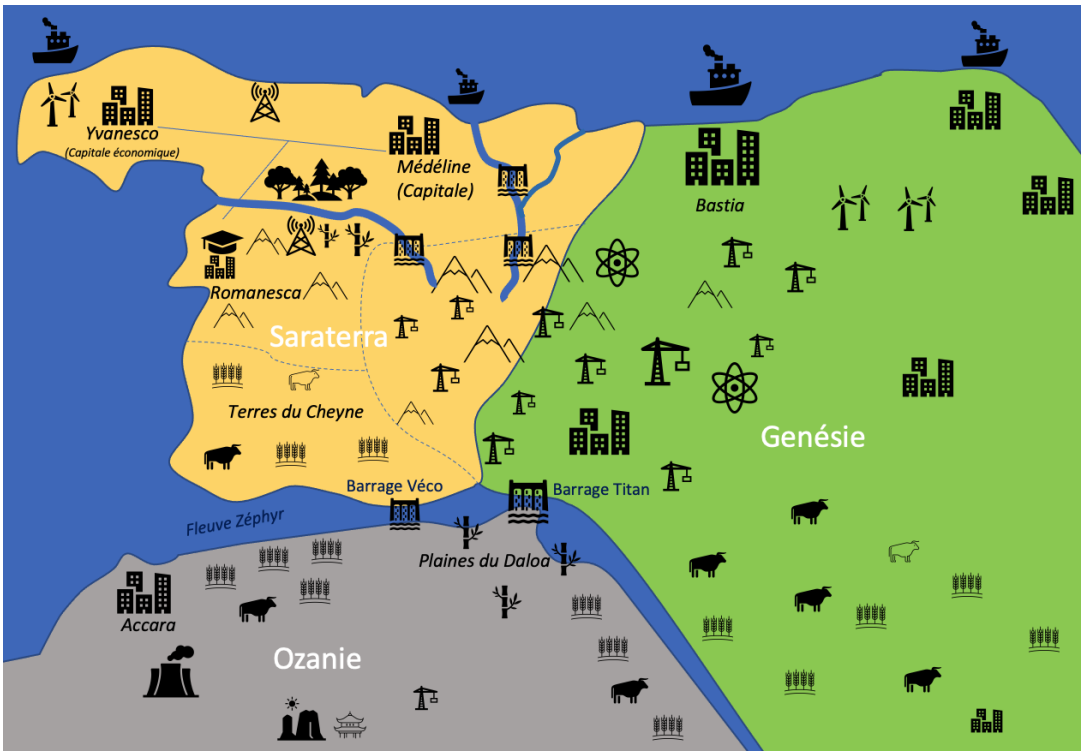
SARATERRA

La cybersécurité à l'ère de l'ordinateur quantique

Note: les faits et données présentées dans cette étude de cas sont fictifs et ne doivent pas être considérés comme une juste représentation de la réalité de certaines personnes, de certains pays ou de certains événements.

Saraterra

- **Capitale politique** : Médéline (2,5 millions)
- **Capitale commerciale et centre économique** : Yvanesco (3,1 millions)
- **Centre technologique et ville universitaire :** Romanesca (350 000, dont 25% communauté universitaire)
- **Superficie** : 1 256 000 km^2
- **Population** : 9,816,572
- **Densité de la population :** 55% urbaine, 16% banlieue, 29% rural
- **Groupes ethniques :** 71=4% Sarans, 12% Genois, 6% Ozans, 8% autre
- **Langue officielle** : Le Genois
- **Type de gouvernement** : Démocratie parlementaire
- **PIB :** 435 milliards de dollars



CARTE DU PAYS DE SARATERRA ET DE SES ENVIRONS – AN 2022

Contexte historique

L'empire Genois voit le jour en 1472 avec la conquête du territoire Saran à l'ouest et Ozan au sud du fleuve Zéphyr par le royaume Genois. Les Sarans et Genois sont des peuples commerçants avec de nombreux ports et échanges avec les territoires outre-mer, à la différence des Ozans, peuple

nomade vivant de l'abondance de la pêche et de la flore comestible du fleuve. Les différences culturelles entre les habitants de part et d'autre du fleuve se traduisent par des divergences d'opinions marquées et le peuple fier des Ozans se plie de plus en plus difficilement à l'autorité Genoise.

En 1781, la montée au pouvoir d'un nouveau chef Ozan déclenche le début d'une période de révolte. Après plusieurs années de guerre et de tentatives de conquête violentes du territoire de part et d'autre du fleuve, un traité de paix est établi en 1801 accordant la souveraineté aux Ozans (création de l'Ozanie), mais le peuple Genois conservera la possession et les droits d'exploitation du fleuve Zéphyr. Le reste du royaume Genois devient alors la Genésie.

Les années de conflits et de guerre laissent leur trace sur la relation entre Genois et Ozans, et la perte des droits à « son » fleuve crée des tensions dans la communauté de l'Ozanie. L'exploitation qu'en a faite la Genésie depuis n'a fait qu'exacerber les tensions internationales.

En 1956, la mise en service du barrage Titan inonde une partie des plaines de l'Ozanie, ce qui aura plusieurs impacts environnementaux. Le barrage permet à la Genésie de répondre à une partie de ses besoins énergétiques croissants et d'exporter le surplus à ses deux voisins.

Au cours des années 60, les différences culturelles entre les Sarans et Genois s'accentuent. Les Sarans ayant une vision davantage sociale-démocrate et un souci par rapport à la préservation de la nature, leur désir d'indépendance politique se renforce. Ils désirent particulièrement reprendre possession de leur territoire historique en vue des projets d'exploitation minière massifs Genois. La reconnaissance internationale du peuple Saran étant déjà bien établie, et son territoire étant riche en ressources naturelles, Saraterra se sépare de la Genésie et signe sa déclaration d'indépendance en 1977. Les relations sont demeurées cordiales entre les deux pays, aujourd'hui considérés comme alliés, avec un traité de libre-échange et la conservation de la monnaie Genoise.

En 2001, Saraterra met en service le barrage Véco qui, contrairement à Titan, a été conçu après des études évaluant les impacts environnementaux et sociaux afin d'éviter d'exacerber les tensions politiques et d'établir des relations plus diplomatiques avec les Ozans. Les Sarans ont ainsi regagné le respect d'une partie de la population de l'Ozanie. Cependant, les traités énergétiques défavorables pour l'Ozanie sont encore source de tension diplomatique entre les trois états.

L'Ozanie vit actuellement une crise énergétique, avec 45% de sa production provenant du charbon et du gaz naturel, 30% provenant du nucléaire de la Genésie et 25% de l'hydroélectricité de la Genésie et Saraterra. Dans ce contexte de rancune historique par rapport aux droits d'exploitation du fleuve, les relations avec les Ozans sont précaires. Au-delà de la rivalité politique et économique entre la Genésie et l'Ozanie, les tensions autour des ententes énergétiques sont d'autant plus teintées par les animosités historiques. Le régime totalitaire de l'Ozanie et la montée de sa militarisation depuis les années 50 inquiète d'autant plus les deux pays du nord, et particulièrement la Genésie, qui n'a jamais su remédier à la colère causée par le barrage Titan.

Géographie

Le territoire Saran est principalement couvert de steppes tempérées, avec des montagnes éparses à l'ouest et une chaîne de monts alpins à l'est divisant le pays en deux zones climatiques. Le nord est un pays sauvage de forêt Boréale. La région du sud-est représente le grenier agricole du pays avec la majeure partie des terres fertiles. Le pays est bordé à l'ouest et au nord par la Mer de Fermi. Les principaux ports d'exportation sont situés dans les villes de Médéline, la capitale politique du pays, et Yvanesco, son centre économique. Un réseau de chemins de fer relie les principaux centres avec les régions les plus faiblement peuplées du Sud, permettant le transport des ressources.

Économie

L'économie de Saraterra est historiquement basée sur l'exploitation de ses ressources naturelles, le commerce outre-mer avec ses nombreux ports et son positionnement stratégique. Ses forêts et chaines de montagnes de l'ouest regorgent de fer, d'aluminium, de silicium, de cuivre et d'argent. À la suite de son indépendance, une grande vague de nationalisation a eu lieu pour les secteurs minier, forestier et de l'énergie, permettant au pays de reprendre le contrôle de son économie face aux propriétaires étrangers. Au cours des dernières décennies, la chute des prix des métaux ainsi que l'augmentation de l'accessibilité aux ressources ont encouragé les gouvernements successifs à transformer l'économie vers une économie de services et de haute technologie concentrée dans les grandes villes de Saraterra, notamment dans la ville universitaire de Romanesca.

Cette transformation de l'économie ne s'est pas faite sans heurts. Alors que les régions de l'ouest et du nord près de la capitale jouissent d'une économie florissante, les régions moins densément peuplées du sud et de l'est se sentent abandonnées. Ces régions présentent des taux de chômage nettement plus élevés et des retards quant à l'implantation d'infrastructures vitales pour le développement, tel un réseau Internet à haut débit en région. Avec 4% de la population vivant sous le seuil de la pauvreté, le taux de chômage global du pays est de 7%, mais est plus élevé (11%) et en hausse dans les régions rurales, en particulier dans les régions minières à cause du ralentissement du secteur. La situation a donc créé un clivage dans la population avec une vision du monde moderne plus « progressiste » dans les villes d'importance et plus « conservatrice » en région.

Avec un taux de littératie de plus de 91%, la population de Saraterra a toujours valorisé la culture et l'éducation. L'Université de Romanesca est reconnue mondialement pour son excellence. Les années 90 voient la naissance d'un mouvement social-démocrate et de meilleurs programmes sociaux afin de pallier les écarts entre la population rurale et urbaine, ainsi qu'une réforme du système d'éducation avec l'école obligatoire et gratuite jusqu'à 16 ans.

Politique

Le parti présentement au pouvoir est le Parti Libéral Saran (PLS), un parti libéral, qualifié de centre gauche, ralliant les progressistes, avec une vision d'état plus interventionniste, social-démocrate, portée sur le développement des énergies renouvelables et les relations internationales. Ils ont récemment été élus avec la promesse électorale de dynamiser l'économie du pays : la récession dans le secteur minier et le taux de chômage en hausse en région amènent le PLS à vouloir consolider une nouvelle stratégie économique afin de minimiser les risques de crise économique.

Depuis l'indépendance, le système électoral est principalement bipartite avec le Parti de l'État Fondamental (PEF) – conservateur, qualifié de centre droite, ralliant parfois des éléments de l'extrême droite avec une vision d'état non interventionniste favorisant le libre marché et peu enclin à l'immigration – qui est l'autre parti d'importance et présentement dans l'opposition officielle.

Autres partis :

- Parti Environnement
- Le Parti Loyaliste (Objectif de réunification avec la Genésie)
- Le Parti Solidaire Ozan

Partie 1 – Problématique

Cybersécurité quantique – Synthèse préparée par le Scientifique en chef et Le Conseil de Sécurité des Communications

Aujourd'hui, à l'ère de l'information, bon nombre des biens les plus précieux d'une personne - ses finances, son dossier médical et, dans une large mesure, son identité - sont protégés par les "clés" complexes de la cryptographie. La cybersécurité actuelle (ou classique) est fiable parce que la clé de chiffrement utilisée pour une transmission en ligne est basée sur des problèmes mathématiques qui sont extrêmement difficiles à résoudre, même pour les ordinateurs les plus puissants. Les protocoles de cryptographie actuels, tels que RSA et la cryptographique à courbe elliptique (CCE), sont basés sur la difficulté à factoriser les grands nombres entiers ou à trouver des logarithmes discrets.

Toutefois, un nouveau type d'ordinateur, l'ordinateur quantique, a un potentiel disruptif énorme malgré le fait qu'il soit encore au stade de la recherche et développement. La science qui le sous-tend est complexe, mais des prototypes fonctionnels émergent de groupes de recherche du monde entier. L'impact des ordinateurs quantiques sur la cryptographie sera majeur : utiliser des clés plus longues – la manière conventionnelle d'augmenter la sécurité – ne suffira pas, et des méthodes radicalement nouvelles seront nécessaires pour établir des communications et identités digitales sécures. Autrefois, la question était de savoir si les ordinateurs quantiques allaient devenir une réalité. Maintenant, la question posée est : "Quand, et où, deviendront-ils une réalité?". Tout de même, certaines critiques continuent de croire que l'ordinateur quantique est impossible à réaliser.

Si, d'ici 10 ans, de puissants ordinateurs quantiques deviennent disponibles, mais qu'il faut à une organisation 11 ans pour réorganiser son infrastructure pour devenir « quantiquement » sécure, il est déjà trop tard pour que cette organisation soit imperméable à la menace quantique. En outre, pour se protéger contre la compromission des informations qui ont été communiquées un certain nombre d'années auparavant, le passage aux techniques de sécurité quantique doit se faire au moins autant d'années avant que les ordinateurs quantiques ne soient disponibles.

Heureusement, les sciences quantiques rendent également possible une solution à cette menace. La cryptographie quantique peut protéger de l'information d'une manière que même un ordinateur quantique ne peut pas briser les codes pour y accéder. La solution, appelée « distribution de clés quantiques (QKD) » est déjà disponible et utilisée pour protéger d'importants transferts bancaires et d'autres communications. Cette technologie est la première pierre d'un « Internet quantique ».

Il existe également une solution alternative, les protocoles de « cryptographie post-quantique ». Comme les méthodes actuelles, ils recourent à des technologies conventionnelles et reposent sur des hypothèses quant à l'infaisabilité de certains calculs mathématiques. Ces protocoles protègent contre toutes les formes connues d'attaques cryptographiques quantiques ou conventionnelles.

Les conséquences d'un manque de préparation à une attaque quantique pourraient être énormes: la compromission et l'effondrement des systèmes financiers, des réseaux énergétiques, du commerce électronique et d'autres infrastructures numériques sur lesquelles repose la société.

Dans ce cadre, le Scientifique en chef de Saraterra a commissionné un expert en sciences quantiques et une experte en cybersécurité de lui fournir leurs rapports sur l'état des connaissances en cybersécurité quantique et les menaces associées.

Le Scientifique en chef, en collaboration avec le Conseil de sécurité des communications de Saraterra, a ainsi rédigé trois propositions de projets pouvant répondre à différents degrés aux menaces en cybersécurité. Ces propositions sont détaillées ci-bas.

Proposition #1 – Accent sur la cybersécurité classique

Résumé

Considérant que la menace d'une attaque quantique reste tout de même spéculative, cette proposition se concentre sur l'investissement de ressources supplémentaires en cybersécurité classique. Ces investissements continuent l'effort déjà engagé du gouvernement vers une transition numérique des services et industries, et accéléreront celle-ci par un investissement accentué pour protéger les actifs présents.

Coûts d'implantation et besoins de formation spécifique

Cette proposition prend la forme d'un programme d'accompagnement des entreprises de Saraterra afin d'augmenter leurs capacités en cybersécurité classique le plus rapidement possible. Aucun coût en infrastructure ne sera requis puisque celles existantes sont suffisantes.

Ce partenariat public-privé doublera chaque dollar public investi par la contribution d'entreprises privées intéressées à se doter de capacités en cybersécurité classique. 100 M$ supplémentaires permettront de bonifier les programmes de formation afin de pallier le manque de main-d'œuvre dans ce secteur.

<u>Investissements publics (1,1 G$)</u>

- Programme d'accompagnement public pour la création d'emplois en cybersécurité classique : 1 G$
- Augmentation des capacités des programmes de formation existants : 100 M$

<u>Investissements privés (2 G$)</u>

- Prise en charge des emplois créés en cybersécurité publique : 2 G$

Retombées économiques attendues

- Création d'emplois : 5 000 en technologies de l'information

Ces emplois seront distribués à travers le pays afin d'accomplir une transition numérique à l'échelle nationale. Les modalités de ces emplois sont déjà connues et leur création peut être instantanée si la main-d'œuvre est disponible. Il y a d'ailleurs un potentiel élevé d'immigration économique dans ce domaine, car les emplois sont relativement peu spécialisés. Les salaires associés à ces emplois seront moyens.

Retombées politiques internationales attendues

-

Protection attendue

L'investissement réalisé par cette proposition permet de protéger les entreprises de Saraterra contre les cyberattaques d'aujourd'hui et d'augmenter la conscience populaire en cybersécurité. Toutefois, si l'ordinateur quantique vient à exister, ces investissements ne permettront pas de s'en protéger.

Proposition #2 – Cryptographie post-quantique

Résumé

Considérant que la menace d'une attaque quantique reste tout de même spéculative, le risque et les conséquences associés au statu quo sont trop importants pour ne pas agir. Cette proposition se concentre sur la création de nouveaux standards cryptographiques et logiciels pour contrer les attaques quantiques connues. Ces investissements nécessiteront la création de nouveaux standards, leur implémentation dans les protocoles nationaux de cybersécurité et la formation d'experts en cybersécurité et cryptographie à travers le pays sur ces protocoles et les attaques quantiques.

Coûts d'implantation et besoins de formation spécifique

Cette proposition consiste en la création d'un centre national de recherche en cybersécurité pour mener la création de nouveaux standards cryptographiques d'ici les cinq prochaines années.

Investissements publics (1,1 G$ sur 5 ans)

- Création d'un centre national en cybersécurité : 1 G$
    - Création de nouveaux standards cryptographiques : 900 M$
    - Adaptation des programmes de formation existants : 50 M$
    - Création d'un programme de formation continue : 50 M$
- Adoption des nouveaux standards cryptographiques : 100 M$
    - Mise à jour de l'infrastructure en place

Investissements privés attendus (1 G$ à la suite de la création des standards)

- Adaptation et réorganisation du réseau de transfert de l'information (500 M$)
- Prise en charge d'emplois en cybersécurité quantique par les entreprises (500 M$)

Retombées économiques attendues

- Création d'emplois : 100 emplois immédiats jusqu'à 2000 emplois dans 5 à 10 ans pour la création et la croissance du nouveau centre national en cybersécurité
- Une fois les standards développés, leur adoption à travers des secteurs variés de notre économie nécessitera l'implication de firmes de génie-conseil ainsi que des employés internes en cybersécurité et TI dans de nombreuses entreprises. Nous anticipons ~1000 emplois de ce type.

Nous recommandons la création de ce centre dans la ville de Romanesca, où l'expertise en sciences quantique et en cybersécurité est présentement concentrée, et où ces nouveaux emplois seraient créés afin d'en profiter. Les emplois futurs en cybersécurité quantique seront créés plus globalement dans le pays. Les salaires associés à ces emplois seront moyens-élevés.

Retombées politiques internationales attendues

La création de nouveaux standards est une occasion de faire du pays la référence sur la scène internationale au sujet de la cybersécurité quantique. Il est possible d'envisager l'exportation de nos standards et savoir-faire à l'extérieur de notre pays et l'adoption de ceux-ci par nos alliés.

Protection attendue

La protection atteinte par cette proposition dépendra des standards adoptés. En adoptant une stratégie basée sur la création d'un groupe de travail expert, il est raisonnable de s'attendre à être protégé contre les attaques quantiques les plus probables à ce jour. Toutefois, il n'y a aucune garantie de protection absolue dans un futur éloigné puisqu'un standard pourrait être lui aussi « attaquable » par de nouveaux développements en informatique et algorithmie quantique.

Proposition #3 – Internet quantique à grande échelle (IQGE)

Résumé

Considérant que la menace d'une attaque quantique reste tout de même spéculative et que le risque et les conséquences associés au statu quo pourraient être catastrophiques, la proposition *Internet quantique à grande échelle (IQGE)*, basée sur la distribution quantique de clé, invite à complètement revoir le fonctionnement de nos communications. Ces investissements nécessiteront une infrastructure nouvelle compatible avec les technologies de transfert d'information quantique, un changement de standard de cryptographie et de nouveaux programmes de formation en informatique et cybersécurité quantique.

Coûts d'implantation et besoins de formation spécifique

Cette proposition consiste en un partenariat public-privé pour la réorganisation totale du réseau de l'information et l'implémentation de nouvelles infrastructures de fibre souterraine à l'échelle nationale permettant le transfert d'information sécurisée « quantiquement ». Cette transition nécessitera de nombreuses actions disruptives, dont des travaux d'excavation majeurs, qui s'échelonneront sur 10 ans et qui auront des conséquences majeures pour notre pays.

<u>Investissements publics (20 G$ sur 10 ans)</u>

- Création d'un centre de recherche en cybersécurité quantique (5 G$)
    - Création de nouveaux standards de cryptographie quantique
- Implémentation d'une infrastructure de communication quantique à l'échelle nationale (13 G$)
- Création d'un programme de formation en cybersécurité quantique (1 G$)
- Création d'un programme de formation continue (1 G$)

<u>Investissements privés (10 G$ sur 10 ans)</u>

- Adaptation et réorganisation du réseau de transfert de l'information (8 G$)
- Prise en charge d'emplois en cybersécurité quantique par les entreprises (2 G$)

Retombées économiques attendues

- Création de nouvelles entreprises
- Création d'emplois (~ 23 000 emplois directs) dans de nombreux secteurs économiques
    - Recherche scientifique et formation : 2 000 (au total après 10 ans)
    - Ingénierie et secteur manufacturier: 5 000 par année sur 5 ans
    - Secteur primaire : 3500 par année sur 10 ans
    - Construction : 5 000 par année sur 10 ans
    - Technologies de l'information et télécommunications : 10 000 (au total après 10 ans)
- Dynamiser l'économie en région aura des répercussions positives sur les commerçants et les citoyens
- Rétention de talent dans la ville universitaire et augmentation des taux d'employabilité dans la région de Romanesca

Les emplois créés seront localisés partout au pays, dépendamment du secteur d'emploi en question. Les emplois du secteur de la construction seront dispersés pour créer l'infrastructure de communication quantique nécessaire entre les grandes agglomérations du pays, alors que les emplois de haute technologie et logiciel seront principalement concentrés dans la ville de Romanesca. Les technologies quantiques nécessaires au déploiement d'un *Internet quantique* requièrent des terres rares disponibles dans les gisements miniers du pays. Les modalités de certains

de ces emplois sont inconnues, puisqu'ils seront dans de nouveaux services et de nouvelles entreprises. Les salaires associés à ces emplois seront variés, allant de moyens (construction, industries manufacturières et minières) à élevés (recherche, technologies de l'information et télécommunication).

Retombées politiques internationales attendues

La création de nouveaux standards est une occasion de faire du pays la référence sur la scène internationale au sujet de la cybersécurité quantique. Il est possible d'envisager l'exportation de nos standards et savoir-faire à l'extérieur de notre pays et l'adoption de ceux-ci par nos alliés.

Protection attendue

La protection promise par cette proposition est absolue, même advenant l'émergence d'un ordinateur quantique universel. Toutefois, la technologie de distribution quantique de clé est encore au stade de recherche et développement.

Tableau récapitulatif

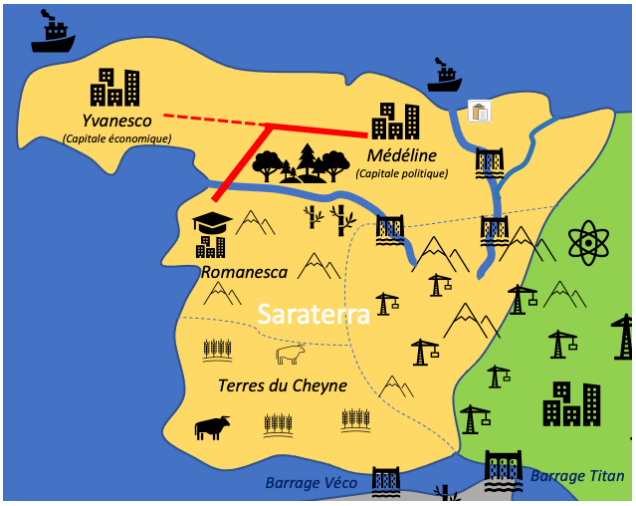
Proposition	1 - Cybersécurité classique	2 - Cryptographie post-quantique	3 - Internet quantique à grande échelle
Actions majeures	Programme d'accompagnement en cybersécurité classique	Création d'un centre national en cybersécurité	1. Création du centre de recherche en cybersécurité quantique 2. Partenariat public-privé pour l'implémentation d'une infrastructure nationale de télécommunication quantique
Création d'emplois	~ 5 000 emplois en technologies de l'information	100 à 2000 emplois d'ici 5 ans au Centre national en cybersécurité 1000 emplois en entreprise venant de l'adoption des standards à travers le pays (Formation et secteur public)	Recherche et formation (2 000) Ingénierie et secteur manufacturier (5000) Secteur primaire (3500) Construction (7000/année sur 5 ans) Technologies de l'information et télécommunications (5000) Formation et secteur public (500) Total : ~ 23 000 emplois directs
Investissements publics	1.1 G$	1.1 G$	20 G$
Investissements privés	2 G$	1G$	10 G$
Implémentation	Immédiat	5 ans	10 ans
Augmentation du PIB (435 G$)	~ 735 millions (0,2%)	~ 300 millions (0,1%)	~ 3,2 milliards (0,75%)
Endroit où les investissements seront faits	Dans tout le pays	Majoritairement à Romanesca et autres grandes villes	Partout (Infrastructure réseau) En région (Secteur minier) Grandes villes (Hautes technologies)
Maturité de la technologie	Élevée	Moyen	Faible
Niveau de cybersécurité	Faible	Moyen	Élevé
Niveau de risque et retour sur l'investissement	Faible	Moyen	Élevé

Partie 2 – Problématique

Nous sommes en mai 2030, 8 ans après l'adoption du projet d'Internet quantique à grande échelle (IQGE) par le gouvernement du Parti Libéral Saran (PLS) en 2022.

Historique du projet IQGE 2022-2030

Durant la phase de recherche et développement (2022 à 2027), il est rapidement devenu évident que l'envergure du projet IQGE avait été complètement sous-estimée. Le passage des concepts à une technologie mature et robuste a nécessité beaucoup plus de ressources et de temps que prévu. Malgré tout, le centre de cybersécurité de Saraterra (CCS) est maintenant opérationnel avec près de 1500 employés en recherche et le projet a généré plus de 3700 emplois.



La production de l'infrastructure de l'IQGE et des appareils spécialisés nécessaires à son installation a débuté en 2025 et les travaux d'excavation pour les lignes souterraines ont été entamés à l'été 2026. À l'été 2027, en vue du début des travaux de chantier et installation de la ligne entre Romanesca et Médéline, les inquiétudes pour la préservation des systèmes hydriques se sont accentuées et des manifestations organisées par le Parti Environnement ont fait pression sur le gouvernement. Des changements ont été apportés au plan des infrastructures afin de surplomber la grande rivière blanche, avec l'ajout d'un détour majeur de la ligne vers Romanesca pour des enjeux de préservation d'écosystèmes, occasionnant d'autres dépassement de coûts.

De surcroît, la population voit la majorité des revenus du projet revenir à des entreprises ayant leur siège social à l'étranger et la plupart des emplois générés comme étant éphémères. Les rumeurs de corruption entre les entrepreneurs en construction ont exacerbé les opinions négatives du projet et l'opinion considérant le projet comme un gaspillage d'argent public se répand dans la population.

Élections de novembre 2029

Profitant de l'opposition montante au projet et de l'inquiétude face au risque de crise économique mondiale, les partis de l'opposition ont rapidement adopté un discours défavorable à l'IQGE, l'exposant comme une dépense indécente et corrompue. Ainsi, lors de la campagne électorale de l'automne 2029, le parti de l'État Fondamental (PEF) a promis de mettre un terme au projet et de mener une enquête sur le milieu de la construction. Le PEF soutient que les fonds nécessaires pour terminer le projet devraient être utilisés pour solidifier l'économie manufacturière du pays.

Profitant de la grogne populaire et l'usure du pouvoir du PLS, le PEF a remporté les élections avec 51% des voix, dont la majorité provient de Médéline et des régions. Le Parti Environnement a remporté un nombre record de sièges (24% des voix), plaçant en dernière position le PLS avec 20% des votes. Ces élections ont mis en lumière la division marquée entre les habitants des grandes villes et le reste de la population : à Romanesca et Yvanesco, où se concentre la majorité des emplois reliés au projet, le discours pour la continuation l'emporte. Dans la capitale politique de Médéline, les opinions sont plus mitigées, mais la majorité (62%) est contre le projet. En région agricole, la majorité des habitants s'y opposent et en région minière les opinions sont plus partagées.

Partie 3 – Problématique

Nous sommes en juin 2031, un an après la décision du PEF d'arrêter le projet de l'IQGE.

Cyberattaque sur une infrastructure électrique cruciale

Ce matin, le 13 juin 2031, une panne d'électricité de douze heures (minuit à midi) a été reportée près d'Yvanesco, touchant 50 usines et 50 000 abonnés. Un hôpital a été affecté et a dû utiliser sa génératrice d'urgence, limitant les capacités de soin et augmentant la visibilité de l'événement. Cela a fait la une de tous les journaux du pays; les citoyens et entreprises demandent une explication.

Il est maintenant 14h et la situation est sous contrôle, malgré les pertes économiques estimées à plus de 30 M$.

Vers 9h ce matin, le gouvernement a reçu un message de la part de pirates informatiques revendiquant la panne. Ils auraient attaqué le centre de contrôle électrique principal du pays, situé sur la ligne non complétée de l'IQGE près d'Yvanesco, pour rediriger le débit électrique vers l'Ozanie. Ils laissent au gouvernement jusqu'à 16h pour répondre aux demandes suivantes, sans quoi ils menacent une panne généralisée d'Yvanesco :

1. Une rançon de 100 M$.
2. La reconnaissance de la souveraineté territoriale du fleuve Zéphyr à l'Ozanie.
3. Une renégociation des traités énergétiques entre Saraterra et l'Ozanie.
4. Le retrait des surtaxes imposées aux biens en provenance d'Ozanie.

Situation au gouvernement

Le gouvernement a demandé en urgence au Centre de cybersécurité de Saraterra une mise à jour sur leurs capacités en cyberdéfense et les modalités de cette attaque, remise au ministre de la Sécurité nationale. Vous savez maintenant que l'attaque proviendrait d'une cellule extrémiste en Ozanie, connue pour être financée par le gouvernement Ozan. Vous n'avez aucune information à savoir si elle agit sous les ordres de l'Ozanie, ou bien si elle mène son propre agenda en dépit du pouvoir en place en Ozanie.

Le Premier ministre a signalé une rencontre d'urgence du Conseil des ministres pour établir la stratégie de réponse aux pirates ainsi que pour établir la stratégie de communication envers la population du pays.

Le Président de l'Ozanie est à la tête du pays depuis près de 15 ans. Peu de personnes osent s'opposer au régime en place et il est généralement admis à l'extérieur de l'Ozanie qu'une dictature y est en place.

Partie 1 – Déroulement

Déroulement de l'étude de cas

Phase 1 - Évaluation de technologies concurrentes pour protection des données contre les attaques quantiques

Nous sommes en 2022. Le parti au pouvoir est le Parti Libéral Saran.

Le scientifique en chef a produit un rapport de synthèse sur la cybersécurité quantique que vous avez en votre possession. Ce rapport a été commissionné par le ministre Science Économie et Innovation afin de guider le développement de la stratégie en cybersécurité de la nation de Saraterra. Au fil de trois simulations, vous évaluerez le potentiel scientifique, social et économique des projets pour finalement prendre une décision sur quel projet sera financé par le Ministère Science Économie et Innovation.

Voici les rôles qui seront attribués aux différentes tables pour cette phase :

1. Scientifique en sciences quantiques
2. Scientifique en cybersécurité
3. Scientifique en chef de Saraterra
4. Sous-ministre aux industries stratégiques
5. Chef de cabinet du ministre Science Économie et Innovation
6. Ministre Science Économie et Innovation

Trois simulations seront jouées lors de cette phase. Vous avez 30 minutes pour vous y préparer, en groupe. Une seule personne de votre table devra jouer votre rôle assigné lors des simulations.

Simulation #1 (15 minutes)
Objectif : Évaluation des technologies.
Tables impliquées : 1,2,3

Le scientifique en chef rencontre une dernière fois ses collègues experts en sciences quantiques et en cybersécurité afin de déterminer sa propre position basée sur la validité scientifique des projets.

Simulation #2 (15 minutes)
Objectif : Évaluation des retombées sociales, politiques, environnementales et économiques
Tables impliquées : 4,5

Le chef de cabinet du ministre Science Économie et Innovation cherche à déterminer les retombées potentielles de chaque projet, d'un point de vue social, politique, environnemental ou économique, afin de pouvoir conseiller le ministre.

Simulation #3 (15 minutes)
Objectif : Choisir le projet retenu
Tables impliquées : 3,5,6

Le ministre Science Économie et Innovation rencontre son chef de cabinet en compagnie du scientifique en chef afin de prendre la décision finale. Ensuite, il participe à une mêlée de presse devant journalistes.

Partie 2 – Déroulement

Dépassement de coûts et cyberattaque quantique présumée dans un pays allié : Décision face à la continuation du projet

Nous sommes en 2030, 8 ans après l'adoption du projet d'Internet quantique à grande échelle (IQGE – Projet #3 de la Phase 1) par le gouvernement du Parti Libéral Saran (PLS) en 2022. Le Parti de l'État Fondamental (PEF) vient de remporter les élections et de renverser le gouvernement du PLS qui régnait depuis 12 ans. De surcroît, une rumeur d'une cyberattaque en Genésie s'est récemment propagée dans les médias Genois. Dès son arrivée au pouvoir, le PEF a commandé un rapport général sur la situation actuelle du projet proposant deux plans d'action. Vous connaissez aussi l'existence d'un rapport préélectoral rédigé par le centre de cybersécurité de Saraterra (CCS) qui fait l'état de nos connaissances sur la rumeur d'une supposée cyberattaque en Génésie.

Le rapport contenant les plans d'action pour l'IQGE présente aussi les données budgétaires et les retombées de la continuité ou non du projet IQGE.

DÉROULEMENT

Au fil de trois simulations, vous devrez décider et débattre de l'avenir du projet tout en évaluant les risques qui lui sont liés. Voici les rôles qui sont attribués aux différentes tables pour cette phase :

1. Chef-fe de l'opposition (PLS)
2. Chef-fe de cabinet du Premier ministre (PEF)
3. Ministre des Relations internationales (PEF)
4. Ministre de la Sécurité nationale (PEF)
5. Premier-e ministre (PEF)
6. Président-e du centre de cybersécurité de Saraterra

Simulation #1 (15 minutes)

Objectif : Déterminer la probabilité d'une attaque imminente sur notre pays.

Tables impliquées : 3,4,6

Le ministre de la Sécurité nationale convoque le ministre des Relations internationales et le Président du CCS afin de déterminer s'il doit s'attendre à ce que Saraterra soit la cible d'une attaque imminente, afin de conseiller le Premier ministre lors de la simulation suivante.

Simulation #2 (15 minutes)

Objectif : Décider de la continuation du projet au sein du PEF et se préparer pour la période de questions qui suivra en Chambre des communes.

Tables impliquées : 2,4,5

Le Premier ministre doit décider s'il réalise sa promesse d'arrêter le projet IQGE, considérant les situations sociales (représentées par son chef de cabinet) et de sécurité nationale (représentées par le ministre de la Sécurité nationale). Cette décision devra être défendue à la simulation suivante.

Simulation #3 (15 minutes)

Objectif : Questionner le PEF (parti au pouvoir) sur leur décision prise à la simulation précédente lors d'un débat en Chambre des communes.

Tables impliquées : 1,5

Le chef de l'opposition (PLS) mène une période de questions envers la décision prise par le PEF de continuer ou non le projet de l'IQGE.

Partie 3 – Déroulement

Attaque sur une infrastructure névralgique électrique : Gestion de crise

Nous sommes en 2031, un an après la décision du gouvernement du PEF de mettre un terme définitif au projet de l'IQGE, un choix salué par la population de Saraterra.

Une cyberattaque a eu lieu sur le « Centre de contrôle électrique » de Saraterra. Des milliers de citoyens ont vécu une panne de courant de plusieurs heures, et une inquiétude générale s'installe dans la population. Une rançon a été demandée par une cellule extrémiste située en Ozanie connue de vos services de renseignements, en plus de revendications concernant les droits d'exploitation au fleuve Zéphyr par l'Ozanie, sans quoi elle menace de causer une panne généralisée de longue durée.

Votre objectif est de gérer cette crise en établissant à la fois la stratégie de réponse du gouvernement et la stratégie de communication envers la population de Saraterra.

Voici les rôles qui seront attribués à vos tables pour cette phase :

1. Ministre de la Sécurité Publique de Saraterra
2. Premier ministre de Saraterra
3. Ministre des Finances de Saraterra
4. Ministre des Relations internationales de Saraterra
5. Ministre de la Sécurité nationale de Saraterra
6. Attaché de presse du Premier ministre Saraterra

Simulation #1 (20 minutes)

Objectif : Établir une stratégie de réponse envers les assaillants et une stratégie de communication envers notre population.

Tables impliquées : 1,2,4,5

Les ministres de Saraterra sont convoqués par le Premier ministre afin de déterminer dans quels cas Saraterra paiera la rançon et déterminer le message à envoyer à la population.

Simulation #3 (10 minutes)

Objectif : Envoyer un message clair à la population de Saraterra pour les informer sur les mesures mises en place par votre gouvernement.

Tables impliquées : 2,6 (lire ci-bas)

Cette simulation sera divisée en trois parties :

2 minutes : Déterminer le message envoyé à la population par le Premier ministre, basé sur les interactions précédentes, ainsi que le format du message
2 minutes : Déclaration du Premier ministre
6 minutes : Questions des journalistes

Annexe A – Plans d'action pour l'IQGE

Phase 2 – Remis aux tables 2 (Chef de cabinet) et 4 (Premier ministre PEF)

Plan A : Continuation du projet IQGE

L'investissement public estimé pour le Projet IQGE s'élève maintenant à 42,7 milliards $, totalisant un dépassement de coûts de 12,7 milliards $ par rapport au budget initial. L'achèvement des travaux de la ligne entre Romanesca et Médéline nécessitera 3,1 milliards $ additionnels et l'exécution de l'embranchement vers Yvanesco (centre économique) requiert un investissement additionnel de 12,2 milliards $, menant le coût total du projet à 58 milliards $, près du double du budget initial.

L'achèvement du projet permettrait de soutenir 11 642 emplois directs actuels d'ici la mise en service du réseau en 2035 et générerait 4 400 emplois additionnels en technologies de l'information entre 2030-2035. L'opération du réseau assurerait 9 750 emplois permanents après 2035, pour une période d'au moins 10 ans. La création de richesse (sans compter les effets indirects) s'élèverait en moyenne à 2,5 milliards $ (dont 1,85 milliard $ en masse salariale) sur 5 ans, un niveau correspondant à environ 0,6% du PIB du pays, puis à 1,7 milliard $ après la mise en service. L'équilibre budgétaire sur l'investissement public de l'IQGE serait atteint en près de 15 ans.

Plan B : Arrêt du projet IQGE et diversification de l'économie

Le «Plan stratégique» du Parti de l'État Fondamental propose l'arrêt immédiat des travaux de chantier et l'interruption des activités du centre de recherche en cybersécurité quantique, mais l'adoption du programme d'accompagnement en cybersécurité classique, nécessitant un investissement public de 1,1 milliard $.

Certains emplois dans le secteur manufacturier et le secteur primaire seraient à risque avec l'arrêt du projet. Le gouvernement prévoit donc 1,5 milliard $ en subventions aux entreprises afin de favoriser leur transition vers la production de biens essentiels. Cependant, sur une optique à moyen terme (5-10 ans) ces secteurs devraient croître de façon importante grâce à l'augmentation de l'autonomie de production du pays et la réduction des imports. Ce plan permettrait de maintenir 10 940 emplois (1,73 milliard $ en masse salariale) répartis à travers les régions.

À court terme, la revente des infrastructures de l'IQGE à des entreprises privées pourrait générer 7,8 milliards $, permettant de réduire la dette du pays et de maintenir les programmes sociaux.

La projection de l'augmentation du PIB à moyen long terme est de 3 à 5 milliards $ par année sur au moins 15 ans, soit 2% du PIB du pays. En prenant en compte les recettes gouvernementales, l'équilibre budgétaire sur l'investissement public de l'IQGE serait atteint en moins de 5 ans.

Tableau récapitulatif – Projections économiques des deux scénarios

	Continuation de l'IQGE	**Arrêt de l'IQGE**
Investissements supplémentaires	15,3 milliards $	2,6 milliards $
Poids de l'investissement sur la dette	3,5% du PIB	0,6% du PIB
Retour à l'équilibre budgétaire estimé	15 ans	5 ans
Emplois (localisation)	Temporaires, 2030-2035 : ~ 16 000 (à travers le pays) Permanents, après 2035 : 9750 (centres urbains)	10940 (à travers le pays)

Rapport spécial Centre de cybersécurité de Saraterra (CCS)

Phase 2 – Remis aux tables 4 (ministre de la Sécurité nationale) et 6 (Président du CCS)

Rapport datant du 10 avril 2030, avant les élections nationales de Saraterra
À l'adresse du ministre de la Sécurité nationale

Résumé exécutif :

- Notre équipe de sécurité nationale a décelé des signatures de cyberattaques en Genésie;
- Les cyberattaques visaient des infrastructures du secteur de l'énergie;
- Une cellule extrémiste en Ozanie est le suspect principal;
- Nos services de renseignements confirment qu'il existe un risque réel pour que nos infrastructures électriques soient une cible potentielle;
- Nous estimons à 75% les chances que les assaillants aient découvert une faille informatique dans les cyberdéfenses de Titan et à 25% qu'ils aient accès à un système informatique inconnu à ce jour (dans ce cas précis, un potentiel réel d'un ordinateur quantique);
- Notre protection actuelle est insuffisante contre des attaques similaires;
- Le réseau de l'IQGE partiel actuel ne permet pas de protéger les informations financières entre Médéline et Yvanesco.

Les risques de cyberattaque quantique ont considérablement augmenté lors de la dernière année, jusqu'à devenir une menace pour notre pays.

Historique

Le 18 juin 2029, l'électricité produite par une centrale électrique mineure en Genésie a soudainement été redirigée vers une route imprévue pour une durée de 40 secondes. Ce problème avait alors été attribué à une défaillance du système d'optimisation de traitement de l'électricité.

Le 7 novembre 2029, le barrage électrique Titan de la Genésie a subi le même traitement, mais pour une durée de 180 secondes. Cela a causé des pannes d'électricité mineures pour plus d'un million d'abonnés en Genésie.

À la suite de ce second événement, les experts en cybersécurité de la Genésie ont mené une enquête avec comme visée principale une cellule extrémiste d'Ozanie connue pour ses revendications concernant les droits « inhérents à l'Ozanie » au fleuve Zéphyr et donc à l'hydroélectricité produite dans celui-ci.

Aucune revendication n'a été faite.

Étant donné le niveau de sophistication de l'attaque, il est peu probable qu'un groupe de pirates amateurs ait la capacité de réaliser de telles attaques sans le support d'un État ou d'une organisation de grande envergure pour de l'espionnage industriel.

Les informations semblent révéler un projet Secret Défense en Ozanie visant une guerre informatique. Des rumeurs parlent d'un programme de R&D secret pour l'obtention d'une puissance de calcul inégalée dans lequel l'Ozanie investit depuis 10 ans.

Analyse

Ces cyberattaques sont impossibles avec les capacités informatiques connues en Ozanie. Surpasser les cyberdéfenses du système de Titan nécessiterait plusieurs années pour le superordinateur le plus puissant au monde. Les assaillants semblent donc avoir trouvé une faille majeure dans les cyberdéfenses de Titan ou ont accès à un système informatique inconnu à ce jour.

Il y a une possibilité non nulle qu'un ordinateur quantique ait été développé et que cette organisation y ait accès. Selon nos analyses, celui-ci serait composé d'au moins 400 qubits logiques pour avoir pu briser les cyberdéfenses de Titan.

Une hypothèse est que l'événement du 18 juin 2028 était un test réalisé sur un système informatique moins résistant. En effet, par comparaison, les cyberdéfenses de la centrale mineure pourraient être brisées par un ordinateur quantique estimé à environ 20 qubits logiques.

Aucun autre système informatique connu n'a la capacité de briser les codes de cybersécurité présentement utilisés. Il est possible que les assaillants aient réussi à développer un système nouveau genre, quoique cette possibilité soit très faible.

Aucune attaque de ce type n'a été répertoriée en territoire Saran. Toutefois, il est possible qu'une attaque très courte ne puisse être identifiée. Il est difficile de prévoir quand la prochaine attaque aurait lieu, avec comme seule donnée que l'intervalle entre les deux attaques précédentes était d'environ 10 mois, mais il se pourrait qu'elle se produise d'ici quelques mois.

En prenant en compte toutes ces informations, nous estimons à 75% les chances que les assaillants aient découvert une faille informatique dans les cyberdéfenses de Titan et à 25% qu'ils aient accès à un système informatique inconnu à ce jour (vraisemblablement un ordinateur quantique).

État de la protection

Les cyber protections en place actuellement ne sont pas suffisantes pour repousser une attaque telle que celle décrite ci-haut si elle est menée par un ordinateur quantique.

Le réseau IQGE présentement en construction permettrait techniquement de protéger nos systèmes névralgiques contre ce type d'attaque. Toutefois, il est impératif de mettre en contact les gestionnaires de cybersécurité des infrastructures à risque en contact avec les spécialistes du CCS afin d'assurer que les protocoles mis en place soient sécuritaires et que ces infrastructures soient incluses dans le système de protection.

Spécifiquement, nous recommandons au CCS d'entrer en contact avec les gestionnaires de cybersécurité de nos infrastructures électriques le plus rapidement possible afin d'analyser de nouveau nos cyberdéfenses pour toute faille possible.

Par ailleurs, le réseau IQGE partiel ne protège présentement pas la majorité des informations financières du pays, qui transitent entre Médéline et Yvanesco. Avec la collaboration du ministère Science, Économie et Innovation, il a été estimé que les pertes journalières d'une cyberattaque sur le système financier de Saraterra représenteraient 3,4 milliards de dollars par jour.

Dans le cas ultime où une entité ennemie aurait accès à un ordinateur quantique fonctionnel, il est crucial de poursuivre les recherches effectuées au CCS et d'étendre nos activités d'espionnage pour contrer cette menace.

Les informations contenues dans ce document proviennent en partie de partenaires internationaux dont la fiabilité est élevée et avec lesquelles nous possédons des ententes de confidentialité robustes.

Rapport spécial sur l'Ozanie

Phase 2 – Remis à la table 3 (ministre des Relations internationales)

Phase 3 – Remis à la table 4 (ministre des Relations internationales)

Rapport de l'ambassadeur Saran en Ozanie pour le ministre des Relations internationales – mai 2030

Situation socio-économique de l'Ozanie

Le Parti Libéral Saran (PLS) anciennement au pouvoir et ayant toujours eu une vision portée sur les relations internationales, a entretenu d'étroits liens avec l'Ozanie, son deuxième partenaire économique d'importance.

Cependant, la hausse des tarifs d'hydroélectricité vendue à l'Ozanie, les surtaxes sur les exports et la hausse du prix de certains métaux ont sans conteste contribué à la crise dans le secteur manufacturier en Ozanie. Dans le contexte où les marchés mondiaux sont déstabilisés, l'Ozanie a connu une baisse de 9,8% de son PIB au 4e trimestre de 2028, marquant le début de sa crise économique. Avec le taux de chômage en hausse, le pays a connu une baisse du niveau de vie moyen, et une hausse significative des demandes d'aide à la banque alimentaire et du taux de criminalité, en particulier dans les grandes villes. La situation économique a par ailleurs causé une vague importante d'immigration Ozanne vers Saraterra depuis 2027.

À la suite de la deuxième hausse des tarifs d'hydroélectricité de Saraterra, le Président Ozan a tenté de nouvelles négociations avec la Genésie pour une baisse de ses prix d'énergie, mais le gouvernement Genois est demeuré impassible, voire indifférent aux difficultés des Ozans.

Par ailleurs, le Parti de l'État Fondamental (PEF) vise à développer son autonomie de production de biens, et établir de nouvelles politiques protectionnistes, en réduisant l'immigration afin de favoriser les emplois aux Sarans, et prévoit l'ajout de taxes sur les imports de produits agroalimentaires et une augmentation des surtaxes sur ses exports. Ces mesures auront sans doute des impacts additionnels néfastes sur l'Ozanie.

Ambitions militarotechnologiques de l'Ozanie

Le régime totalitaire Ozan inquiète les pays du nord depuis des années, d'autant plus depuis l'arrivée au pouvoir du président actuel en 2017. Malgré les difficultés économiques du pays, le budget militaire a continué d'augmenter (passant de 43,9 milliards en 2019 à 65,8 milliards en 2029). Par ailleurs, en 2021, le gouvernement Ozan a accordé des sommes sans précédent à la recherche. Avec 66,9 milliards en recherche fondamentale et appliquée, 72,5 milliards pour le développement expérimental des technologies, et 500 millions pour des programmes attraction de talent envers les pays du sud, le Président a clairement souligné ses ambitions de redorer la fierté Ozane en positionnant le pays à l'avant-garde du développement technologique, avec une armée forte et une diplomatie protectionniste.

Le Président Ozan accusant les pays du nord pour la crise économique du pays, la population Ozanne est convaincue que ses voisins sont à blâmer pour les difficultés du peuple. Des actes de vandalisme faits par des Ozans dans les capitales politiques en Genésie et Saraterra (graffitis haineux contre les dirigeants Genois et Sarans), dénotent de l'amertume du peuple et de la colère envers le manque d'empathie des pays du nord. En Ozanie on enregistre des mouvements plus extrémistes revendiquant toujours les droits d'exploitation du fleuve, avec la croyance que les centrales du fleuve devraient appartenir aux Ozans. Le ministère de la Sécurité publique de Saraterra a également enregistré des activités suspectes dévoilant des traces de financement provenant de groupes d'intérêt privé indéterminés pour financement de cellules extrémistes.

Mise à jour – Rapport spécial Centre de cybersécurité de Saraterra (CCS)

Phase 3 – Remis à la table 5 (ministre de la Sécurité nationale)

À l'adresse du ministre de la Sécurité nationale - 13 juin 2031

Cyberattaque

À minuit le 13 juin 2031, une cyberattaque a ciblé le centre de contrôle électrique de Saraterra. Les pirates ont détourné le flux d'électricité allant vers un quartier industriel près d'Yvanesco pour rediriger cette électricité vers l'Ozanie, touchant 50 usines et 50 000 abonnés, de minuit à midi.

Les pirates proviennent d'une cellule extrémiste d'Ozanie. Les informations semblent révéler un projet secret de défense en Ozanie visant une guerre informatique.

Les pirates ont contacté le gestionnaire du centre de contrôle électrique vers 8h30 ce matin, par courriel. Dans ce courriel se trouvaient leurs revendications :

- Une rançon de 100 M$;
- La reconnaissance de la souveraineté territoriale du fleuve Zéphyr à l'Ozanie;
- Une renégociation des traités énergétiques entre Saraterra et l'Ozanie;
- Le retrait des surtaxes imposées aux biens en provenance d'Ozanie;

Leurs menaces :

- Prendre un contrôle total de la gestion électrique de Saraterra;
- Rediriger 25% de l'électricité générée vers l'Ozanie;

Et le moyen de les contacter :

- Déposer l'argent dans le compte #010010110100001 de cryptomonnaie QubitCoin;
- Faire une annonce télédiffusée sur la chaîne nationale de Saraterra, évoquant les actions prises en lien avec les revendications de la cellule, et ce au maximum à 16h.

État de la protection

Le Centre de contrôle de l'électricité de Saraterra est situé sur la ligne non terminée de l'IQGE, sans quoi nous aurions peut-être pu nous défendre contre cette attaque. Notre personnel a révisé toutes les protections en place sur le réseau électrique au début de 2031 et n'a trouvé aucune faille.

Selon nos analyses, les chances que cette cellule ait accès à des capacités de calcul décuplées (telles que celles d'un ordinateur quantique) sont maintenant de 65%. L'état connu des ordinateurs quantiques limite toutefois notre capacité de croire à un tel accomplissement. Nous estimons donc à 35% les chances que les pirates exploitent une faille dont nous ignorons l'existence et notre personnel est mobilisé pour la trouver.

Actuellement, nous ne pouvons donc pas nous défendre des cyberattaques provenant de ces pirates.

Nous recommandons au gouvernement d'agir sur le plan politique le plus rapidement possible pour diminuer les risques de représailles par ces pirates.

Si nous ne répondons pas à leurs exigences, il faudra mettre en place un plan afin de retirer complètement le centre de contrôle d'internet. Nous sommes déjà en communication avec le gestionnaire principal à ce sujet.

Déroulement suggéré de la journée

Partie 1 – Atelier

08h00 – Accueil des invités et petit déjeuner de réseautage

08h30 – Mots de bienvenue

09h00 – Étude de cas, phase 1

10h30 – Pause santé

10h45 – Étude de cas, phase 2

12h15 – Dîner

13h00 – Conférences

14h00 – Étude de cas, phase 3

15h45 – Pause santé

16h00 – Réflexion sur les liens entre le milieu de la recherche et les gouvernements

16h30 – Fin de l'atelier

Intervention en matière de conseil scientifique

Nous entamons la troisième décennie du XXIe siècle et ce sont aujourd'hui les technologies quantiques qui sont classées parmi les avenues scientifiques ayant le potentiel de révolutionner le monde, par leur fonctionnement radicalement différent des technologies d'aujourd'hui.

L'application la plus connue de l'ordinateur quantique est sans doute l'algorithme de Shor qui permet de factoriser un nombre entier, une tâche extrêmement difficile à réaliser sur un ordinateur classique. La majorité de nos cryptosystèmes sont donc basés sur l'impossibilité de factoriser de grands nombres en un temps raisonnable avec nos outils actuels. Ainsi, l'implémentation de l'algorithme de Shor sur un ordinateur quantique assez puissant rendrait vulnérable toute information présentement protégée par les protocoles existants de cryptographie. Cette application potentielle de l'ordinateur quantique pose des questions éthiques sur plusieurs fronts (militaires, économiques, vie privée, etc.) et plusieurs institutions rivalisent entre elles pour un accès rapide et privilégié à un tel outil.

Il est important que les personnes en position de décision dans notre société soient informées des opportunités que procurent la science quantique et les technologies qui en découlent, mais aussi des impacts du développement de ces dernières sur notre société et notre planète.

De même, il est important que les scientifiques soient en mesure de comprendre les impacts potentiels de leurs recherches, ainsi que les méthodes efficaces pour communiquer les résultats principaux de leurs recherches aux personnes en position de décision.

QUESTIONS DE RÉFLEXION

Questions de rétrospective suggérées après chaque phase :

1. Quelle a été l'importance des données probantes et de la science? Dans quelle mesure ont-elles été prises en compte dans la décision, en regard des autres considérations ?
2. La situation était-elle réaliste?
3. Certains enjeux ont-ils été omis?
4. Quel était le personnage le plus crédible?
5. Demander spécifiquement aux mentors de commenter le déroulement à leurs tables, et le produit final.

Questions suggérées lors de la réflexion finale sur les liens entre le milieu de la recherche et les gouvernements :

1. Qu'avons-nous appris de notre atelier?
2. Quelles initiatives devrions-nous envisager pour renforcer les liens entre le milieu de la recherche et les instances gouvernementales en matière de conseil scientifique?
3. Comment les scientifiques peuvent contribuer à l'usage des données probantes en politique?
4. Pareillement, comment les personnes dans l'appareil politique ou gouvernemental peuvent contribuer à l'usage des données probantes dans leurs décisions?

AUTRES RESSOURCES

(2020). Les cyberattaques visant le secteur canadien de l'électricité (Bulletin sur les cybermenaces). Centre canadien pour la cybersécurité.

Mosca, M., & Piani, M. (2022). 2021 Quantum Threat Timeline Report. Global Risk Institute.

Comandar, L., Bobier, J.-F., Coden, M., & Deutscher, S. (2021). Ensuring Online Security in a Quantum Future. Boston Consulting Group

CRÉDITS PHOTO

COUVERTURE : Programmation d'un algorithme quantique. Crédit : Institut quantique

Les auteurs tiennent à remercier Julie Dirwimmer, Ghislain Lefebvre et Martin Laforest pour leurs commentaires perspicaces.

International Network for Governmental Science Advice

À PROPOS D'INGSA

INGSA est une plateforme d'échange où les décideurs politiques, les praticiens, les membres de la communauté de recherche et des académies peuvent partager leur expérience, renforcer leurs capacités et développer des approches théoriques et pratiques, qui visent à renforcer l'usage des données probantes pour établir les politiques publiques à différents paliers gouvernementaux.

INGSA s'intéresse principalement à la place de la science dans l'élaboration des politiques publiques, plutôt qu'aux conseils sur la structure et la gouvernance des systèmes publics de science et d'innovation. L'organisation réalise sa mission de la manière suivante :

- L'échange de réflexions, de résultats de recherche et d'initiatives par le biais de conférences, d'ateliers et d'un site Internet ;
- La collaboration avec d'autres organisations lorsqu'il existe des intérêts communs ou concomitants;
- L'aide au développement de systèmes de conseil scientifique par le biais d'ateliers de renforcement des capacités ;
- La production d'articles et des rapports basés sur des recherches comparatives sur la science et la pratique du conseil scientifique.

Toute personne intéressée par le partage d'expériences professionnelles, le renforcement des capacités et le développement d'approches théoriques et pratiques en matière de conseil scientifique gouvernemental est invitée à rejoindre l'INGSA.

En vous inscrivant au réseau de l'INGSA, vous recevrez des mises à jour sur nos nouvelles et nos événements et vous serez informé des possibilités de participer à des projets de collaboration.

Rendez-vous sur http://www.ingsa.org pour plus d'informations.

L'INGSA a bénéficié du soutien de :
The Wellcome Trust ● Centre de recherches pour le développement international, Canada ● Royal Society London.

International Science Council

L'INGSA est une organisation internationale basée en Nouvelle-Zélande, hébergée à l'Université d'Auckland par Koi Tū : Centre for Informed Futures. Elle opère sous l'égide du Conseil international de la science.
A: PO Box 108-117, Symonds Street, Auckland 1150, New Zealand | T: +64 9 923 6442 | E: info@ingsa.org W: www.ingsa.org | Twitter: @INGSciAdvice