INSTITUT QUANTIQUE UdS

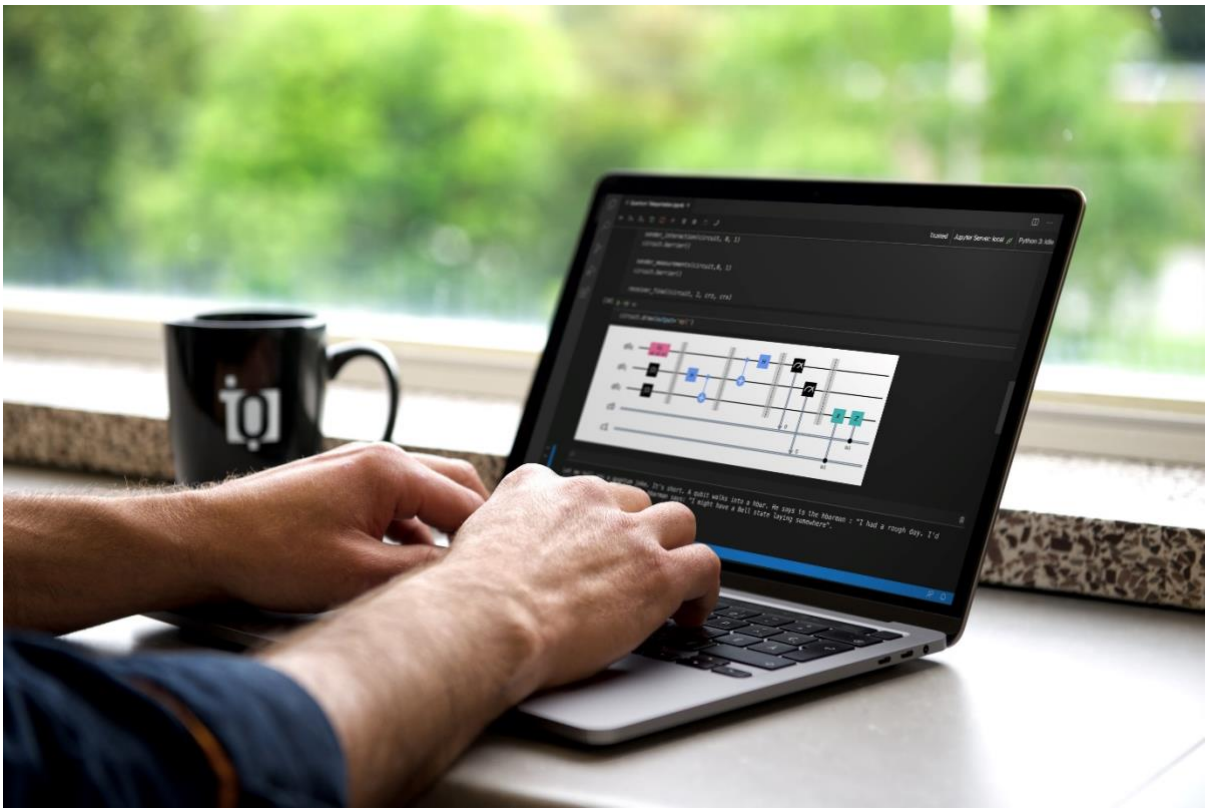
International Network for Governmental Science Advice

INGSA CASE STUDY

SARATERRA

Cybersecurity in the age of quantum computing

Written by: Karl Thibault, Jessica Baril and Christian Sarra-Bournet



PROGRAMMING A QUANTUM ALGORITHM

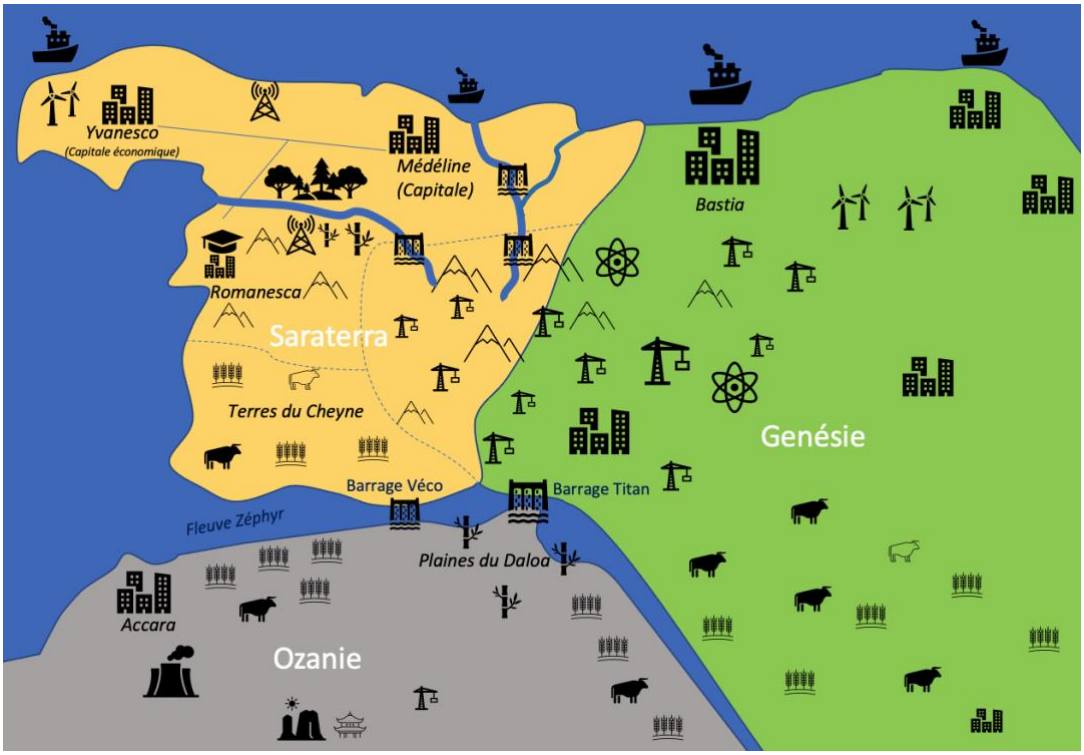
SARATERRA

Cybersecurity in the age of quantum computing

Note: the facts and data presented in this case study are fictitious and should not be taken to represent any real people, countries or events.

Saraterra

- **Political capital**: Medeline (2.5 million)
- **Commercial capital and economic centre**: Yvanesco (3.1 million)
- **Technology centre and university city:** Romanesca (350,000, of which 25% university community)
- **Area**: 1,256,000 km^2
- **Population**: 9,816,572
- **Population density:** 55% urban, 16% suburban, 29% rural
- **Ethnic groups:** 71=4% Saran, 12% Genois, 6% Ozan, 8% other
- **Official language**: Genois
- **Type of government**: Parliamentary democracy
- **GDP:** 435 billion dollars



MAP OF SARATERRA AND NEIGHBOURING COUNTRIES – 2022

Historical background

The Genois Empire came into being in 1472 with the conquest of the Saran territory to the west and Ozan to the south of the Zephyr River by the Genois Kingdom. The Saran and the Genois were trading peoples with many ports and exchanges with overseas territories, unlike the Ozan, a

nomadic people living off the river's abundant fish and edible flora. The cultural differences between the inhabitants on either side of the river resulted in marked differences of opinion, and the proud Ozan people became increasingly resistant to Genois authority.

In 1781, the rise to power of a new Ozan chief triggered a period of revolt. After several years of war and attempts to conquer territory on both sides of the river, a peace treaty was established in 1801 granting sovereignty to the Ozan (and the creation of Ozania), but the Genois people retained possession and the exploitation rights to the Zephyr River. The rest of the Genois Kingdom then became Genesia.

Years of conflict and war left their mark on the relationship between the Genois and the Ozan, and the loss of rights to “their” river created tensions in the Ozania community. The exploitation of the river by Genesia since that time has only further exacerbated international tensions.

In 1956, the commissioning of the Titan Dam flooded a section of the Ozan plains, which had many environmental impacts. The dam allowed Genesia to meet part of its growing energy needs and export the surplus to its two neighbours.

During the 1960s, the cultural differences between the Saran and the Genois grew more apparent. The Saran had a more social-democratic vision and a concern for the preservation of nature, and their desire for political independence grew stronger. In particular, they wanted to regain possession of their historic territory in the face of massive Genois mining projects. With international recognition of the Saran people already well established, and a territory rich in natural resources, Saraterra separated from Genesia and signed its declaration of independence in 1977. Relations have remained cordial between the two countries, which are now considered allies, with a free trade treaty and the retention of the Genois currency.

In 2001, Saraterra commissioned the Veco Dam which, unlike Titan, was designed after studies were carried out to evaluate the environmental and social impacts in order to avoid exacerbating political tensions and to establish more diplomatic relations with the Ozan. The Saran thus regained the respect of a portion of the Ozan population. However, energy agreements unfavourable to Ozania are still a source of diplomatic tension between the three states.

Ozania is currently experiencing an energy crisis, with 45% of its production coming from coal and natural gas, 30% from Genesia’s nuclear production, and 25% in the form of hydroelectricity from Genesia and Saraterra. In this context of historical resentment over the rights to exploit the river, relations with the Ozan are precarious. Beyond the political and economic rivalry between Genesia and Ozania, tensions over energy agreements are further tainted by historical animosities. Ozania’s totalitarian regime and the rise of militarization since the 1950s is of particular concern to the two northern countries, especially Genesia, which has never been able to defuse the anger caused by the Titan Dam.

Geography

Saraterra is mainly covered by temperate steppes, with scattered mountains in the west and a chain of alpine mountains to the east dividing the country into two climate zones. The north is boreal forest wilderness. The southeastern region is the country's agricultural breadbasket with most of the fertile land. The country is bordered to the north and west by the Fermi Sea. The main export ports are located in the cities of Medeline, the country’s political capital, and Yvanesco, its economic centre. A railway network connects the main centres with the more sparsely populated areas of the south, allowing the transportation of resources.

Economy

With its many ports and its strategic location, Saraterra's economy is historically based on the exploitation of its natural resources and overseas trade. Its western forests and mountain ranges are rich in iron, aluminum, silicon, copper and silver. Following independence, a large wave of nationalization swept the mining, forestry and energy sectors, allowing the country to regain control of its economy from foreign owners. In recent decades, falling metal prices and increased accessibility to resources have encouraged successive governments to transform the economy towards a service and high-tech economy concentrated in the country's major cities, notably in the university city of Romanesca.

This economic transformation has not been without its problems. While the western and northern regions near the capital enjoy a flourishing economy, the less densely populated southern and eastern regions feel abandoned. These regions have significantly higher unemployment rates and delays in the implementation of vital development infrastructure, such as a high-speed internet network. With 4% of the population living below the poverty line, the country's overall unemployment rate is 7%, but higher (11%) and rising in rural areas, particularly in the mining regions due to the slowdown in the sector. The situation has thus created a divide in the population with a more "progressive" world view in the major cities and a more "conservative" one in the regions.

With a literacy rate of over 91%, the population of Saraterra has always valued culture and education. The University of Romanesca has a worldwide reputation for excellence. The 1990s saw the birth of a social democratic movement and better social programs to bridge the gap between the rural and urban populations, as well as the reform of the education system with compulsory free schooling until the age of 16.

Politics

The party currently in power is the Saran Liberal Party (SLP), a liberal, centre-left, progressive party with a more interventionist, social-democratic vision of the state, focusing on renewable energy development and international relations. They were recently elected with the promise of boosting the country's economy: the recession in the mining sector and rising unemployment rates in the regions have led the SLP to want to consolidate a new economic strategy in order to minimize the risks of an economic crisis.

Since independence, the electoral system has been mainly bipartisan with the Fundamental State Party (FSP)—a conservative, centre-right party resistant to immigration with some far-right support and a non-interventionist vision of the state favouring the free market —as the other major party and currently the official opposition.

Other parties:

- Environment Party
- Loyalist Party (aiming for reunification with Genesia)
- Ozan Solidarity Party

Part 1 – The issue

Quantum cybersecurity – Summary prepared by the Chief Scientist and the Communications Security Council

In today's age of information, many of our most precious assets—finances, medical records and, to a large extent, identity—are protected by complex cryptography "keys". Current (or classical) cybersecurity is reliable because the encryption key used for an online transmission is based on mathematical problems that are extremely difficult to solve, even for the most powerful computers. Current cryptography protocols, such as RSA and elliptic curve cryptography (ECC), are based on the difficulty of factoring large integers or finding discrete logarithms.

However, a new type of computer, the quantum computer, has enormous disruptive potential despite the fact that it is still in the research and development stage. The science behind it is complex, but working prototypes are emerging from research groups around the world. The impact of quantum computers on cryptography will be major: using longer keys—the conventional way to increase security—will no longer suffice, and radically new methods will be needed to establish secure digital communications and identities. In the past, the question was whether quantum computers would become a reality. Now, the question is: "When, and where, will they become a reality?" Still, some critics continue to believe that the quantum computer is impossible to achieve.

If, within 10 years, powerful quantum computers become available, but it takes an organization 11 years to reorganize its infrastructure to become "quantum secure", it is already too late for that organization to resist the quantum threat. Furthermore, to protect information that was transmitted a given number of years ago from being compromised, the transition to quantum security techniques must be made at least that many years before quantum computers become available.

Fortunately, quantum science also provides a solution to this threat. Quantum cryptography can protect information in such a way that even a quantum computer cannot break the codes to access it. The solution, called "quantum key distribution" (QKD), is already available and used to protect large bank transfers and other communications. This technology is the first building block of a "quantum internet".

There is also an alternative solution, "post-quantum cryptography" protocols. Like current methods, they use conventional technologies and are based on assumptions about the intractability of certain mathematical calculations. These protocols protect against all known forms of quantum or conventional cryptographic attacks.

The consequences of not being prepared for a quantum attack could be enormous: the compromise and collapse of financial systems, energy networks, e-commerce and other infrastructures on which society depends.

In this context, Saraterra's Chief Scientist commissioned a quantum science expert and a cybersecurity expert to provide him with reports on the state of knowledge in quantum cybersecurity and the associated threats.

The Chief Scientist, in collaboration with the Saraterra Communications Security Council, has drafted three project proposals that address cybersecurity threats to varying degrees. These proposals are detailed below.

Proposal #1 – Focus on classical cybersecurity

Summary

Considering that the threat of quantum attack remains speculative, this proposal focuses on investing additional resources in classical cybersecurity. These investments are a continuation of the government's ongoing efforts towards a digital transition of services and industries, and will accelerate this transition through increased investment to protect existing assets.

Implementation costs and specific training needs

This proposal takes the form of a support program for Saraterra companies to help them enhance their classical cybersecurity capabilities as quickly as possible. No infrastructure costs will be required as existing infrastructures are sufficient.

This public-private partnership will match every public dollar invested with contributions from private companies interested in building classical cybersecurity capabilities. An additional $100 million will be used to enhance training programs to address the labour shortage in this sector.

Public investment ($1.1 billion)

- Public support program for job creation in classical cybersecurity: $1 billion
- Increasing the capacity of existing training programs: $100 million

Private investment ($2 billion)

- Funding for public cybersecurity jobs: $2 billion

Expected economic benefits

- Job creation: 5,000 jobs in the IT sector

These jobs will be spread across the country to achieve a digital transition on a national scale. The details of these jobs are already known and they can be created immediately if the labour force is available. There is also a high potential for economic immigration in this area, as the jobs are relatively low-skilled. The wages associated with these jobs will be moderate.

Expected international political impact

-

Expected protection

The investments made under this proposal will protect Saraterra's businesses from the cyber attacks of today and increase public awareness of cybersecurity. However, if the quantum computer becomes a reality, these investments will not protect against it.

Proposal #2 – Post-quantum Cryptography

Summary

Considering that the threat of quantum attack remains speculative, the risk and consequences associated with the status quo are too great not to act. This proposal focuses on creating new cryptographic and software standards to counter known quantum attacks. These investments will require the creation of new standards, their implementation in national cybersecurity protocols, and the training of cybersecurity and cryptography experts across the country in these protocols and quantum attacks.

Implementation costs and specific training needs

This proposal consists of the creation of a national cybersecurity research centre to drive the creation of new cryptographic standards within the next five years.

Public investment ($1.1 billion over 5 years)

- Creation of a national cybersecurity centre: $1 billion
    - Creation of new cryptographic standards: $900 million
    - Adaptation of existing training programs: $50 million
    - Creation of a continuing education program: $50 million
- Adoption of new cryptographic standards: $100 million
    - Updating of existing infrastructure

Expected private investment ($1 billion following the creation of the new standards)

- Adaptation and reorganisation of the information transfer network ($500 million)
- Corporate funding for quantum cybersecurity jobs ($500 million)

Expected economic benefits

- Job creation: 100 immediate jobs and up to 2,000 jobs in 5 to 10 years for the creation and growth of the new national cybersecurity centre
- Once the standards have been developed, their adoption across the varied sectors of our economy will require the involvement of engineering consulting firms as well as in-house cybersecurity and IT staff in many companies. We anticipate ~1,000 such jobs.

We recommend establishing this centre in the city of Romanesca, where there is already a concentration of quantum science and cybersecurity expertise to fill the new jobs that will be created. Future jobs in quantum cybersecurity will be created more broadly across the country. The wages associated with these jobs will be medium-high.

Expected international political impacts

The creation of new standards is an opportunity to make the country an international reference in quantum cybersecurity. It is possible to envisage the export of our standards and know-how beyond our borders and their adoption by our allies.

Expected protection

The protection achieved through this proposition will depend on the standards adopted. By adopting a strategy based on the creation of an expert working group, it is reasonable to expect protection against the most likely quantum attacks currently known. However, there is no guarantee of absolute protection in the more distant future, as a standard could also be “attacked” by new developments in quantum computing and algorithms.

Proposal #3 – Large-scale quantum internet (LSQI)

Summary

Considering that the threat of quantum attack remains speculative and that the risk and consequences associated with the status quo could be catastrophic, the *large-scale quantum internet (LSQI)* proposal, based on quantum key distribution, calls for a complete redesign of our communication systems. These investments will require a new infrastructure that is compatible with quantum information transfer technologies, a change in cryptography standards, and new training programs in quantum computing and cybersecurity.

Implementation costs and specific training needs

This proposal consists of a public-private partnership for the total reorganization of the information network and the implementation of new underground fibre infrastructures on a national scale, allowing the transfer of "quantum secure" information. This transition will require many disruptive actions, including major excavation work, over a 10-year period, with significant consequences for our country.

<u>Public investment ($20 billion over 10 years)</u>

- Creation of a quantum cybersecurity research centre ($5 billion)
    - Creation of new quantum cryptography standards
- Implementation of a nationwide quantum communication infrastructure ($13 billion)
- Creation of a quantum cybersecurity training program ($1 billion)
- Creation of a continuing education program ($1 billion)

<u>Private investment ($10 billion over 10 years)</u>

- Adaptation and reorganization of the information transfer network ($8 billion)
- Corporate funding for quantum cybersecurity jobs ($2 billion)

Expected economic benefits

- Creation of new businesses
- Job creation (~ 23,000 direct jobs) in several economic sectors
    - Scientific research and training: 2,000 (total after 10 years)
    - Engineering and manufacturing sector: 5,000/year over 5 years
    - Primary sector: 3,500/year over 10 years
    - Construction: 5,000/year over 10 years
    - IT and telecommunications: 10,000 (total after 10 years)
- Boosting the economy in the regions will have positives repercussions for merchants and citizens
- Retention of talent in the university city and increased employability rates in the Romanesca region

The jobs created will be located across the country, depending on the employment sector in question. Construction sector jobs will be widely dispersed to build the necessary quantum communication infrastructure between the country's major centres, while high-tech and computer jobs will be concentrated mainly in the city of Romanesca. The quantum technologies needed to deploy a *quantum internet* require rare earth elements found in the country's ore deposits. The details of some of these jobs are unknown, as they will be in new services and businesses. The wages associated with these jobs will range from medium (construction, manufacturing and mining industries) to high (research, IT and telecommunications).

Expected international political impacts

The creation of new standards is an opportunity to make the country an international reference in quantum cybersecurity. It is possible to envisage the export of our standards and know-how beyond our borders and their adoption by our allies.

Expected protection

This proposal promises absolute protection, even in the event of the emergence of a universal quantum computer. However, quantum key distribution technology is still in the research and development stage.

Summary Table

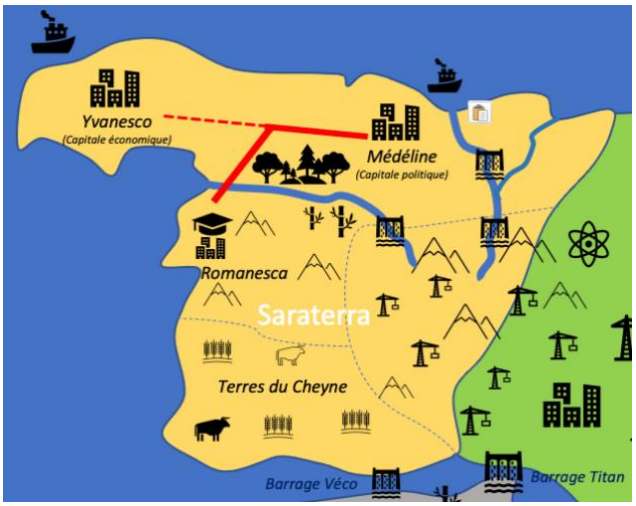
Proposal	1 – Traditional cybersecurity	2 - Post-quantum cryptography	3 – Large-scale quantum internet
Major actions	Classical cybersecurity support program	Creation of a national cybersecurity centre	1. Creation of a quantum cybersecurity research centre 2. Public-private partnership for the implementation of a national quantum telecommunications infrastructure
Job creation	~ 5,000 IT jobs	100 to 2,000 jobs within 5 years at the national cybersecurity centre 1,000 jobs in companies resulting from the adoption of the standards across the country (Training and public sector)	Research and training (2,000) Engineering and manufacturing sector (5,000) Primary sector (3,500) Construction (7,000/year over 5 years) IT and telecommunications (5,000) Training and public sector (500) Total: ~ 23,000 direct jobs
Public investment	$1.1 billion	$1.1 billion	$20 billion
Private investment	$2 billion	$1 billion	$10 billion
Implementation	Immediate	5 years	10 years
Increase in GNP ($435 billion)	~ 735 million (0.2%)	~ 300 million (0.1%)	~ 3.2 billion (0.75%)
Where the investments will be made	Across the country	Mostly in Romanesca and other large cities	Everywhere (network infrastructure) In the regions (mining sector) Large cities (high-tech jobs)
Maturity of the technology	High	Medium	Low
Level of cybersecurity	Low	Medium	High
Level of risk and return on investment	Low	Medium	High

Part 2 – The issue

It is May 2030, 8 years after the large-scale quantum internet (LSQI) project was adopted by the Saran Liberal Party (SLP) government in 2022.

Background to the LSQI 2022-2030 project

During the research and development phase (2022 to 2027), it quickly became clear that the scope of the LSQI project had been completely underestimated. The transition from concept to a mature and robust technology required far more time and resources than anticipated. In spite of this, the Saraterra Cybersecurity Centre (SCC) is now operational with close to 1,500 research staff and the project has generated over 3,700 jobs.



Production of the LSQI infrastructure and the specialised equipment required for its installation began in 2025 and the excavation work for the underground lines was initiated in the summer of 2026. In the summer of 2027, in preparation for the start of construction and installation of the line between Romanesca and Medeline, concerns about water system preservation increased and demonstrations organized by the Environment Party put pressure on the government. Changes were made to the infrastructure plan in order to pass over the Great White River, with the addition of a major diversion of the Romanesca line to protect the local ecosystem, resulting in further cost overruns.

Moreover, the public saw the majority of the project's revenues going to companies based outside the country and regarded most of the jobs generated as short-term. Rumours of corruption among construction contractors exacerbated negative opinions of the project, and the view that the project was a waste of public money spread among the population.

November 2029 election

Taking advantage of growing opposition to the project and concerns about the risk of a global economic crisis, the opposition parties quickly became critical of the LSQI project, portraying it as an indecent and corrupt expense. During the autumn 2029 electoral campaign, the Fundamental State Party (FSP) promised to terminate the project and conduct an investigation into the construction industry. The FSP argued that the funds needed to complete the project should be used to strengthen the country's manufacturing economy.

Benefitting from popular discontent and the erosion of the SLP's power, the FSP won the election with 51% of the vote, with most of their support coming from Medeline and the regions. The Environment Party won a record number of seats (24% of the vote), leaving the SLP in last place with 20% of the vote. The election highlighted the sharp divide between the big cities and the rest of the country: in Romanesca and Yvanesco, where the majority of the jobs related to the project were concentrated, there was strong support for its continuation. In the political capital of Medeline, opinions were more mixed, but the majority (62%) were against the project. In agricultural areas, most voters were opposed to the project, and in the mining region, opinions were more divided.

Part 3 – The issue

It is June 2031, one year after the decision by the FSP to stop the LSQI project.

Cyber attack on a critical energy infrastructure

This morning, June 13, 2031, a twelve-hour (midnight to noon) power failure was reported near Yvanesco, affecting 50 factories and 50,000 customers. A hospital was impacted and was forced to use its emergency generator, reducing treatment capacity and increasing the visibility of the event. It made the front page of every newspaper in the country; citizens and businesses are demanding an explanation.

It is now 2 p.m. and the situation is under control, despite economic losses estimated at over $30 million.

Around 9 a.m. this morning, the government received a message from hackers claiming responsibility for the outage. They allegedly attacked the country's main power control centre, located on the incomplete LSQI line near Yvanesco, and redirected the power flow to Ozania. They are giving the government until 4 o'clock to meet the following demands, failing which they are threatening a widespread blackout of Yvanesco:

1. A $100 million ransom.
2. Recognition of Ozania's territorial sovereignty over the Zephyr River.
3. Renegotiation of energy agreements between Saraterra and Ozania.
4. The removal of duties on goods from Ozania.

Situation in government

The government has requested an urgent update from the Saraterra Cybersecurity Centre on their cyber defence capabilities and the details of the attack, which was given to the Minister of National Security. You now know that the attack is believed to have come from an extremist cell in Ozania, known to be funded by the Ozan government. You have no information as to whether they are acting under orders from Ozania, or whether they are pursuing their own agenda independently of those in power.

The Prime Minister has called an emergency meeting of the Council of Ministers to establish a strategy for responding to the hackers and a strategy for communicating with the population.

The Ozan President has been in power for almost 15 years. Few dare to oppose the current regime, and it is generally accepted outside Ozania that the country is under a dictatorship.

Case Study Exercises

Part 1 – Exercises

Phase 1 - Evaluation of competing technologies for protecting data against quantum attacks

The year is 2022. The Saran Liberal Party is in power.

The Chief Scientist has produced a summary report on quantum cybersecurity, which you have in your possession. This report was commissioned by the Minister of Science, Economy and Innovation to guide the development of Saraterra's cybersecurity strategy. Over the course of three simulations, you will assess the scientific, social and economic potential of the projects and decide which project will be funded by the Ministry of Science, Economy and Innovation.

The following roles will be assigned to the different tables for this phase:

1. A quantum scientist
2. A cybersecurity scientist
3. Chief Scientist of Saraterra
4. Deputy Minister for Strategic Industries
5. Chief of Staff to the Minister of Science, Economy and Innovation
6. Minister of Science, Economy and Innovation

Three simulations will be played during this phase. You have 30 minutes to prepare as a group. Only one person from your table will play your assigned role during the simulations.

Simulation #1 (15 minutes)
Objective: Technology assessment
Tables involved: 1,2,3

The Chief Scientist meets one last time with his expert colleagues in quantum science and cybersecurity to determine his own position based on the scientific validity of the projects.

Simulation #2 (15 minutes)
Objective: Assessment of the social, political, environmental and economic impacts
Tables involved: 4,5

The Chief of Staff to the Minister of Science, Economy and Innovation seeks to determine the potential impact of each project from a social, political, environmental and economic point of view, in order to advise the Minister.

Simulation #3 (15 minutes)
Objective: Project selection
Tables involved: 3,5,6

The Minister of Science, Economy and Innovation meets with her Chief of Staff and the Chief Scientist to make a final decision. She then participates in a media scrum.

Part 2 – Exercises

Cost overruns and alleged quantum cyber attack in an allied country: Decision on whether to continue the project

It is 2030, 8 years after the adoption of the large-scale quantum internet project (LSQI – Project #3 of Phase 1) by the Saran Liberal Party (SLP) government in 2022. The Fundamental State Party (FSP) has just won the election and overthrown the SLP government, which had been in power for 12 years. In addition, the rumor of a cyber attack in Genesia has recently spread in the Genois media. Immediately after coming into power, the FSP commissioned a general report on the current state of the project, proposing two action plans. You are also aware of the existence of a preelection report by the Saraterra Cybersecurity Centre (SCC) outlining our knowledge of the rumoured cyber attack in Genesia.

The report containing the action plans for the LSQI also presents budgetary data and the impacts of continuing or discontinuing the LSQI project.

Over the course of three simulations, you will have to discuss and decide the future of the project while assessing the risks involved. The following roles will be assigned to the different tables for this phase:

1. Leader of the opposition (SLP)
2. Chief of Staff to the Prime Minister (FSP)
3. Minister of International Relations (FSP)
4. Minister of National Security (FSP)
5. Prime Minister (FSP)
6. President of the Saraterra Cybersecurity Centre

Simulation #1 (15 minutes)

Objective: Determine the probability of an imminent cyber attack on our country.

Tables involved: 3,4,6

The Minister of National Security convenes the Minister of International Relations and the President of the SCC to determine whether he should expect Saraterra to be the target of an imminent attack, in order to advise the Prime Minister in the next simulation.

Simulation #2 (15 minutes)

Objective: Decide whether the FSP will continue the project and prepare for the subsequent question period in the House of Commons.

Tables involved: 2,4,5

The Prime Minister must decide whether to keep his promise to stop the LSQI project, considering the social situation (represented by his Chief of Staff) and national security situation (represented by the Minister of National Security). This decision will have to be defended in the next simulation.

Simulation #3 (15 minutes)

Objective: Question the FSP (party in power) on their decision made in the previous simulation during a House of Commons debate

Tables involved: 1,5

The leader of the opposition (SLP) conducts a question period on the decision made by the FSP to continue or discontinue the LSQI project.

Part 3 – Exercises

Attack on a critical electricity infrastructure: Crisis management

The year is 2031, one year after the FSP government's decision to put a definitive end to the LSQI project, a choice supported by the people of Saraterra.

A cyber attack has taken place on Saraterra's main power control centre. Thousands of citizens experienced a power outage lasting several hours, and general concern is growing among the population. A ransom has been demanded by an extremist cell in Ozania known to your intelligence services, in addition to demands for Ozan exploitation rights to the Zephyr River, failing which the attackers threaten to cause a prolonged widespread power outage.

Your objective is to manage this crisis by establishing both the government's response strategy and a strategy for communicating with the people of Saraterra.

The following roles will be assigned to your tables for this phase:

1. Minister of Public Security
2. Prime Minister of Saraterra
3. Minister of Finance
4. Minister of international Relations
5. Minister of National Security
6. Press Secretary to the Prime Minister of Saraterra

Simulation #1 (20 minutes)

Objective: Establish a strategy for responding to the attackers and a strategy for communicating with our population.

Tables involved: 1,2,3,4,5

Saraterra's ministers are convened by the Prime Minister to determine under what circumstances Saraterra will pay the ransom and determine what message to send to the population.

Simulation #2 (10 minutes)

Objective: Send a clear message to the people of Saraterra informing them of the measures put in place by your government.

Tables involved: 2,6 (see below)

This simulation will be divided into three parts:

2 minutes: Draft the Prime Minister's message to the population based on the previous interactions, and determine the format of the message
2 minutes: Statement by the Prime Minister
6 minutes: Questions from journalists

Appendix A – Action plans for the LSQI

Phase 2 – Given to Tables 2 (Chief of Staff) and 4 (FSP Prime Minister)

Plan A: Continuing the LSQI project

Estimated public investment for the LSQI project now stands at $42.7 billion, representing a cost overrun of $12.7 billion compared to the initial budget. An additional $3.1 billion is needed to complete the line between Romanesca and Medeline, and construction of the branch line to Yvanesco (economic centre) requires an additional investment of $12.2 billion, bringing the total cost of the project to $58 billion, almost double the initial budget.

Completion of the project would support 11,642 current direct jobs by the time the network is commissioned in 2035 and would generate 4,400 additional IT jobs in 2030-2035. The operation of the network would provide 9,750 permanent jobs after 2035, for a period of at least 10 years. Wealth creation (excluding indirect benefits) would average $2.5 billion (including $1.85 billion in payroll) over 5 years, an amount equivalent to about 0.6% of the country's GDP, and $1.7 billion after the commissioning. Balancing the budget following public investment in the LSQI would take just under 15 years.

Plan B: Stopping the LSQI project and diversifying the economy

The Fundamental State Party's "Strategic Plan" proposes an immediate halt to construction work and the suspension of the activities of the quantum cybersecurity research centre and the adoption of the traditional cybersecurity support program, requiring public investment of $1.1 billion.

Some manufacturing and primary sector jobs would be at risk if the project is stopped. The government therefore plans to provide $1.5 billion in subsidies to businesses to help them make the transition to the production of essential goods. However, in the medium term (5-10 years) these sectors should grow significantly thanks to the country's increased self-sufficiency in goods production and the reduction of imports. This plan would maintain 10,940 jobs ($1.73 billion in payroll) spread across the regions.

In the short term, the resale of LSQI infrastructure to private companies could generate $7.8 billion, making it possible to reduce the country's debt and maintain its social programs.

The projected increase in GDP in the medium to long term is $3 to $5 billion/year over at least 15 years, or 2% of the country's GDP. Taking into account government revenues, balancing the budget following public investment in the LSQI would take less than 5 years.

Summary Table – Economic projections of the two scenarios

	Continuation of the LSQI	**Discontinuation of the LSQI**
Additional investments	$15.3 billion	$2.6 billion
Contribution of the investment to the national debt	3.5% of GDP	0.6% of GDP
Estimated return to a balanced budget	15 years	5 years
Jobs (location)	Temporary, 2030-2035: ~16,000 (nationwide) Permanent, after 2035: 9,750 (urban centres)	10,940 (nationwide)

Special report: Saraterra Cybersecurity Centre (SCC)

Phase 2 – Given to Tables 4 (Minister of National Security) and 6 (President of the SCC)

Report dated April 10, 2030, before the Saraterra national election

For the attention of the Minister of National Security

Executive summary:

- Our national security team has detected cyber attack signatures in Genesia;
- The cyber attacks targeted energy sector infrastructures;
- An extremist cell in Ozania is the prime suspect;
- Our intelligence confirms that there is a real risk that our electricity infrastructure is a potential target;
- We estimate a 75% chance that the attackers have discovered a computer vulnerability in Titan's cyber defences and a 25% chance that they have access to a hitherto unknown computer system (specifically, there is a real possibility that they have a quantum computer);
- Our current protection is insufficient against similar attacks;
- The existing partial LSQI network does not protect financial data between Medeline and Yvanesco.

The risk of a quantum cyber attack has increased considerably in the last year, to the point of becoming a threat to our country.

Background

On June 18, 2029, the electricity produced by a minor power plant in Genesia was suddenly redirected to a different line for a period of 40 seconds. The problem was attributed to a failure of the power processing optimization system.

On November 7, 2029, the same thing occurred at the Titan electric dam in Genesia, but for a period of 180 seconds. This caused minor power outages for more than one million customers in Genesia.

Following this second event, Genesia's cybersecurity experts conducted an investigation, focusing on an Ozan extremist cell known for its claims concerning Ozania's "inherent rights" to the Zephyr River and thus to the hydroelectricity generated by it.

Nobody has claimed responsibility for the attacks.

Given the level of sophistication of the attacks, it is highly unlikely that they were carried out by a group of amateur hackers without the support of a government or large-scale industrial espionage organization.

Intelligence suggests that Ozania has a secret defence project on cyber warfare. There are also rumours that the country has been investing in a secret R&D program to develop unparalleled computing power for the past 10 years.

Analysis

These cyber attacks are impossible with the known computing capabilities of Ozania. It would take the world's most powerful supercomputer several years to overcome the cyber defences of Titan's system. The attackers therefore appear to have found a major vulnerability in Titan's cyber defences, or have access to a hitherto unknown computer system.

There is a non-zero possibility that a quantum computer has been developed and that this organization has access to it. According to our analyses, it would have needed at least 400 logical qubits to have been able to breach Titan's cyber defences.

One hypothesis is that the event of June 18, 2028 was a test carried out on a less resistant computer system. Indeed, by comparison, the cyber defences of the minor plant could be breached by a quantum computer with about 20 logical qubits.

No other known computer system has the capacity to break the cyber security codes currently in use. It is possible that the attackers have succeeded in developing a new kind of system, although the probability is very low.

No such attacks have been recorded in Saraterra. However, it is possible that a very brief attack may be undetectable. It is difficult to predict when the next attack will take place, as all that is known is that the two previous attacks occurred about 10 months apart, but it could happen within the next few months.

Taking all this information into account, we estimate a 75% chance that the attackers have discovered a computer vulnerability in Titan's cyber defences and a 25% chance that they have access to a hitherto unknown computer system (probably a quantum computer).

Protection status

The cyber protections currently in place are not sufficient to defend against an attack such as the one described above if it is carried out by a quantum computer.

The LSQI network currently under construction would technically protect our critical systems against this type of attack. However, it is imperative that the cybersecurity managers of the infrastructures at risk work with SCC specialists to ensure that the protocols put in place are secure and that these infrastructures are included in the protection system.

Specifically, we recommend that the SCC contact the cybersecurity managers of our electricity infrastructures as soon as possible to re-examine our cyber defences for any possible vulnerabilities.

Meanwhile, the partial LSQI network does not currently protect the majority of the country's financial information, which travels between Medeline and Yvanesco. With the collaboration of the Ministry of Science, Economy and Innovation, it has been estimated that the daily losses of a cyber attack on Saraterra's financial system would amount to $3.4 billion/day.

Given the worst-case possibility that an enemy entity gains access to a functioning quantum computer, it is crucial that we continue the research carried out at the SCC and expand our espionage activities to counter this threat.

Some of the information in this document is from highly trusted international partners with whom we have robust confidentiality agreements.

Special report on Ozania

Phase 2 – Given to Table 3 (Minister of International Relations)

Phase 3 – Given to Table 4 (Minister of International Relations)

Report of the Saran Ambassador to Ozania for the Minister of International Relations – May 2030

Socioeconomic situation in Ozania

The former ruling Saran Liberal Party (SLP), which always had a strong focus on international relations, maintained close ties with Ozania, its second-largest economic partner.

However, rising rates for hydroelectricity sold to Ozania, duties on exports and increasing prices for certain metals have undoubtedly contributed to the crisis in Ozania's manufacturing sector. In the context of destabilized global markets, Ozania's GDP decreased by 9.8% in the 4th quarter of 2028, marking the start of an economic crisis. With unemployment rates on the rise, the country has seen a decline in the average standard of living and a significant increase in food bank applications and crime rates, particularly in the major cities. The economic situation has also caused a wave of Ozan immigration to Saraterra since 2027.

Following the second increase in Saraterra's hydroelectricity rates, the Ozan President attempted to negotiate with Genesia for a reduction in its energy prices, but the Genois government remained unmoved, if not indifferent, to the Ozans' plight.

Furthermore, the Saraterra Fundamental State Party (FSP) intends to develop greater self-sufficiency in the production of goods and establish new protectionist policies, reducing immigration to favour employment for Saran citizens, and plans to tax imports of agri-food products and increase duties on its exports. These measures are likely to have additional negative impacts on Ozania.

Ozania's military-technological ambitions

Ozania's totalitarian regime has been a concern for the northern countries for years, especially since the current president came into power in 2017. Despite the country's economic difficulties, the military budget has continued to increase (from $43.9 billion in 2019 to $65.8 billion in 2029). Furthermore, in 2021, the Ozan government allocated unprecedented sums to research. With $66.9 billion in fundamental and applied research, $72.5 billion for experimental technology development, and 500 million for programs to attract talent to the South, the President has clearly highlighted his ambitions to restore Ozan pride by positioning the country at the forefront of technological development, with a strong military and protectionist diplomacy.

With the Ozan President blaming northern countries for the country's economic crisis, the Ozan people are convinced that their neighbours are to blame for their difficulties. Acts of vandalism by Ozan in the political capitals of Genesia and Saraterra (hateful graffiti against the Genois and Saran leaders) indicate the bitterness of the people and their anger towards the lack of empathy shown by the northern countries. In Ozania, extremist movements continue to claim exploitation rights to the river, with the belief that the river's power plants should belong to the Ozan. The Ministry of Public Security in Saraterra has also noted suspicious activities revealing evidence of funding from unspecified private interest groups to finance extremist cells.

Update – Special report: Saraterra Cybersecurity Centre (SCC)

Phase 3 – Given to Table 5 (Minister of National Security)

For the attention of the Minister of National Security – June 13, 2031

Cyber attack

At midnight on June 13, 2031, a cyber attack targeted the Saraterra electricity control centre. Hackers diverted the flow of electricity to an industrial district near Yvanesco and redirected it to Ozania, affecting 50 factories and 50,000 customers from midnight to noon.

The hackers belong to an extremist cell in Ozania. Intelligence appears to indicate the presence of a secret Ozan defence project on cyber warfare.

The hackers contacted the manager of the electrical control centre at about 8:30 this morning by email. This email contained their demands:

- A $100 million ransom;
- Recognition of Ozania's territorial sovereignty over the Zephyr River;
- Renegotiation of energy agreements between Saraterra and Ozania;
- The removal of duties on goods from Ozania;

Their threats:

- Take full control of Saraterra's electricity management;
- Redirect 25% of the electricity generated to Ozania;

And how to contact them:

- Deposit money into QubitCoin cryptocurrency account #010010110100001;
- Make a televised announcement on Saraterra national television outlining the actions taken in response to the cell's demands, no later than 4 p.m.

Protection status

Saraterra's electricity control centre is located on the unfinished LSQI line, otherwise we might have been able to defend ourselves against this attack. Our staff reviewed all the protections in place on the power grid in early 2031 and found no vulnerabilities.

According to our analysis, the chance of this cell having access to significantly enhanced computing capabilities (such as those of a quantum computer) is now 65%. The known state of quantum computers, however, reduces the likelihood of such an accomplishment. We therefore estimate that there is a 35% chance that the hackers are exploiting a vulnerability that we did not know existed, and our staff have been mobilized to find it.

As a result, we are currently unable to defend ourselves from cyber attacks by these hackers.

We recommend that the government take political action as soon as possible to reduce the risk of retaliation by these hackers.

If we do not meet their demands, a plan will have to be put in place to completely disconnect the control centre from the internet. We are already in communication with the senior manager in this regard.

Suggested program for the day

Part 1 – Workshop

8:00 – Arrival of guests and networking breakfast

8:30 – Welcoming remarks

9:00 – Case study, Phase 1

10:30 – Break

10:45 – Case study, Phase 2

12:15 – Lunch

1:00 – Presentations

2:00 – Case study, Phase 3

3:45 – Break

4:00 – Discussion on the links between government and the research community

4:30 – End of workshop

Remark on science advice

As we enter the third decade of the 21st century, quantum technologies are ranked among the scientific developments that have the potential to revolutionize the world, due to their radical departure from today's technologies.

Perhaps the best-known application of quantum computing is Shor's algorithm for finding the prime factors of an integer, a task that is extremely difficult to perform on a conventional computer. The majority of our cryptosystems are based on the impossibility of factoring large numbers in a reasonable time with our current tools. The implementation of Shor's algorithm on a sufficiently powerful quantum computer would therefore make any information currently protected by existing cryptographic protocols vulnerable. This potential application of the quantum computer raises ethical questions on several fronts (military, economic, privacy, etc.) and a number of institutions are vying for rapid and privileged access to such a tool.

It is important that those in decision-making positions in our society are informed of the opportunities offered by quantum science and its attendant technologies, as well as the impacts of developing these technologies on our society and our planet.

It is also important that scientists are able to understand the potential impacts of their research, and effective methods of communicating the key findings of their research to those in decision-making positions.

QUESTIONS FOR DISCUSSION

Suggested follow-up questions after each phase:

1. How important was evidence and science? To what extent were they factored into the decision, relative to other considerations?
2. Was the situation realistic?
3. Were any issues omitted?
4. Who was the most credible character?
5. Ask the mentors to comment on how the activities unfolded at their tables, and the final product.

Suggested questions during the final discussion on the links between government and the research community:

1. What did we learn from our workshop?
2. What initiatives should we consider for strengthening ties between government and the research community in terms of science advice?
3. How can scientists contribute to the use of evidence in politics?
4. Similarly, how can people in politics or government contribute to the use of scientific evidence in their decisions?

OTHER RESOURCES

(2020). The cyber threat to Canada's electricity sector (Cyber Threat Bulletin). Canadian Centre for Cyber Security.

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

PHOTO CREDITS

COVER: Programming a quantum algorithm. Credit: Institut quantique

The authors wish to thank Julie Dirwimmer, Ghislain Lefebvre and Martin Laforest for their insightful comments.

International Network for Governmental Science Advice

ABOUT INGSA

INGSA is a forum where policy makers, practitioners, national academies, and academics can share experience, build capacity and develop theoretical and practical approaches to the use of scientific evidence in informing policy at all levels of government.

INGSA's primary focus is on the place of science in public policy formation rather than advice on the structure and governance of public science and innovation systems. It achieves its mission by:

- Exchanging lessons, evidence and new concepts through conferences, workshops and a website;
- Collaborating with other organisations where there are common or overlapping interests;
- Assisting the development of advisory systems through capacity-building workshops;
- Producing articles and discussion papers based on comparative research into the science and art of scientific advice.

Anyone with an interest in sharing professional experience, building capacity and developing theoretical and practical approaches to governmental science advice is welcome to join the INGSA network.

By signing up to the INGSA Network you will receive updates about our news and events and learn of opportunities to get involved in collaborative projects with other INGSA network members.

Visit http://www.ingsa.org for more information.

INGSA has received financial support from:
The Wellcome Trust ● International Development Research Centre, Canada ● Royal Society London.

International Science Council

INGSA is a New Zealand-based international organisation hosted at the University of Auckland by Koi Tū: Centre for Informed Futures. It operates under the auspices of the International Science Council.
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