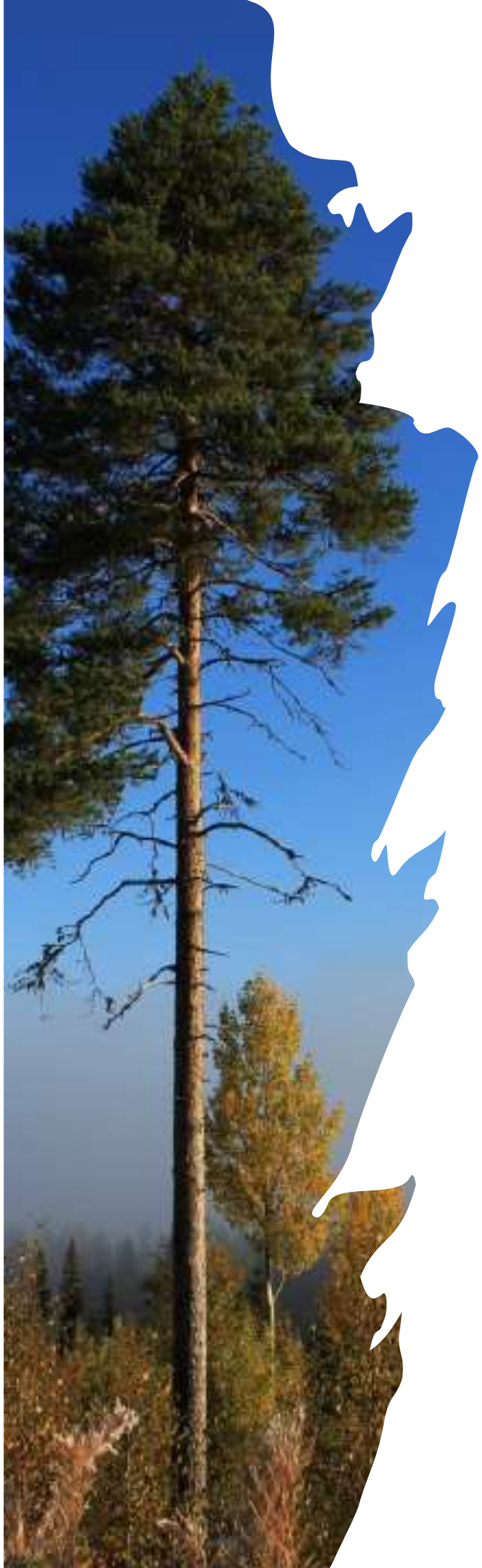


Tabletop Exercise (TTX)

Foreword

Foreword

The Nordic Pine 2024 Tabletop Exercise (TTX) represents a significant step in enhancing our collective resilience in the face of modern hybrid threats and energy security challenges. This exercise package is designed not only to provide a structured, scenario-based learning environment but also to inspire and guide future exercises. The materials contained within this package cover a comprehensive array of injects, scenario overviews, participant handbooks, response forms, and summaries, offering a full picture of the complexity and dynamics faced by the participants during the exercise.

Inside this package, you will find:

- Detailed scenario descriptions that simulate the geopolitical, cyber, and energy security challenges.
- Inject response forms capturing the decisions and strategies employed by the various teams.
- Key takeaways and lessons learned, designed to help organizations reflect on their own preparedness.
- Supplemental materials such as presentation slide decks and communication templates to aid in creating your own exercises or developing further training modules.

We hope that this exercise package serves as a valuable tool for those looking to strengthen their strategic, operational, and tactical responses to crises, both in the energy sector and beyond. We encourage you to use this as a foundation to build upon, customize, and integrate into your own training programs.

I would like to extend my heartfelt thanks to Anton Lif, who has played an instrumental role in developing and refining this material, bringing it to its final form. Special thanks also go to Freddy Jönsson Hanborg for his leadership and collaboration in running the exercise. Their expertise and dedication have been pivotal to the success of Nordic Pine 2024.

Finally, I urge all participants and readers to continue fostering a culture of training, learning, and collaboration. The challenges we face are complex, but through exercises like these, we can enhance our readiness and ensure a resilient future.

Sincerely,

Carl Heath
Deputy Exercise Director, Nordic Pine 2024
Senior Researcher, RISE

Contents

PLAYER HANDBOOK

SAS 191 - Nordic Pine 2024

2024-09-12, Version 1.1

Content

1. Introduction

The Player's handbook is created to set the scene and provide the participants with key essentials before entering the NORDIC PINE 2024 TableTop Exercise (TTX). It is designed to offer a comprehensive overview without delving into advanced complexities. The focus is on ensuring that all participants, regardless of their prior experience, have the necessary information and context to engage effectively in the exercise.

Welcome to NORDIC PINE 2024, where we collectively enhance our preparedness and resilience in the face of evolving energy security challenges.

2. The most essentials

2.1 Preparations

- Ensure that you are registered to the desired site – *Jönköping or Espoo or Online*.
- Take part of, site specific, General Information Package (GIP) – *Jönköping or Espoo*.
- Installation/test of Cisco Webex - *The exercise primarily utilizes Webex for communication. Microsoft Teams will be used as back-up.* Link to the meeting will be sent out later.
- Bring own laptop, headset.
- Prepare media spokespersons - *International and national media will visit the exercise. The respective actor is asked to prepare spokespeople who can stand up for interviews, etc.*

2.2 Program

Program: *See next page, 5*.

Complementary information - some clarifications:

- On-site start: 08:00 CET Jönköping and 09:00 EEST, Espoo.
- Online, common start-up for all participants (in Jönköping, Espoo, and online) at 03:00 EDT / 10:00 CET / 11:00 EEST – *Webex link to the meeting will be sent out later.*
- On the morning (Sweden and Finland) of the 25th there will only be on-site activities. The TTX restarts online at 07:00 EDT / 13.00 CET / 14.00 EEST.
- On-site specific timings, such as timings for the study visits will be addressed separately by the site directors.

2.3 Media

Under the management of the NATO Public Diplomacy Department (NATO PDD), international and national media outlets will visit the exercise. Notably, they will be present in Jönköping from September 24th to 26th. Additionally, there are plans for both physical and digital participation in Espoo. The media coverage may include international print and online outlets, as well as national media from Sweden and Finland. As there is a pronounced interest in being able to conduct interviews with participating actors, both in Jönköping and Espoo, respective actor (training audience, observers, lectures) is asked to prepare spokespeople.

2.4 Global ECCO

Representatives from the Naval Postgraduate School (NPS) and Global ECCO will be facilitated the Global ECCO game as an (on-site) icebreaker. With the aim to facilitate increased communication and collaboration within the Training Audience (TA) small groups at each training site. Global ECCO has developed over 18 strategic online gaming applications with a focus on irregular warfare, hybrid threats, strategic competition, and other topics relevant to Regional Defence Fellows and alumni.

Read More: Global ECCO - Global ECCO - Naval Postgraduate School (nps.edu)

Nordic Pine 2024 – TTX Program 23-27th September

Time EDT/CET/EEST	23 SEPTEMBER	24 SEPTEMBER	25 SEPTEMBER	26 SEPTEMBER	27 SEPTEMBER
02.00/08.00/09.00	*Travel*	Welcome, startup (On-site) Global Ecco – *Onsite only JÖNKÖPING and ESPOO*	*Local study visits:* • *JÖNKÖPING* • *ESPOO*	TTX - Inject Based Decision Training	
03.00/09.00/10.00					AAR Brief
04.00/10.00/11.00		Welcome, opening remarks			
05.00/11.00/12.00		Preparatory Lecture: Introduction to Hybrid Threats		Completing Scenario and Initial Feedback	DV & Media
06.00/12.00/13.00		*BREAK*	*BREAK*	*BREAK*	
07.00/13.00/14.00		TTX - Inject Based Decision Training	Keynote: Daniel Mortensen	Keynote: Sarah Lohman	*Travel*
08.00/14.00/15.00			TTX - Inject Based Decision Training	Review and Reflection: Group Discussions and Lessons Learned	
09.00/15.00/16.00					
10.00/16.00/17.00		Keynote: Enrique Kremers	Keynote: Peter Burgherr	Closing remarks	
11.00/17.00/18.00	*Icebreaker*			*Final Dinner*	

2.5 Expert lectures

The following senior subject matter experts will be present during parts of the exercise and will each give a keynote.

Dr Enrique Kremers
Topic: *"Energy Transition & Critical Infrastructure Protection: Highly Decentralized and Intelligent Energy Systems"*

Dr Enrique Kremers is an expert in the simulation of complex systems, currently working with IABG, a leading engineering and tech-consultancy firm in Germany. With over 15 years of experience, in senior roles such as *Head of Complex Systems Research* at the European Institute for Energy Research (EIFER) and *Expert for Complex Energy Systems & Simulation* at EDF he is specialized in developing innovative solutions for energy, infrastructure, and operations using simulation methods and digital twins. His core competencies include complexity science, swarm intelligence, digitized energy systems, and business intelligence.

Daniel Mortensen
Topic: *Offshore Wind Defence & Security*

Daniel Mortensen has worked with Operations & Maintenance, Business Development, Project Management, and Business Implementation for 14 years, gaining experience from a large variety of organizations and high-tech systems. He has a master's degree level of Military Science, including the management of advanced technology projects from the Royal Danish Defense College. His educational qualifications are further developed through experience in identifying, developing, and managing technological and organizational projects. This includes the process from capturing project ideas and bringing them to the initial Business Case/Plan level to delivering according to project and business specified performance criteria. In recent years, he has been with DONG Energy, Wind Power, in roles such as Windfarm Package Manager, Project Management support, Offshore Logistics business development, Team Lead for setting up a new organizational unit, Deputy Project Management, and Project Management. He holds the rank of Navy Commander (MBA) with a background in Submarines, Special Forces, and National Armament. He is skilled with Prince2, PMI, and Military Decision-Making Models for project management.

Peter Burgherr
Topic: *Drivers, barriers and systemic impacts of large-scale renewable deployment: Wind Power in Europe.*

Peter Burgherr joined the Paul Scherrer Institut (PSI) as a risk analyst 2001. He currently heads the Technology Assessment (TA) group, which conducts comprehensive energy system assessments to support sustainable energy transition decision-making. He is also a lecturer at the Swiss Federal Institute of Technology Zurich (ETHZ). Peter's research interests include risk assessment in the energy sector, decision support systems, and stakeholder interaction. He is responsible for PSI's Energy-Related Severe Accident Database (ENSAD), the world's largest database on severe accidents in the energy sector and has developed several MCDA tools. He regularly presents his work at international conferences, publishes in peer-reviewed scientific journals, contributes to books, and trains students at different levels. He holds an MSc and PhD from ETHZ.

Dr Sarah Lohmann
Topic: *Cyber and AI Vulnerabilities and Mitigations for Renewable Energy Systems*

Dr Sarah Lohmann is a Visiting Researcher at the Army Cyber Institute at West Point (USMA) and Full-Time Teaching Faculty at the University of Washington Information School specializing in cybersecurity and

emerging technologies. Her current research focus is on the protection of Smart and energy critical infrastructure from cyber threats. As an employee of the UW since 2019, Sarah has also taught in the UW's Jackson School and Communications Departments. A former U.S. State Department civil servant, Sarah recently spent two years doing field research in Europe as a cyber-SME and Visiting Research Professor for the US Army War College. She is currently co-leading the cyber research for a NATO Science and Technology project in collaboration with West Point's Army Cyber Institute. She is an editor and contributing author of three recent books: What Ukraine Taught NATO about Hybrid Warfare, Countering Terrorism on Tomorrow's Battlefield, and Emerging Technologies and Terrorism. Previously, she started and led the cyber program at Johns Hopkins University's American German Institute, where she is a Non-Resident Fellow. She is on the Advisory Board of the Maritime Cybersecurity Centre of Excellence and on the Editorial Board of the defence journal Parameters. She has a BA from Wheaton College, Illinois, and MA from American University in Washington, D.C. and a PhD from Universitaet der Bundeswehr in Germany.

2.6 Communication channels

Primary Communication. The exercise primarily utilizes a digital platform (Cisco Webex) for communication. This platform serves as the main conduit for delivering injects, receiving responses, and facilitating any necessary real-time interactions between exercise control and participants. Microsoft Teams is used as a backup.

Secondary Communication. Phone and email serve as backup communication channels. These are used in case of technical issues with the primary platform or for communications that require a more direct or immediate response.

Contact Lists. Prior to the exercise, all participants will receive comprehensive contact lists. These lists will include contact information for key personnel such as Site Directors, ODE team members, and technical support staff.

3. Exercise structure

3.1 Format

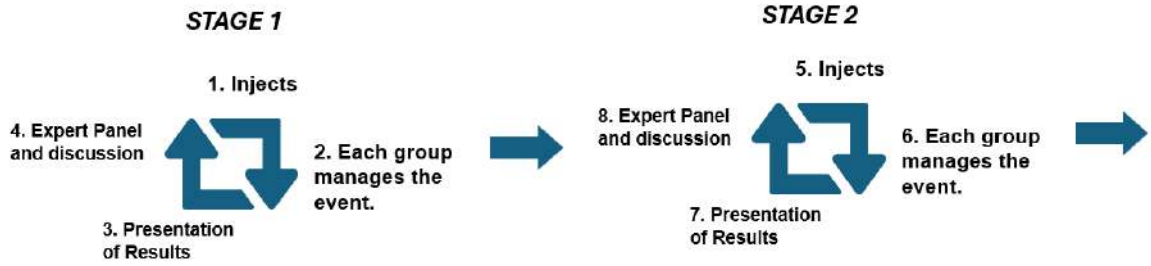
The NORDIC PINE 2024 exercise is designed to be conducted in a distributed format, allowing for flexibility in participation and execution. The scenario is structured to accommodate the participants in mixed groups of 4-8 persons working together as teams, either at physical distributed locations (sites), fully remotely or hybrid. This format enables a wide range of participants to engage in the exercise simultaneously, regardless of their geographical location.

Each team operates independently, progressing through the exercise phases and responding to injects. Responses to each inject are submitted via a digital form, ensuring a standardized and efficient process for data collection and evaluation. This approach allows for real-time assessment of team performances and enables the exercise control to adapt the scenario as needed.

Each stage concludes with a summarizing and reflective discussion. During this session, the TA/STA can direct questions and comments to the other groups likewise the experts within the Officer Directing the Exercise (ODE).

The ODE operate either distributed or from a central facility, coordinating the exercise across all sites and remote groups simultaneously. This distributed control ensures consistency in the exercise experience for the target audience while allowing for the necessary flexibility to address site-specific needs or challenges.

Implementation of stages – principal flow chart



3.2 Roles and responsibilities

The Training Audience (TA) and Secondary Training Audience (STA) will be divided into mixed groups of 4-8 people:

- Groups and group affiliation will be presented later.
- Possibly the groups will be re-mixed during the exercise. To contribute to the spread of exchange and knowledge.

Each group will include one individual from the exercise organisation, given the following responsibilities:

- Notes – Responsible for summarizing the group's actions and responses in the intended template; “Inject Response form”.
- Evaluation - Responsible summarizing the groups reflections and lessons identified in the intended template; “Hotwash documentation form”.

2.7 Played (fictional) organization

You are part of the Strategic Planning and Response Team (SPRT) of the Nordica Renewable Energy Consortium (NREC). As a joint venture between major energy companies from Sweden, Finland, Denmark, and the Baltic states, NREC stands at the forefront of renewable energy development in the Nordic-Baltic region.

NREC's organizational structure includes:

1. *Executive Board*. Focus is on strategic vision, mission and governance
2. *Operations Department*. Responsible for overseeing the vast network of wind farms and energy storage facilities.
3. *Cybersecurity and IT Department*. Safeguards NREC's digital infrastructure.
4. Communications and Public Affairs Department: Focus on marketing communications, with a minor public affairs team.
5. *Legal and Compliance Department*. Ensures NREC's activities align with the complex web of international and national regulations.
6. *Research and Development Department*. Drives innovation in renewable energy technologies.
7. *Supply Chain Management Department*. Navigates the intricacies of global logistics and supplier relationships.

The Strategic Planning and Response Team, which you are part of, includes senior representatives from each of these departments. Your team has been formed not in response to a specific crisis, but as a proactive measure to enhance NREC's resilience and readiness. Your mandate is to anticipate potential threats, develop comprehensive response strategies, and ensure NREC can navigate the complex challenges of the modern energy landscape.

NREC has invested in preparedness, implementing cybersecurity measures, regular training programs for employees on recognizing hybrid threats, and developing agile communication strategies. The organization prides itself on its transparent operations and commitment to environmental and social responsibility.

As the exercise begins, you find yourselves in a world of simmering tensions and potential threats. While no major crisis has yet unfolded, there's a growing sense that NREC stands on the brink of significant challenges. Your team's mission is to stay ahead of emerging threats, capitalize on opportunities, and steer NREC through the turbulent waters of global energy politics.

Your decisions in the coming hours and days will not only shape the future of NREC but could also have far-reaching implications for the energy security and political stability of the entire Nordic-Baltic region. As you prepare to face the unknown, remember that your diverse skills, combined with NREC's robust infrastructure and preparedness, position you well to tackle whatever challenges may arise.

5.2 The exercise organization

The following roles and responsibilities are included I the Exercise Control (EXCON) organisation:

Site Directors. These individuals are responsible for facilitating the exercise at their respective sites. They serve as the primary point of contact between their site and the Officer Directing the Exercise (ODE). Site Directors ensure that their teams have all necessary resources and information to participate effectively in the exercise.

Officer Directing the Exercise (**ODE**). The ODE has overall responsibility for the execution of the exercise. They coordinate with Site Directors and oversee the entire operation from the central facility.

The Opposing Forces (OPFOR). As part of the ODE team, OPFOR has together with the CRC operational responsibility for the scenario execution.

Chief Response Cell (**CRC**). As part of the ODE team, the CRC has together with OPFOR operational responsibility for the scenario execution. They work closely with the Response Cell leaders to ensure the smooth flow of injects and manage the overall progress of the exercise.

Response Cell (**RC**) Leaders. Specialized RC leaders for Supply Chain, Cyber, and FIMI provide expert support to the CRC during the exercise. They help craft realistic injects and evaluate team responses in their respective areas of expertise.

4. The Scenario

4.1 Scenario design and structure

The NORDIC PINE 2024 scenario is designed to integrate hybrid, cyber, and foreign information manipulation and interference (FIMI) threats into a cohesive narrative. The scenario spans a 12-month period, allowing for a comprehensive examination of how these threats evolve and impact renewable energy systems and national security over time.

The scenario is structured in five distinct phases:

1. Early warning signs
2. Threat escalation
3. Crisis point
4. Response and mitigation
5. Recovery and lesson integration

This structure facilitates the exploration of various aspects of security management, including threat detection, escalation handling, crisis response, and long-term resilience building. Each phase presents unique challenges, requiring participants to adapt their strategies and decision-making processes as the situation evolves.

4.2 Geopolitical context

NORDIC PINE 2024 is set against a geopolitical backdrop that reflects current global tensions and emerging challenges in the energy sector.

NATO-Russia Tensions. The scenario incorporates ongoing tensions between NATO and Russia, particularly in the Baltic region. These tensions manifest in various forms, including military posturing, economic pressures, and information warfare tactics.

China's Global Influence. The exercise explores the implications of China's growing role in global supply chains and technology markets, particularly in the renewable energy sector. This influence is presented as both a potential vulnerability and a geopolitical factor in the unfolding crisis.

EU Energy Independence. Within the European Union, there is an increased focus on achieving energy independence and enhancing energy security. This drive creates both opportunities and challenges as nations navigate the transition to renewable sources while maintaining robust energy systems.

Climate Change Imperatives. Global pressure to transition to renewable energy sources in response to climate change adds complexity to the scenario. Participants must balance immediate security concerns with long-term environmental and economic considerations, for example, retirements of hydrocarbon-based power generation.

Critical Infrastructure Vulnerabilities. The scenario incorporates rising concerns about the vulnerability of critical infrastructure to hybrid threats. It explores how these vulnerabilities can be exploited and how they shape national and international security strategies.

The aim of this geopolitical context is to provide a realistic framework within which participants must make decisions and develop strategies throughout the exercise.

4.3 Key actors (protagonists and antagonists)

NORDIC PINE 2024 features a range of actors, each with distinct roles, capabilities, and objectives.

Protagonists

- **Nordic-Baltic countries**. Sweden, Finland, Denmark, and the Baltic states are at the forefront of the crisis, working to protect their energy infrastructure and national interests.
- **NATO and EU Institutions**. These organizations play key roles in coordinating responses, sharing intelligence, and providing support to affected nations.
- **National energy companies and regulators**. These entities are responsible for maintaining energy supply and implementing security measures.
- **Cybersecurity agencies and CERT teams**. Specialized units focused on detecting, preventing, and responding to cyber threats.

Antagonists

- **Berylia**. Antagonistic actor currently waging wars in and outside of Europe. Portrayed as an actor employing a range of hybrid warfare tactics to undermine Western energy security.
- **Crimsonia**. Leveraging its position as a global supplier of technology and in supply chains for renewable energy components to further its global economic and geopolitical objectives.
- **Non-State Actors**. Various hacktivist groups and proxy organizations, some with clear allegiances, others with more ambiguous motivations.
- **Transnational Criminal Networks**. Opportunistic criminal elements exploiting vulnerabilities in energy systems.

The interactions between these actors create the dynamic environment within which the scenario unfolds.

4.4 Scenario briefing

The world stands at a crossroads, with geopolitical tensions simmering beneath the surface of apparent stability. The Nordic-Baltic region, long a bastion of cooperation and progressive energy policies, finds itself navigating an increasingly complex global landscape. While no major conflicts have erupted, there's a palpable sense of unease as nations grapple with energy security, climate change, and the ever-present spectre of hybrid threats.

In this charged atmosphere, the Nordica Renewable Energy Consortium (NREC) emerges as a beacon of hope and innovation. Formed through a visionary collaboration between Sweden, Finland, Denmark, and the Baltic states, NREC represents an ambitious attempt to revolutionize the region's energy infrastructure. Its crown jewel: a vast network of advanced offshore wind farms coupled with cutting-edge energy storage, promising to significantly boost renewable energy capacity and reduce fossil fuel dependence.

However, NREC's journey has not been without challenges. Global supply chains, already strained by recent economic fluctuations, have shown signs of vulnerability. While no major disruptions have occurred, industry analysts have noted subtle irregularities in the delivery of key components, raising concerns about potential future bottlenecks.

In the digital realm, cybersecurity experts across the region have reported an uptick in probing attacks against energy infrastructure. Though these attempts have been successfully repelled thus far, they serve as a stark reminder of the ever-present digital threats facing critical systems.

Meanwhile, the information landscape has grown increasingly murky. Social media platforms have seen a gradual rise in sceptical narratives surrounding renewable energy projects, questioning their economic viability and environmental impact. While not yet reaching crisis levels, this trend has caught the attention of communications experts who warn of the potential for more coordinated disinformation campaigns.

On the geopolitical front, a neighbouring state has announced plans for upcoming military exercises near the borders of several NREC member countries. While officially described as routine, these manoeuvres have raised eyebrows among security analysts, who note their proximity to key energy infrastructure.

Energy markets, always sensitive to global events, have shown increased volatility in recent months. While no single factor can be pinpointed as the cause, some economic experts have expressed concern about the potential for market manipulation to undermine renewable energy initiatives.

5. Integrated threat landscape – a common baseline

5.1 Threat landscape of renewable energy systems

The transition to renewable energy systems presents both opportunities and vulnerabilities in the broader context of national and international security. As nations increasingly rely on renewable sources to meet their energy needs and climate goals, these systems become critical infrastructure and, consequently, attractive targets for malicious actors.

Renewable energy systems face a diverse array of threats due to their large-scale, rural, centralized facilities and reliance on advanced technologies, and integration with existing power grids. Wind farms, solar power systems, hydroelectric facilities, battery storage, and their associated control systems are all potential targets. The interconnectedness of these systems with traditional energy infrastructure creates a complex web of vulnerabilities that span physical, cyber, and human domains.

A significant vulnerability lies in the supply chains that support renewable energy infrastructure. The global nature of these supply chains, often involving core components manufactured in various countries, introduces risks of sabotage, quality control issues, and potential vulnerabilities in critical hardware and software. For instance, the production of electricity inverters, power substations, or other "intelligent" components connected to the Internet in countries with geopolitical tensions could be leveraged as a point of compromise.

Furthermore, the increasing digitalization and automation of renewable energy systems, while improving efficiency and responsiveness, also expand the attack surface for cyber threats. Smart grids, connected devices, and advanced monitoring systems and the introduction of AI approaches all introduce new vectors for potential exploitation.

As seen during the Covid-19 pandemic, disruptions in supply chains can cause serious problems when organizations are unable to obtain various resources or required components when needed. It is important for stakeholders to realize that in such situations, it may be possible to seek assistance from partner organizations. For example, borrowing extra components from friendly warehouses could be a viable solution when items are unavailable on the market or when delivery times are prohibitively long.

5.2 Hybrid threats

Hybrid threats in the context of renewable energy systems represent a multifaceted challenge that blends conventional and unconventional methods to achieve strategic objectives. These threats are characterized by their ambiguity, adaptability, and the difficulty in attributing them to specific actors.

In the renewable energy sector, hybrid threats may manifest in various forms. For example, a hostile state actor might combine economic pressure, such as manipulating energy markets, with targeted disinformation campaigns aimed at undermining public confidence in renewable energy initiatives. This could be further compounded by covert cyber operations targeting electric grid operations or regulatory bodies.

Another aspect of hybrid threats involves the exploitation of legal and regulatory frameworks. Malicious actors may use legitimate business practices, such as strategic investments or acquisitions in the renewable energy sector, to gain influence or access to sensitive information. This "lawfare" approach can be particularly challenging to counter, as it operates within the bounds of existing legal structures.

The use of proxy actors is another key component of hybrid threats. Non-state groups, including hacktivists, environmental extremists, or even seemingly legitimate NGOs, may be leveraged to carry out actions that serve the strategic interests of state actors while maintaining plausible deniability. These

proxy actors can engage in activities ranging from physical sabotage of renewable energy infrastructure to sophisticated online influence operations.

5.3 Cyber threats

Cyber threats to renewable energy systems represent a rapidly evolving and increasingly critical aspect of the threat landscape. As these systems become more interconnected and reliant on digital technologies, the potential impact of cyber-attacks grow exponentially.

One primary area of concern is the vulnerability of Supervisory Control and Data Acquisition (SCADA) systems used to monitor and control renewable energy facilities. These systems, if compromised, could allow attackers to disrupt power generation, alter critical settings, or even cause physical damage to equipment. The 2015 cyber-attack on Ukraine's power grid serves as a stark reminder of the potential consequences of such vulnerabilities.

Advanced Persistent Threats (APTs) pose a significant challenge in this domain. These sophisticated, long-term intrusion campaigns, often organized in groups, frequently target intellectual property, sensitive operational data, or seek to establish persistent access for future exploitation. In the renewable energy sector, APTs could gather intelligence on emerging technologies, compromise supply chains, or prepare for future disruptive actions.

Ransomware attacks represent another serious threat. The potential for attackers to encrypt critical systems or threaten the release of sensitive data could have severe implications for energy providers, potentially leading to service disruptions or financial losses. The Colonial Pipeline incident in 2021, while not specifically targeting renewable energy, demonstrated the far-reaching consequences of such attacks on energy infrastructure.

Moreover, the threat landscape has evolved to include destructive wipers, often disguised as ransomware. These malicious programs, as seen recently in Ukraine and in incidents like NotPetya that affected companies globally, are designed to destroy data and render systems inoperable. Unlike traditional ransomware, even if a ransom is paid, the affected data and systems cannot be recovered. This adds a new layer of risk, as companies targeted by such attacks face not only data loss but also the potential for long-term operational disruption.

The increasing use of connected devices such as electric meters or thermostats in smart grid systems also introduces new vulnerabilities. These devices, often with limited security features, can serve as entry points for attackers seeking to infiltrate broader energy management systems.

5.4 Foreign information manipulation and Interference (FIMI)

Foreign Information Manipulation and Interference (FIMI) represents a significant threat to the renewable energy sector, operating in the cognitive and information domains to shape perceptions, influence decision-making, and undermine public trust.

In the context of renewable energy, FIMI campaigns might seek to discredit the efficacy or safety of renewable technologies. This could involve the spread of misleading or false information about the environmental impact of wind farms, the reliability of solar power during peak demand periods, or exaggerated claims about the economic costs of transitioning to renewable energy sources.

Social media platforms play a crucial role in the dissemination of such disinformation. Coordinated inauthentic behaviour, including the use of bot networks and troll farms, can amplify misleading narratives and create the illusion of grassroots opposition to renewable energy projects. These campaigns may exploit existing societal divisions, such as rural-urban disparities or concerns about job losses in traditional energy sectors.

Another aspect of FIMI involves the manipulation of scientific discourse. This could include the promotion of pseudoscientific studies that cast doubt on climate change or the effectiveness of renewable technologies. By creating an atmosphere of uncertainty, these efforts can delay policy actions and investment in renewable energy infrastructure.

Economic FIMI is also a concern, where false or misleading information about renewable energy markets, technological breakthroughs, or policy changes can be used to manipulate stock prices or investment patterns. This not only has immediate economic impacts but can also erode long-term confidence in the renewable energy sector.

5.5 Interconnections between threat vectors

The true complexity of the threat landscape emerges when considering the interconnections between hybrid, cyber, and FIMI vectors. These threats do not exist in isolation but rather form a synergistic ecosystem where different tactics reinforce and amplify each other.

For instance, a cyber-attack on a renewable energy facility could be timed to coincide with a disinformation campaign questioning the reliability of renewable sources. The resulting public outcry and potential energy shortages could then be exploited through hybrid tactics, such as offering assistance from a hostile state actor, thereby increasing geopolitical leverage.

Similarly, FIMI campaigns can be used to prepare the information environment for future cyber or physical attacks. By sowing doubt about the security of renewable energy systems or exaggerating their vulnerabilities, malicious actors can create a climate of public opinion that is more accepting of or even demanding changes that might introduce new vulnerabilities.

The supply chain represents another nexus of interconnected threats. A compromise in the supply chain through hybrid tactics (e.g., covert acquisition of a key component manufacturer) could introduce hardware vulnerabilities that enable future cyber-attacks. These attacks could then be obfuscated, or their impact amplified through coordinated disinformation efforts.

Understanding these interconnections is crucial for developing comprehensive defence strategies. It requires a holistic approach to threat assessment and mitigation, breaking down silos between cybersecurity, counterintelligence, and strategic communications efforts. Only by recognizing and addressing the interplay between these various threat vectors can effective resilience be built into renewable energy systems and the broader energy security landscape.

6. Learning outcomes

6.1 Strategic alignment and capability assessment

The learning outcomes for NORDIC PINE 2024 are designed to align with the strategic objectives of the exercise in countering hybrid threats. These outcomes focus on assessing organizational capabilities, including roles, plans, and procedures for addressing crises involving cyber, FIMI, and hybrid threats. Participants will evaluate the effectiveness of existing policies and identify potential gaps in current response strategies in their own respective contexts. This assessment process serves to validate successful approaches and highlight areas requiring improvement or innovation.

6.2 Scenario-based learning and decision-making

The exercise employs scenario-based learning to create an environment where participants explore policy problems from multiple perspectives. Learning outcomes are structured to encourage problem-solving in complex hybrid threat situations. A key feature of an inject based scenario exercise is the enhancement of decision-making skills under conditions of pressure, uncertainty, and urgency. Participants will make decisions based on limited information, simulating real-world constraints encountered in crisis situations.

6.3 Collaboration, communication, and multidisciplinary integration

Learning outcomes emphasize improving collaboration and communication between stakeholders. Participants will gain clarity on roles and responsibilities in hybrid threat scenarios, learning to coordinate across departmental and organizational boundaries. The exercise aims to foster insights that reflect the multidisciplinary nature of contemporary security challenges. This approach ensures participants develop a broad understanding of hybrid threats, considering technical, human, and organizational factors.

6.4 Practical application and continuous improvement

The learning outcomes focus on practical application of knowledge. Participants will test their understanding of existing policies and procedures in simulated crisis scenarios. This approach allows for application of theoretical knowledge to simulated real-world situations. The exercise incorporates feedback mechanisms to capture lessons learned and apply them to improve future preparedness and response capabilities. Participants will be encouraged to reflect on their performance, identifying areas for personal and organizational development.

6.5 Adaptability to emerging threats

Recognizing the evolving nature of hybrid threats in the context of renewable energy systems, the learning outcomes are designed to be adaptable. While based on current practices, they encourage participants to anticipate and prepare for emerging threat scenarios. This approach aims to ensure the exercise's relevance in the face of new challenges. Participants will consider how current strategies might need to adapt to future threats, fostering a mindset of continuous learning and adaptation. The exercise aims to enhance long-term resilience in the face of an evolving threat landscape in the renewable energy sector.

7. Evaluation and feedback

7.1 Assessment methodology

The evaluation methodology for NORDIC PINE 2024 is designed with an aim to provide an objective assessment of participant performance. It employs a structured evaluation framework based on established NATO evaluation systems, adapted for the specific context of cyber, FIMI, and hybrid threats in the renewable energy sector.

The assessment is objective-based, mapping specific training objectives to observable activities. This allows for a focused evaluation of performance against predefined criteria. Real-time monitoring tools are utilized to observe and assess the training audience's performance during the exercise, enabling immediate feedback and adaptive scenario management.

The evaluation process is multi-dimensional, covering various aspects including tactical decision-making, communication, coordination, and adherence to relevant procedures and standards. This comprehensive approach ensures a holistic assessment of participant capabilities.

7.2 Debriefing process

The debriefing process is structured to facilitate immediate reflection and learning. It occurs in two stages:

1. **Hotwash**. Immediately following the exercise, participants engage in a facilitated discussion to share initial impressions, key observations, and immediate lessons learned. This session allows for the capture of time-sensitive insights and promotes initial reflection on the exercise experience.

2. **Formal Debrief**. A more comprehensive debrief is conducted within 48 hours of the exercise conclusion. This session involves a structured review of the exercise, including presentation of preliminary evaluation findings, discussion of key decision points, and identification of areas for improvement. Participants are encouraged to provide feedback on the exercise design and execution.

Both debriefing stages are designed to be collaborative, encouraging open dialogue and critical reflection. They serve not only as evaluation tools but also as learning opportunities, reinforcing key lessons from the exercise.

7.3 After-Action Report structure

The After-Action Report (AAR) serves as the definitive document capturing the outcomes, lessons learned, and recommendations from the exercise. Its structure is as follows:

1. Executive Summary. Provides a high-level overview of the exercise, key findings, and principal recommendations.

2. Exercise Overview. Describes the exercise objectives, scenario, and participants.

3. Analysis of Objectives. Evaluates performance against each of the predefined exercise objectives, supported by evidence-based observations.

4. Key Observations and Findings. Details significant observations across various dimensions (e.g., decision-making, communication, technical responses), identifying both strengths and areas for improvement.

5. Risk and Shortfall Analysis. Highlights identified areas of risk and capability gaps, with an emphasis on their potential operational impacts.
6. Recommendations. Offers concrete, actionable recommendations for addressing identified shortfalls and enhancing overall preparedness.
7. Lessons Identified. Captures broader lessons that may have applicability beyond the immediate exercise context.
8. Participant Feedback. Summarizes feedback received from participants regarding the exercise design, execution, and perceived value.
9. Conclusion. Provides a synthesis of the main findings and outlines next steps for implementing recommendations.
10. Appendices. Includes detailed data, evaluation metrics, and any additional supporting information.

The AAR is designed to be a comprehensive document that not only evaluates the specific exercise but also contributes to the broader body of knowledge on preparing for and responding to cyber, FIMI, and hybrid threats in the renewable energy sector. It serves as a key input for future exercise planning, policy development, and capability enhancement efforts.

8. Appendices

The appendices will be distributed in connection with the startup of the TTX, the 24th September.

The appendices to the NORDIC PINE 2024 exercise documentation provide supporting materials essential for the understanding, execution, and evaluation of the exercise. These documents are designed to information and practical tools for both exercise controllers and participants. The appendices are structured to support the implementation of the exercise and to facilitate the post-exercise analysis.

8.1 Inject handouts

This appendix compiles all supplementary materials associated with specific injects. These handouts may include simulated news reports, technical data sheets, intelligence briefs, or other documents that provide additional context or information to participants. The handouts are designed to enhance the realism of the exercise and provide participants with tangible materials to inform their decision-making processes.

8.2 Inject response form

The inject response form is a standardized template used by participating teams to submit their reactions and decisions in response to each inject. This form ensures consistency in data collection across all exercise locations, facilitating easier analysis and comparison of responses. The structure of the form aligns with the learning objectives of the exercise, prompting participants to address key aspects of their decision-making process.

8.3 Hotwash documentation form

This appendix presents the template used to capture immediate feedback and observations during the post-exercise hotwash sessions. The form is designed to structure the collection of participants' initial impressions, key learnings, and suggestions for improvement. This documentation serves as a valuable input for the more comprehensive after-action review process and helps capture time-sensitive insights immediately following the exercise.

9. References and recommended reading

Jungwirth, R., Giannopoulos, G., Valsamos, G., Cardarilli, M., Willkomm, E., Constantinos, H., Chatzialexandris, I., Georgescu, A., Kuzel, M., Lazzari, A. and Talbot, R., Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats, EUR 31505 EN, Publications Office of the European Union, Luxembourg, 2023, ISBN 978-92-68-03246-6, doi:10.2760/58406, JRC133083.
Factsheets (europa.eu)

NATO. (2016). Cybersecurity: A generic reference curriculum.
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20161025_1610-cybersecurity-curriculum.pdf

NATO Strategic Communications Centre of Excellence. (2022). Constructing a tabletop exercise (TTX).
https://stratcomcoe.org/publications/download/Constructing-a-Table-Top-Exercise-DIGITAL-FINAL-dccfe.pdf

NATO. (2023, December). Russian War against Ukraine Lessons Learned Curriculum Guide.
https://www.nato.int/nato_static_fl2014/assets/pdf/2023/12/pdf/231208-RusWar-Ukraine-Lessons-Curriculum.pdf

NATO. (2024, July 10). Hybrid threats and hybrid warfare reference curriculum. https://www.nato.int/cps/en/natohq/topics_227643.htm

NATO STO SAS 191. (2024). NORDIC PINE 24 – Exercise Plan

Hybrid COE (2023, April): Hybrid threats: A comprehensive resilience ecosystem Hybrid threats: A comprehensive resilience ecosystem - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats

Pamment, J., Nothhaft, H., Agardh-Twetman, H., & Fjällhed, A. (2018). Countering Information Influence Activities: The State of the Art. Swedish Civil Contingencies Agency (MSB). Countering Information Influence Activities: The State of the Art — Lund University

UK Government Communication Service (2021):RESIST Counter-Disinformation Toolkit. RESIST 2 Counter Disinformation Toolkit - GCS (civilservice.gov.uk)

Sukhodolia, O., & Walzer, L. M. (2022). NATO tabletop exercises to further energy resilience and security: Ukraine as a case study. National Institute for Strategic Studies, Ukraine, and US Naval Postgraduate School. f7c6c78c-5d9d-56f2-7836-cb3fc24f6007 (nps.edu)

Tabletop Exercise (TTX)

Scenario Overview

Exercise – a fictive scenario

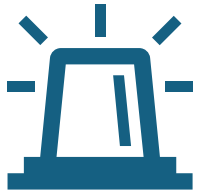
Background story

A Complex Landscape

The Nordic-Baltic region faces a complex global landscape with geopolitical tensions, energy security issues, climate change, and hybrid threats causing unease despite no major conflicts.

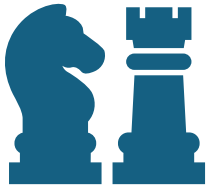
Infrastructure Revolution

The Nordica Renewable Energy Consortium (NREC), a collaboration among Sweden, Finland, Denmark, and the Baltic states, aims to revolutionize energy infrastructure with offshore wind farms and advanced energy storage to reduce fossil fuel dependence.



Vulnerabilities & Vectors

Challenges for NREC include global supply chain vulnerabilities, increased cyberattacks on energy infrastructure, and rising scepticism on social media about renewable energy projects, potentially leading to disinformation campaigns.



Geopolitical tensions

Geopolitical concerns are heightened by a neighbouring state's planned military exercises near NREC member countries, and energy markets have shown increased volatility, raising concerns about market manipulation affecting renewable energy initiatives.

Exercise – a fictive scenario

Nordica Renewable Energy Consortium (NREC).

You are part of the Strategic Planning and Response Team (SPRT) of the Nordica Renewable Energy Consortium (NREC). As a joint venture between major energy companies from Sweden, Finland, Denmark, and the Baltic states, NREC stands at the forefront of renewable energy development in the Nordic-Baltic region.

NREC's organizational structure includes:

1. *Executive Board*. Focus is on strategic vision, mission and governance
2. *Operations Department*. Responsible for overseeing the vast network of wind farms and energy storage facilities.
3. *Cybersecurity and IT Department*. Safeguards NREC's digital infrastructure.
4. Communications and Public Affairs Department: Focus on marketing communications, with a minor public affairs team.
5. *Legal and Compliance Department*. Ensures NREC's activities align with the complex web of international and national regulations.
6. *Research and Development Department*. Drives innovation in renewable energy technologies.
7. *Supply Chain Management Department*. Navigates the intricacies of global logistics and supplier relationships.

Exercise – a fictive scenario

Phase 1 - Early warning signs

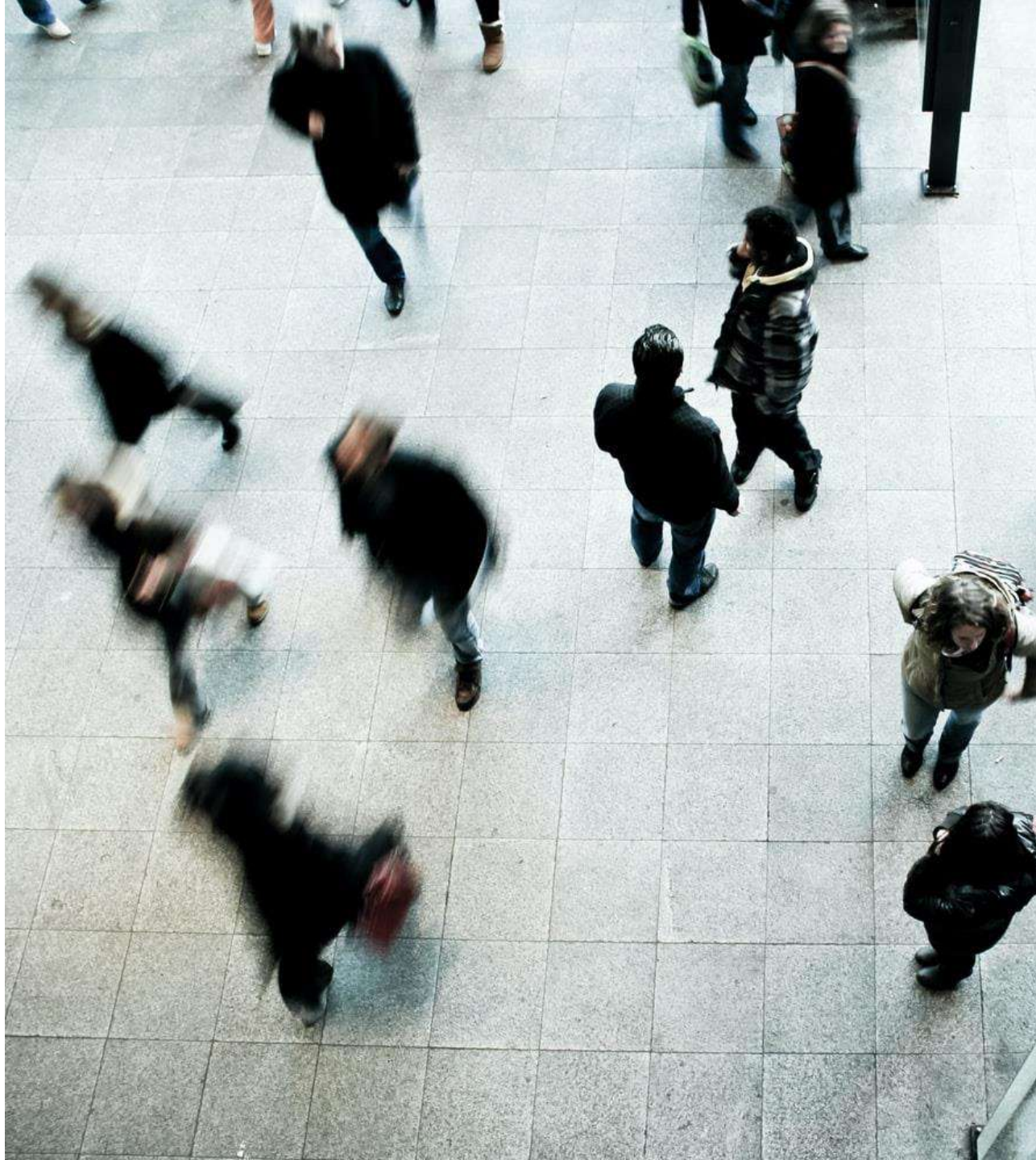
As NREC, you find yourself navigating an increasingly complex geopolitical landscape. It's been three months since the launch of your ambitious offshore wind farm projects, a set of wind farms with multiple wind turbines, tied to one high voltage transmission line, and while progress has been steady, there's a palpable sense of unease in the air.

Global supply chains are showing signs of strain, and whispers of cyber threats against energy infrastructure are growing louder.

Your social media monitoring team has noticed a subtle shift in public sentiment towards renewable energy projects, with scepticism slowly creeping into online discussions.

Meanwhile, a neighbouring state's announcement of military exercises near your operational areas has added another layer of complexity to your strategic planning.

As the Strategic Planning and Response Team, you're tasked with identifying and addressing these early warning signs before they escalate into full-blown crises. Your decisions in this phase will set the tone for NREC's resilience in the face of emerging threats.



Exercise – a fictive scenario

Phase 2 - Escalation of Threats

As NREC, you find yourself six months into your ambitious offshore wind farm projects, and the early warning signs have evolved into more concrete threats. The global situation has deteriorated, with economic pressures and political disagreements straining international relations. Your new wind farm installations are progressing, but each step forward seems to bring new challenges.

The cyber probes you detected earlier have grown more aggressive, and the whispers of discontent on social media have swelled into a chorus of criticism. Your supply chain issues have compounded, and there's a growing sense that these challenges are not merely coincidental. There are major delays in the ongoing construction, with cascading public and social media concerns.

As the Strategic Planning and Response Team, you're now faced with active threats that require immediate attention and strategic decision-making. The choices you make in this phase will determine NREC's ability to withstand the mounting pressure and protect its assets and reputation.

Exercise – a fictive scenario

Phase 3 - Crisis Point

As NREC, you now find yourself at the peak of the crisis, eight months into your offshore wind farm projects.

The situation has escalated dramatically on multiple fronts. International tensions are at a breaking point, with the neighbouring state's military exercises causing significant concern and edging closer to your operational areas. Your new offshore wind farm project is nearing completion, but the challenges you face have grown exponentially.

The cyber threats you've been battling have evolved into full-scale attacks, your supply chain is in disarray, and public opinion has turned sharply against you.

As the Strategic Planning and Response Team, you're now in crisis management mode. The decisions you make in this phase will be critical not just for NREC's survival, but potentially for the energy security and stability of the entire region. You must act swiftly and decisively, balancing short-term crisis response with long-term strategic considerations.

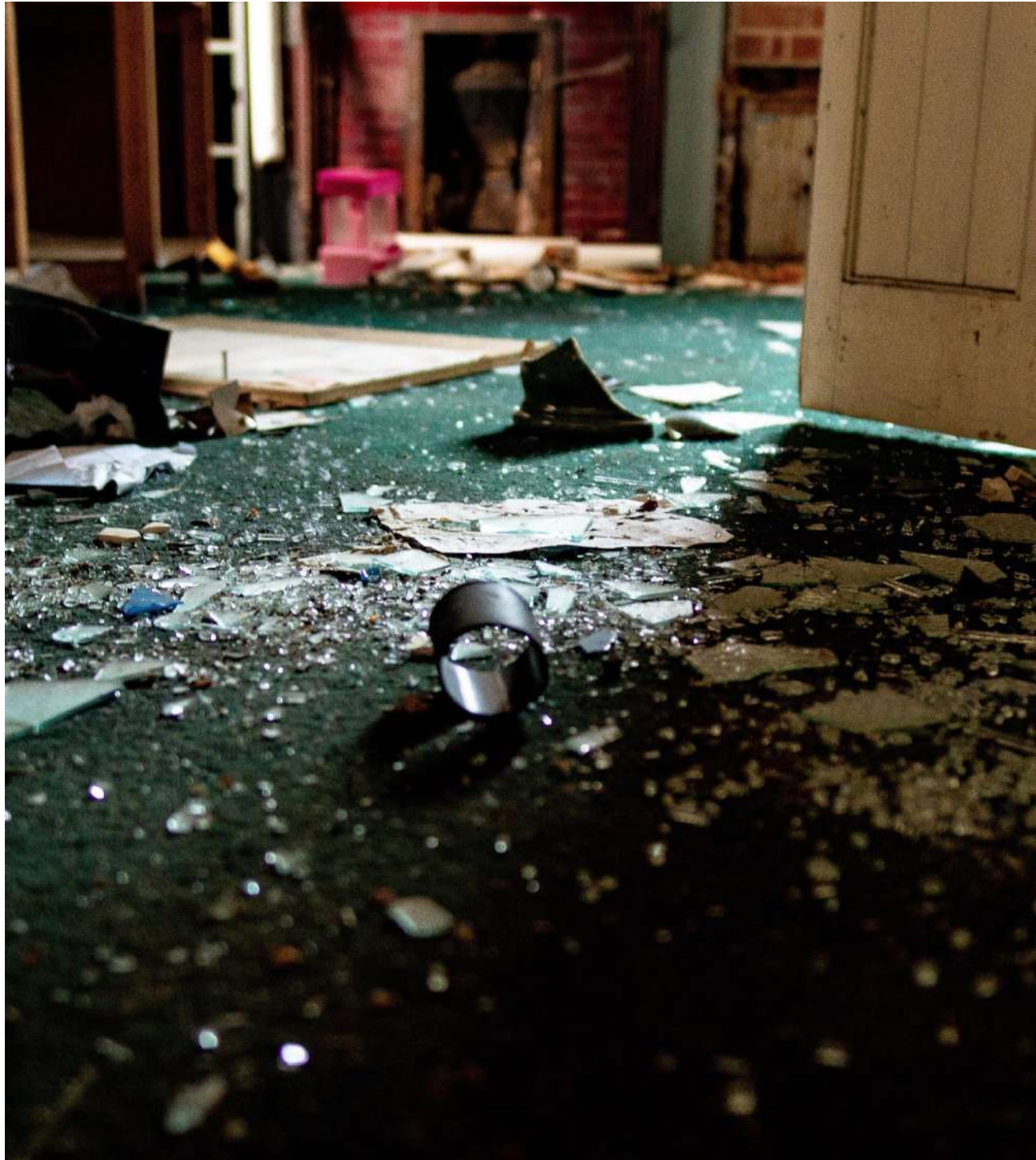
Exercise – a fictive scenario

Phase 4 - Response and Mitigation

As NREC, you've weathered the peak of the crisis and are now ten months into your turbulent journey. The immediate storm has passed, but you're far from calm waters. Your operational offshore wind farm project, while operational, is running at reduced capacity due to the recent attacks and disruptions.

The global situation remains volatile, with increased scrutiny on the energy sector and your operations. As the Strategic Planning and Response Team, your focus has shifted from crisis management to damage control, reputation rebuilding, and long-term resilience planning.

The decisions you make in this phase will be crucial for NREC's recovery and future stability. You must balance the need for transparency with security concerns, address the lingering effects of the crisis, and prepare for potential future threats, all while working to restore normal operations and rebuild trust with stakeholders.



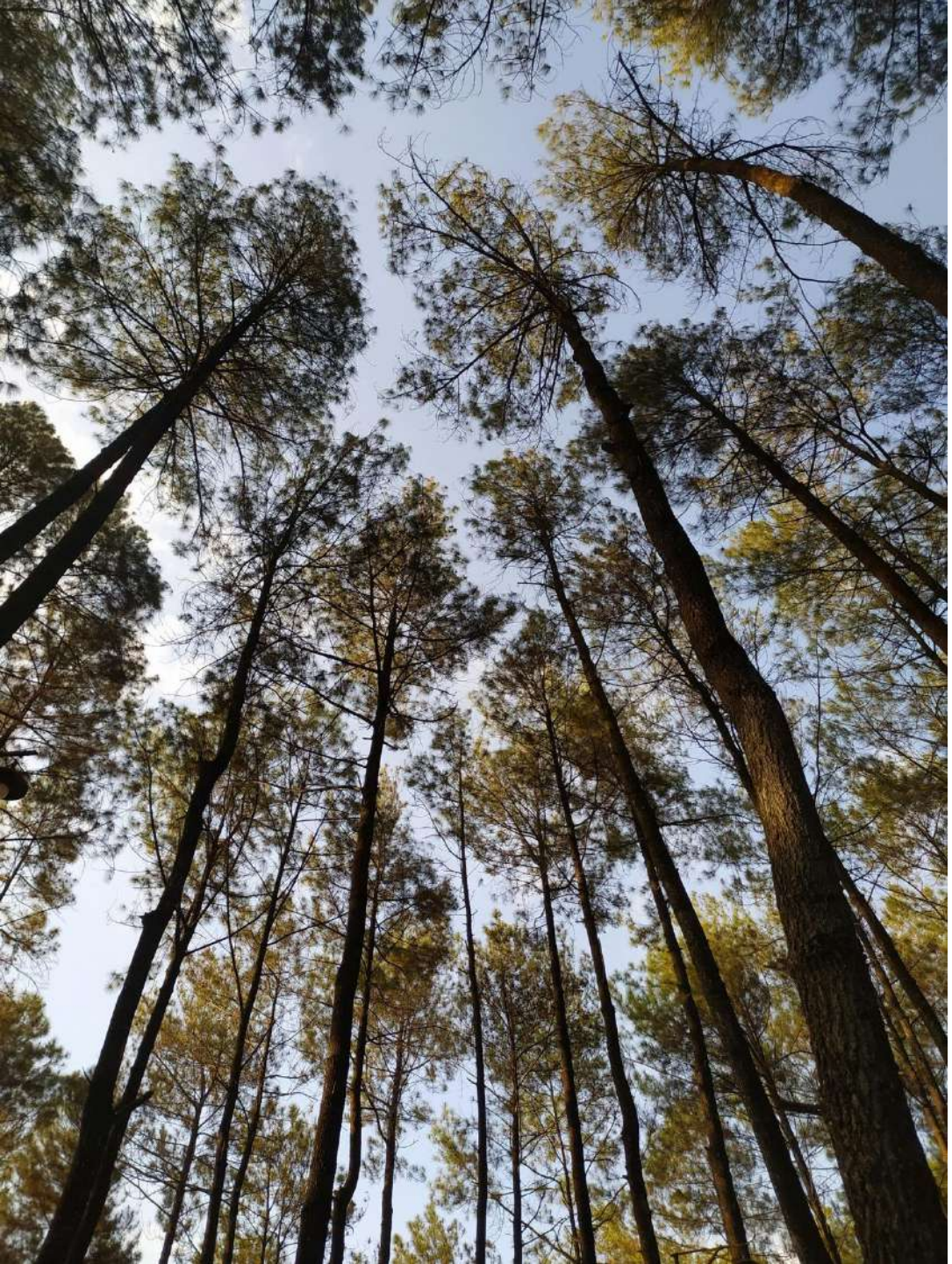
Phase 5 - Recovery and Lessons Learned

As NREC, you've reached the twelve-month mark of this tumultuous journey.

The acute crisis has passed, but its effects continue to ripple through your organization and the broader energy sector. Your offshore wind farm project is fully operational yet operating in a new reality of heightened security concerns and public scrutiny.

The global situation has stabilized somewhat, but a new normal of increased vigilance and complex geopolitical manoeuvring has set in. As the Strategic Planning and Response Team, your focus now is on long-term recovery, implementing lessons learned, and preparing for future challenges.

The decisions you make in this phase will shape NREC's resilience and adaptability in the face of evolving threats. You must balance the need for increased security with operational efficiency, rebuild trust with stakeholders, and position NREC as a leader in secure and sustainable energy production.



Thank you!

Tabletop Exercise (TTX)

Stage Information Package, #1

#1

TTX Stage Information Package: #1

Content

- Stage Instructions
- Scenario overview: Phase 1 - Early warning signs
- Inject 1.1 Cyber + Appendix "Network Traffic Log"
- Inject 1.2 Information + Appendix "Communication Team report"
- Inject 1.3 Supply Chain + Appendix "Potential links"

Stage instructions

- Take part, and read *the Stage Information package,* including.:
    - Scenario overview
    - Three (3) Injects with supportive questions + appendixes
- Discuss solutions to the Injects presented.
- Fill in the *Inject Response Form*
- Be prepared to receive and mange additional injects
- Be prepared to present your Response/Lessons Identified, **<2min.**
- **Keep the time**

Over time, write down comments, feedback associated to the exercise in *the Feedback form*

Exercise – a fictive scenario

Phase 1 - Early warning signs

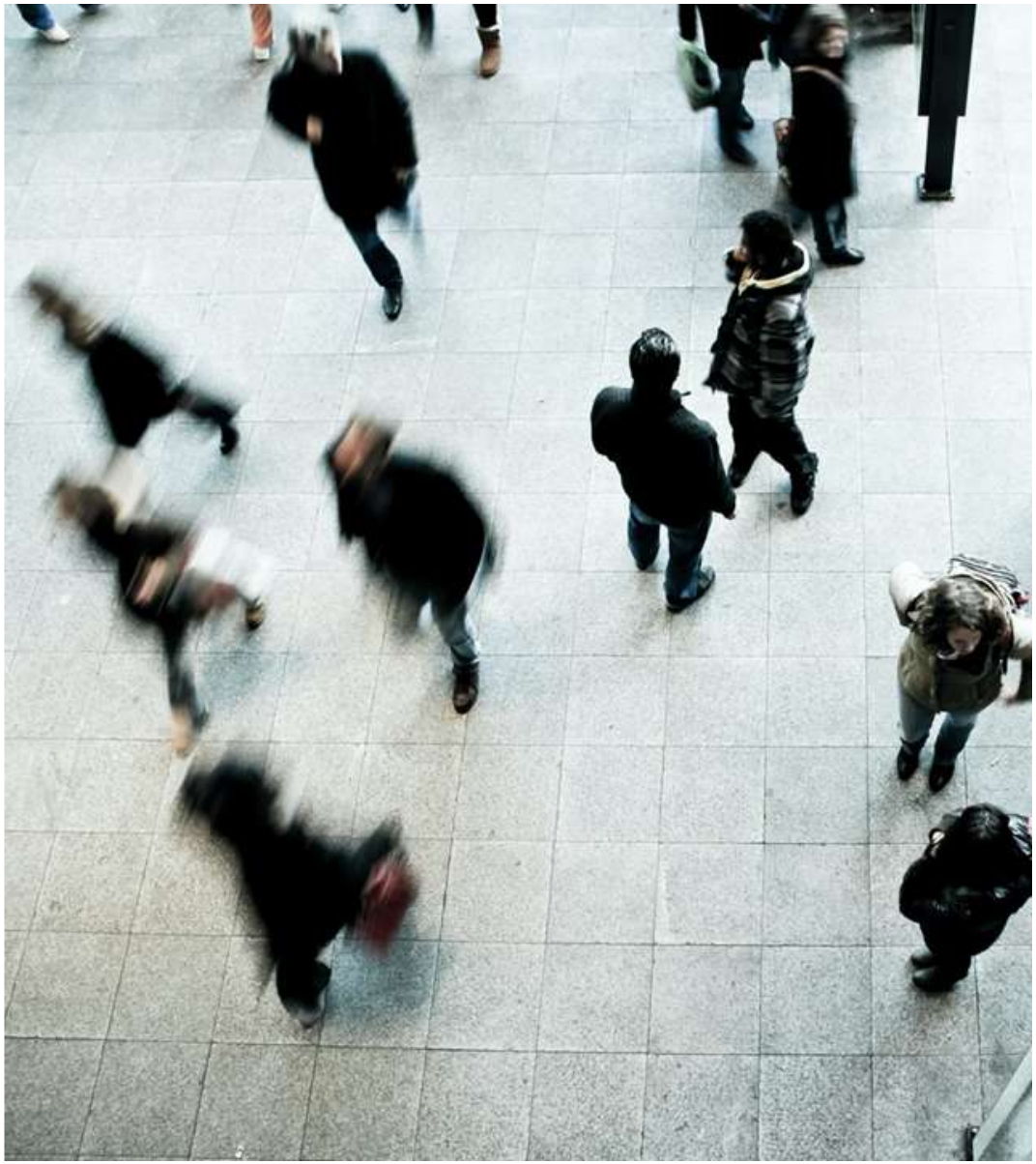
As NREC, you find yourself navigating an increasingly complex geopolitical landscape. It's been three months since the launch of your ambitious offshore wind farm projects, a set of wind farms with multiple wind turbines, tied to one high voltage transmission line, and while progress has been steady, there's a palpable sense of unease in the air.

Global supply chains are showing signs of strain, and whispers of cyber threats against energy infrastructure are growing louder.

Your social media monitoring team has noticed a subtle shift in public sentiment towards renewable energy projects, with scepticism slowly creeping into online discussions.

Meanwhile, a neighbouring state's announcement of military exercises near your operational areas has added another layer of complexity to your strategic planning.

As the Strategic Planning and Response Team, you're tasked with identifying and addressing these early warning signs before they escalate into full-blown crises. Your decisions in this phase will set the tone for NREC's resilience in the face of emerging threats.



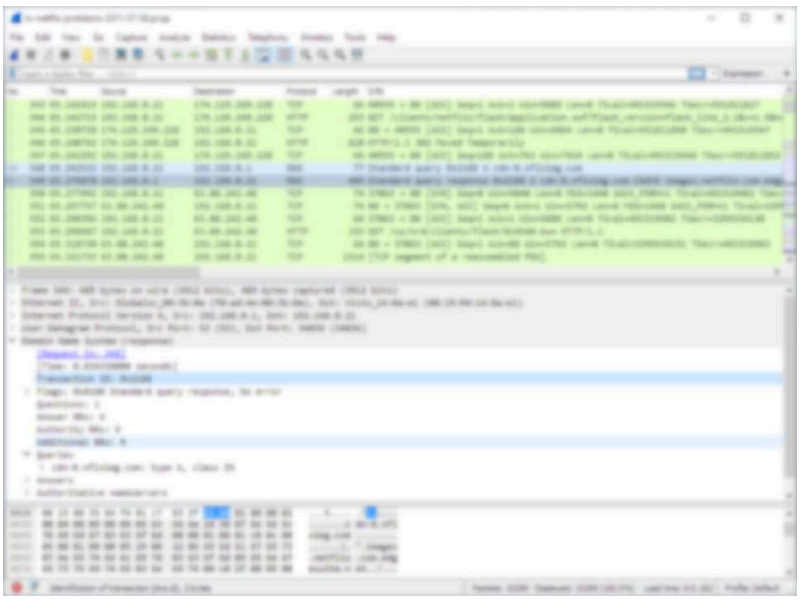
Exercise – a fictive scenario

Inject 1.1 - Cyber

Your cybersecurity team has detected an unusual pattern of probing attempts on the networks associated with your offshore wind turbines. The attacks don't match known signatures, but they're persistent and seem to be mapping out your system architecture. There's no evidence of a breach yet, but the team is concerned that this could be the precursor to a more sophisticated attack. The source of the probes is difficult to trace, appearing to bounce through multiple countries.

1. ***What immediate actions should NREC take in response to this situation? Consider resources, communication strategies, information gathering, network visibility, stakeholder involvement, and supply chain considerations in your response.***
2. ***How might this situation escalate, and what preventive measures can be implemented?***
3. ***How can NREC balance the need for heightened security with maintaining operational efficiency of the wind turbines?***

Appendix: Network Traffic Log



Excerpt:

- **Date/Time:** 10:45:32
  - **Source IP:** 203.0.113.45 … etc
  - **Destination IP:** 10.0.0.5 (Wind Turbine Control Node)
  - **Protocol:** TCP
  - **Port:** 8080
  - **Action:** Denied
  - **Notes:** Multiple attempts from various IP addresses, abnormal traffic pattern
- **Date/Time:** 10:46:15
  - **Source IP:** 198.51.100.23
  - **Destination IP:** 10.0.0.12 (SCADA System)
  - **Protocol:** UDP
  - **Port:** 502
  - **Action:** Denied
  - **Notes:** Unrecognized signature, possible reconnaissance

Exercise – a fictive scenario

- **Date/Time:** 10:47:03
  - **Source IP:** 192.0.2.50
  - **Destination IP:** 10.0.0.8 (Wind Turbine Control Node)
  - **Protocol:** TCP
  - **Port:** 443
  - **Action:** Allowed
  - **Notes:** Established connection, duration 15 seconds, then terminated
- **Date/Time:** 10:48:22
  - **Source IP:** 203.0.113.45
  - **Destination IP:** 10.0.0.5 (Wind Turbine Control Node)
  - **Protocol:** TCP
  - **Port:** 8080
  - **Action:** Denied
  - **Notes:** Repeated attempt, consistent with previous patterns
- **Date/Time:** 10:49:01
  - **Source IP:** 198.51.100.23
  - **Destination IP:** 10.0.0.15 (SCADA System)
  - **Protocol:** UDP
  - **Port:** 502
  - **Action:** Denied
  - **Notes:** Persistent probing, no data payload
- **Date/Time:** 10:50:37
  - **Source IP:** 192.0.2.100
  - **Destination IP:** 10.0.0.8 (Wind Turbine Control Node)
  - **Protocol:** TCP
  - **Port:** 443
  - **Action:** Denied
  - **Notes:** Single attempt, matches prior anomaly pattern

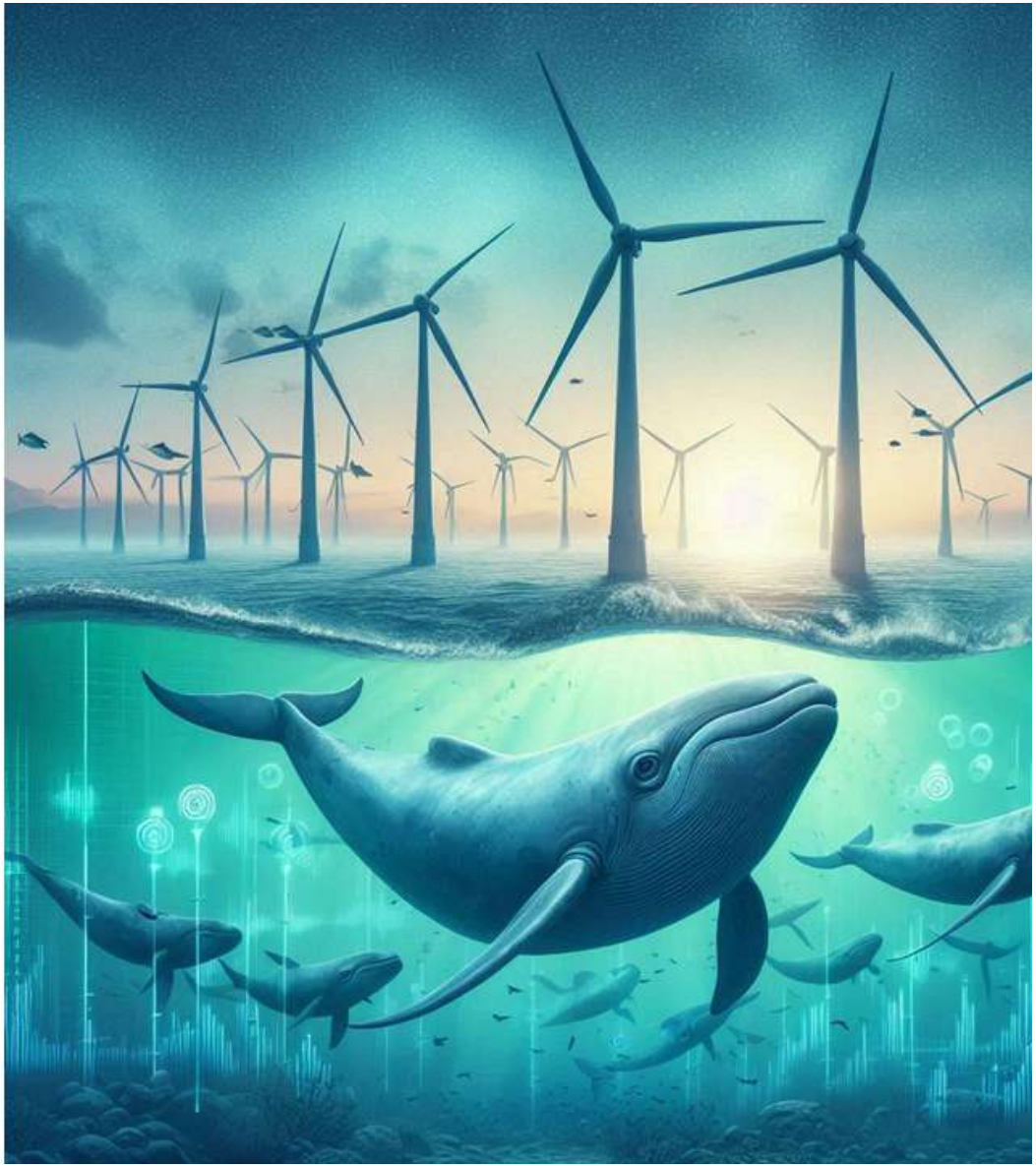
Exercise – a fictive scenario

Inject 1.2 – Information

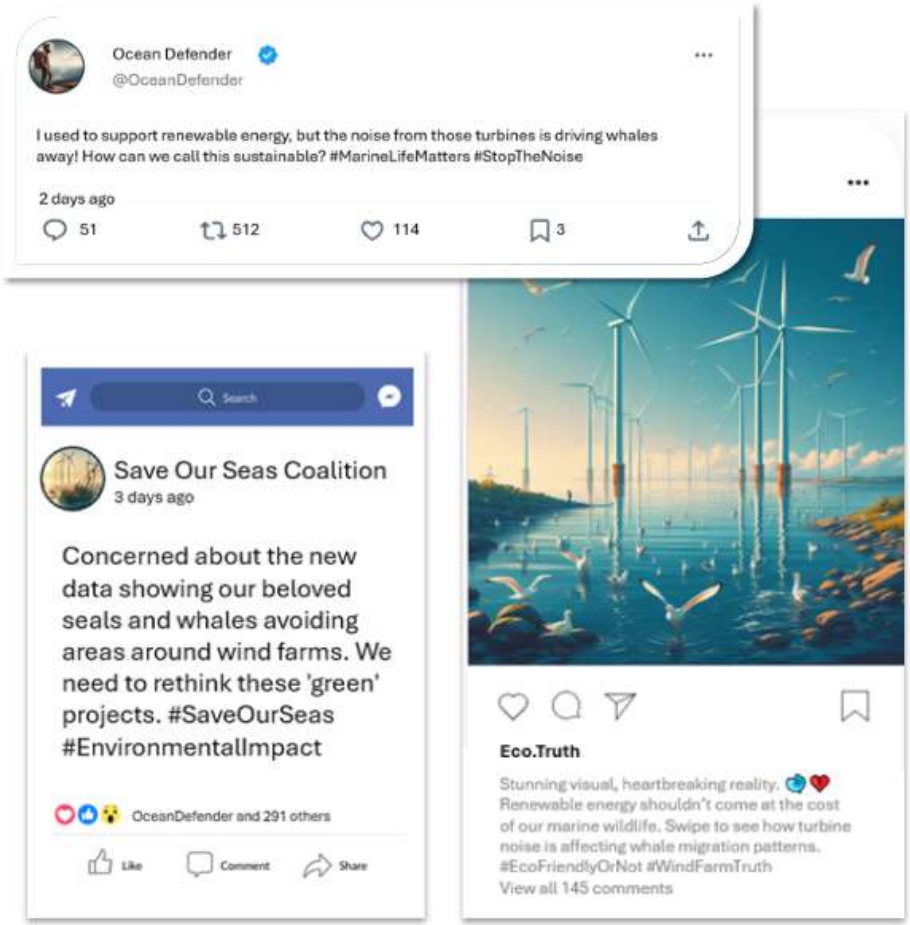
Your communications team has identified a growing trend of social media posts questioning the environmental impact of your offshore wind farms.

The posts, while not overtly hostile, are using scientific-sounding language to suggest that the low-frequency noise from your turbines is disrupting marine mammal migration patterns. This narrative is gaining traction among environmental groups and local fishing communities. Initial fact-checking suggests that the claims are based on misinterpreted or cherry-picked data.

1. ***What immediate actions should NREC take in response to this situation?***
2. ***How might this situation escalate, and what preventive measures can be implemented?***
3. ***How can NREC effectively counter this narrative without appearing dismissive of environmental concerns?***



Exercise – a fictive scenario



Social Media - Examples

1.2 Appendix: Communications Team Report

Our monitoring systems have detected an increasing volume of social media activity that questions the environmental impact of NREC's offshore wind farms. Specifically, these posts focus on the claim that low-frequency noise from the turbines is negatively impacting marine mammal migration patterns.

The narrative is being amplified by environmental groups and local fishing communities, potentially affecting public perception.

Initial fact-checking indicates that the claims are based on selectively interpreted data, but they are gaining traction online.

Exercise – a fictive scenario

Inject 1.3 – Supply Chain

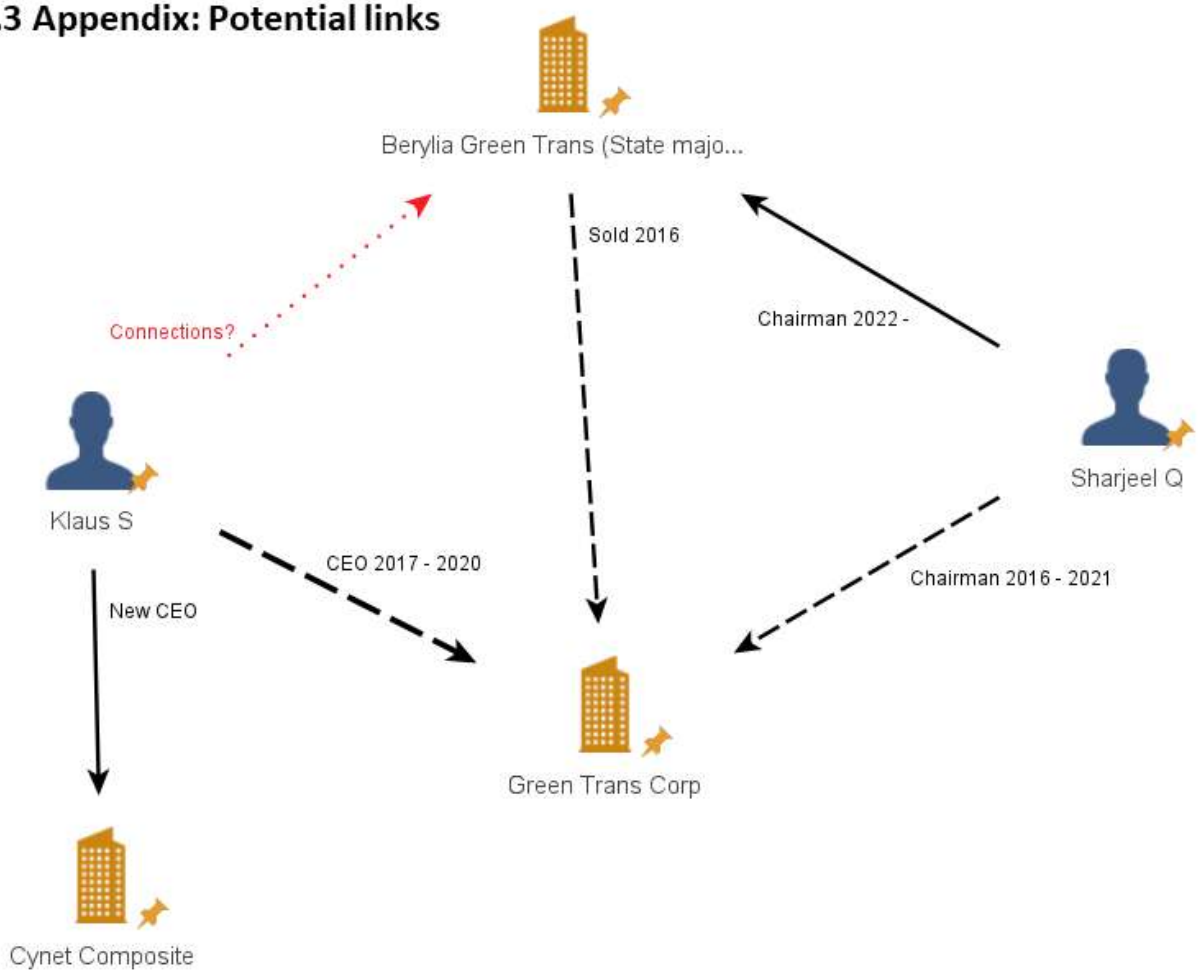
You've received word that a key supplier of specialized composite materials for your turbine blades, based in a country known for its close ties to your regional competitors, is experiencing "unexpected quality control issues."

They've assured you that the delays are temporary, but your supply chain team has noticed that the supplier recently underwent a change in senior management.

Preliminary research suggests potential links between the new management and foreign state-owned enterprises.

1. ***What immediate actions should NREC take in response to this situation?***
2. ***How might this situation escalate, and what preventive measures can be implemented?***
3. ***How can NREC secure its supply chain without causing diplomatic tensions or disrupting ongoing projects?***

1.3 Appendix: Potential links



Exercise – a fictive scenario

Inject 1.4 - Cyber

Your IT department has discovered a series of sophisticated phishing emails targeting employees in your finance and operations departments. Two persons have acted on the emails and compromised systems. The emails appear to be from trusted partners and contain malware capable of exploiting a recently discovered zero-day vulnerability in your project management software.

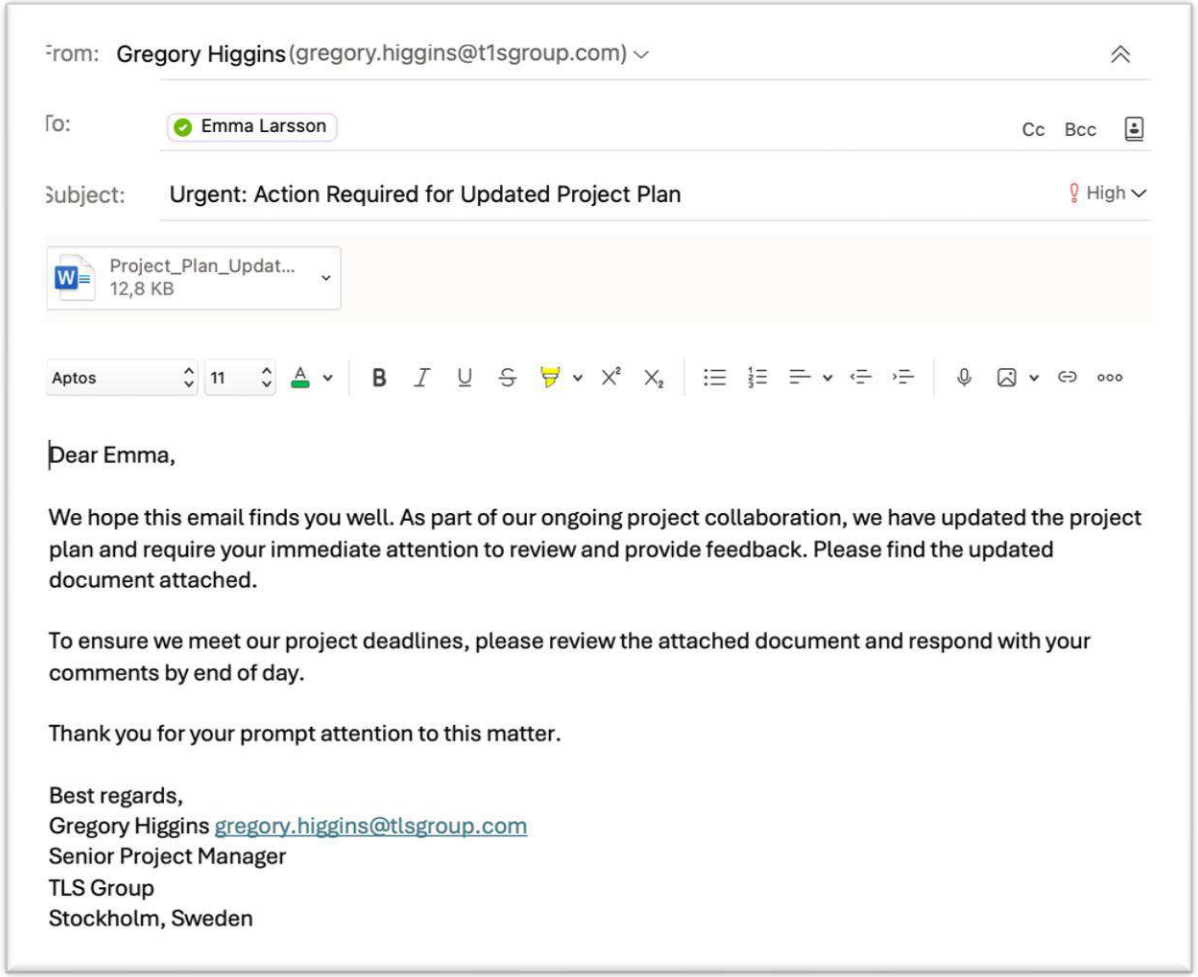
Your current security measures seem to have prevented any successful infections, but the persistence and sophistication of the attempts are concerning.

1. ***What immediate actions should NREC take in response to this situation?***
2. ***How might this situation escalate, and what preventive measures can be implemented?***
3. ***How can NREC improve its employee cybersecurity training without causing undue alarm or hampering productivity?***

Exercise – a fictive scenario

Highlighted Areas of Concern:

1. **From Address:** Although the email appears to come from a trusted partner, the actual email address is slightly altered (e.g., " gregory.higgins@t1sgroup.com " instead of " gregory.higgins@tlsgroup.com ").
2. **Urgency:** The email creates a sense of urgency, which is a common tactic in phishing attempts to prompt quick action without due diligence.
3. **Attachment:** The attached document contains malware capable of exploiting a zero-day vulnerability. Opening this file could lead to system compromise.
4. **Salutation and Signature:** While the names and contact information appear correct, always verify by cross-referencing with known contact details.



Inject 1.5 – Information

A fringe news website has published an article claiming that one of your existing, operational, offshore wind farms is causing unexplained equipment failures on commercial fishing vessels in the area. While the claims are unsubstantiated, they're beginning to circulate in local fishing communities and gaining attention from larger media outlets.

Your initial investigation shows no correlation between your operations and the reported incidents, but the narrative is rapidly spreading and evolving to include vague accusations of cover-ups.

1. ***What immediate actions should NREC take in response to this situation?***
2. ***How might this situation escalate, and what preventive measures can be implemented?***
3. ***How can NREC engage with the local fishing communities to address their concerns while maintaining its reputation for transparency and environmental responsibility?***

Tabletop Exercise (TTX)

Stage Information Package, #2

#2

TTX Stage Information Package: #2

Content

- Stage Instructions
- Scenario overview: Phase 1 - Early warning signs
- Inject 2.1 Cyber + Appendix "Cyber Incident Report"
- Inject 2.2 Information + Appendix "Communication Team report"
- Inject 2.3 Supply Chain + Appendix "Financial Intelligence Report"

Stage instructions

- Take part, and read *the Stage Information package,* including.:
    - Scenario overview
    - Three (3) Injects with supportive questions + appendixes
- Discuss solutions to the Injects presented.
- Fill in the *Inject Response Form*
- Be prepared to receive and mange additional injects
- Be prepared to present your Response/Lessons Identified, **<2min.**
- **Keep the time**

Over time, write down comments, feedback associated to the exercise in *the Feedback form*

Exercise – a fictive scenario

Phase 2 - Escalation of Threats

As NREC, you find yourself six months into your ambitious offshore wind farm projects, and the early warning signs have evolved into more concrete threats. The global situation has deteriorated, with economic pressures and political disagreements straining international relations. Your new wind farm installations are progressing, but each step forward seems to bring new challenges.

The cyber probes you detected earlier have grown more aggressive, and the whispers of discontent on social media have swelled into a chorus of criticism. Your supply chain issues have compounded, and there's a growing sense that these challenges are not merely coincidental. There are major delays in the ongoing construction, with cascading public and social media concerns.

As the Strategic Planning and Response Team, you're now faced with active threats that require immediate attention and strategic decision-making. The choices you make in this phase will determine NREC's ability to withstand the mounting pressure and protect its assets and reputation.

Exercise – a fictive scenario

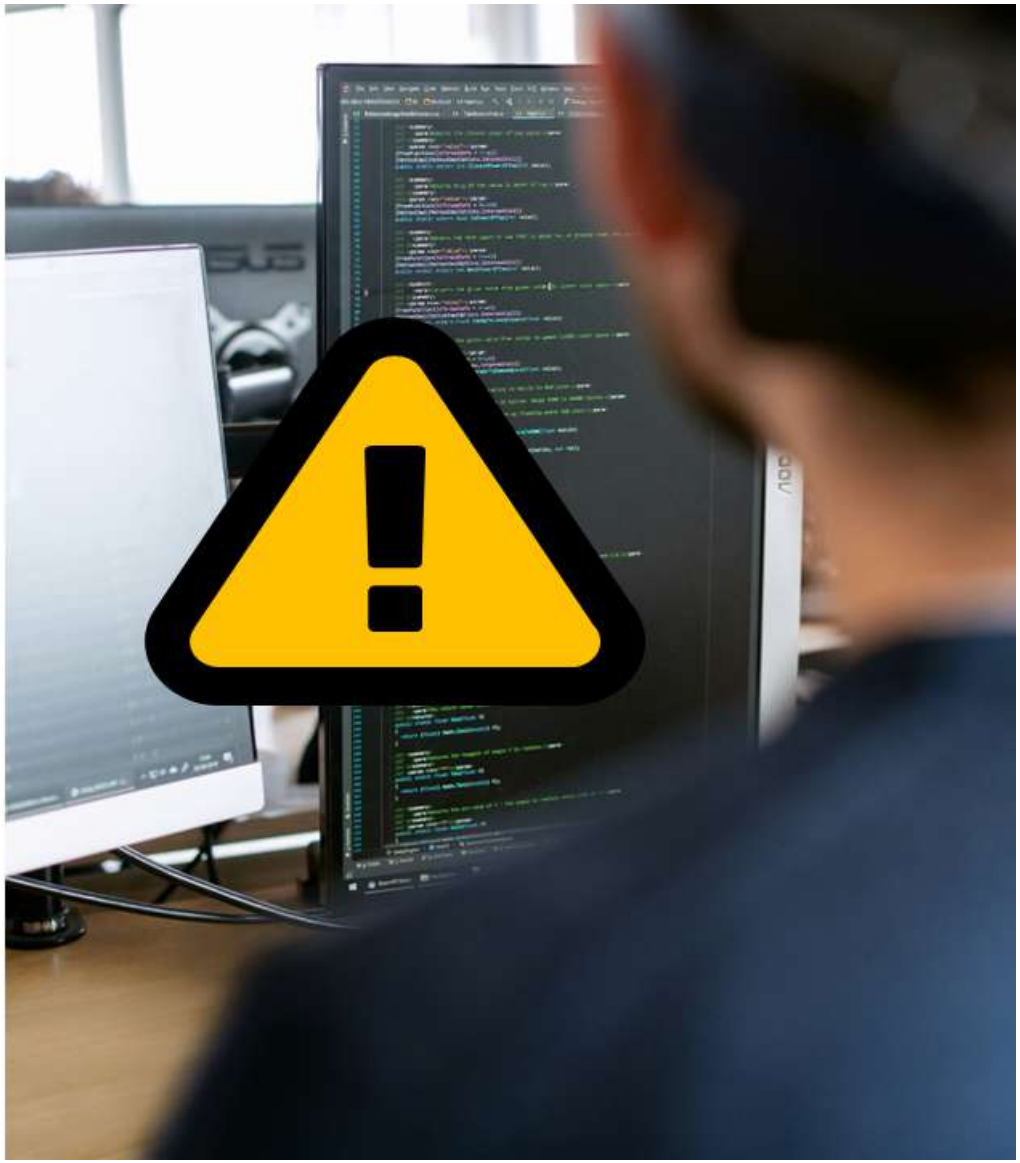
Inject 2.1 - Cyber

Your cybersecurity team has detected a breach in your project management system. The intrusion appears to have been ongoing for several weeks, with the attackers gaining access to sensitive data about your wind farm design and construction schedules.

The method of attack suggests a high level of sophistication, possibly indicating state-sponsored activity. Initial analysis shows that the attackers may have inserted subtle alterations to some of your technical specifications.

1. ***What immediate actions should NREC take in response to this situation?***
2. ***How might this situation escalate, and what preventive measures can be implemented?***
3. ***How can NREC ensure the integrity of its wind farm designs and construction plans while the extent of the breach is still being determined?***

Nordic Pine 2024



Exercise – a fictive scenario

Appendix: Cybersecurity Incident Report

Incident Title: Breach in Project Management System

Incident Summary:

- **Detection:** Your cybersecurity team has detected a breach in the project management system.
- **Duration:** The intrusion appears to have been ongoing for several weeks.
- **Affected Data:** Attackers gained access to sensitive data, including wind farm designs and construction schedules.
- **Method:** The method of attack suggests a high level of sophistication.
- **Alterations:** Initial analysis shows potential subtle alterations to technical specifications.

Affected Systems:

1. **Project Management Software:**
    - Accessed Data: Wind farm designs, construction schedules.
    - Alterations Detected: Subtle changes in technical specifications.
    - Vulnerabilities Exploited: Zero-day vulnerability in the software.

2. Network Infrastructure:
    - Compromised Nodes: Servers hosting project management software.
    - Data Traffic: Unusual data traffic patterns over the past few weeks.

Preliminary Forensic Analysis:

- **Intrusion Method:**
    - Use of sophisticated phishing emails targeting key personnel.
    - Exploitation of a zero-day vulnerability in the project management software.

- Remote access tools installed to maintain persistence.

- Indicators of Compromise (IOCs):
  - Unusual login times and IP addresses.
  - Unauthorized data exports.
  - Unexpected modifications in technical documents.
- Potential Impact:
  - Compromised integrity of wind farm design and construction data.
  - Risk of construction delays and cost overruns due to altered specifications.
  - Exposure of sensitive project timelines and strategic information.

Exercise – a fictive scenario

Inject 2.2 - Information

A coordinated disinformation campaign has emerged across multiple social media platforms, claiming that your wind farms are causing widespread health issues in nearby coastal communities. The campaign is employing sophisticated tactics, including deep fake videos of supposed medical experts and affected residents. Several popular influencers have amplified these claims, and mainstream media outlets are beginning to pick up the story. Your initial fact-checking efforts are struggling to keep pace with the rapidly evolving narrative.

1. ***What immediate actions should NREC take in response to this situation?***
2. ***How might this situation escalate, and what preventive measures can be implemented?***
3. ***How can NREC effectively counter this disinformation campaign without inadvertently giving it more visibility?***

Nordic Pine 2024

Exercise – a fictive scenario

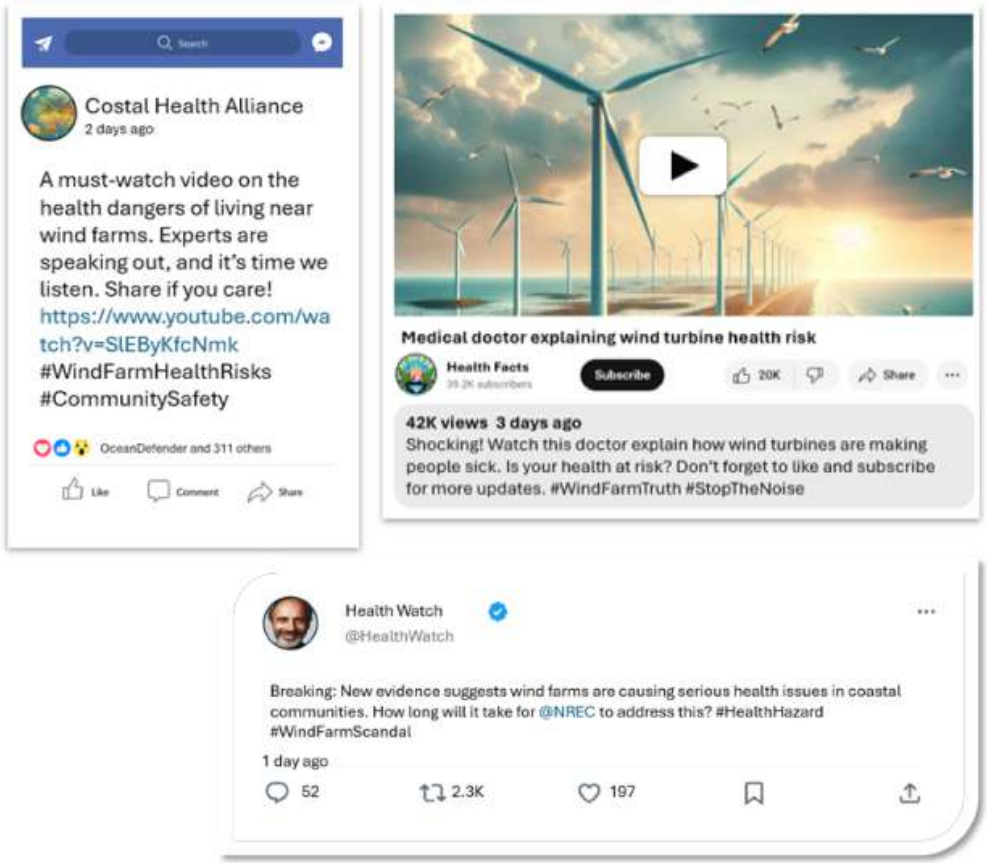
Communications Team Report

Our monitoring systems have detected a coordinated disinformation campaign across multiple social media platforms, alleging that NREC's wind farms are causing widespread health issues in nearby coastal communities.

This campaign utilizes sophisticated tactics, including deep fake videos featuring supposed medical experts and affected residents.

Several popular influencers have begun to amplify these claims, and mainstream media outlets are starting to pick up the story.

Our initial fact-checking efforts are struggling to keep up with the rapidly evolving narrative, making it challenging to counter the spread of misinformation.



Social Media - Examples

Exercise – a fictive scenario

Inject 2.3 – Supply Chain

You've discovered that a foreign investment firm with opaque ownership has been quietly acquiring shares in several of your key component suppliers.

While the acquisitions appear legal, there are concerns about potential supply chain vulnerabilities.

Simultaneously, you've noticed subtle quality issues in recent component shipments, nothing critical yet, but enough to raise suspicions.

Your attempts to investigate the investment firm have been met with layers of shell companies and offshore accounts.

What immediate actions should NREC take in response to this situation?

1. ***How might this situation escalate, and what preventive measures can be implemented?***
2. ***How can NREC protect its supply chain integrity without triggering potential contractual or diplomatic issues?***

Nordic Pine 2024

Exercise – a fictive scenario

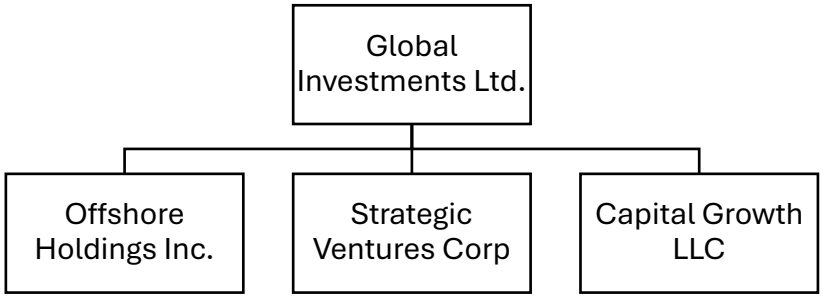
Financial Intelligence Report to NREC

Complex Ownership Structure of Foreign Investment Firm and Recent Acquisitions

1. Summary

This report outlines the findings related to a foreign investment firm that has been acquiring shares in several key component suppliers for our wind farm project. The ownership structure of the firm is complex and obscured by multiple layers of shell companies and offshore accounts. Recent acquisitions and subtle quality issues in component shipments raise concerns about potential supply chain vulnerabilities.

2. Ownership Structure:



Global Investments Ltd. Cayman Islands. Investment and holdings

Offshore Holdings Inc. British Virgin Islands. Major shareholder in Global Investments Ltd.

Strategic Ventures Corp. Luxembourg. Subsidiary of Offshore Holdings Inc.

Capital Growth LLC Delaware, USA. Minor shareholder in Global Investments Ltd.

3. Recent Acquisitions:

Supplier A:

Company Name: WindTech Components

Shares Acquired: 25%

Date of Acquisition: 8 August 2024

Acquisition Method: Direct purchase through Global Investments Ltd.

Supplier B:

Company Name: GreenEnergy Supplies

Shares Acquired: 30%

Date of Acquisition: 15 July 2024

Acquisition Method: Acquired via Strategic Ventures Corp.

Supplier C:

Company Name: EcoParts Manufacturing

Shares Acquired: 20%

Date of Acquisition: 25 July 2024

Acquisition Method: Indirect purchase through Capital Growth LLC

4. Concerns and Observations:

Opaque Ownership

The true ownership of Global Investments Ltd. is obscured by multiple shell companies and offshore accounts, making it difficult to ascertain the ultimate beneficial owners.

Quality Issues

Recent shipments from WindTech Components and GreenEnergy Supplies have shown subtle quality issues, raising suspicions about potential tampering or cost-cutting measures.

Supply Chain Vulnerability

The acquisitions, while legal, suggest a strategic interest in key suppliers that could lead to potential manipulation or disruption of our supply chain.

Exercise – a fictive scenario

Inject 2.4 – Cyber

Your operations team has reported erratic behaviour in the control systems of several offshore wind turbines.

The issues seem to be intermittent and subtle, causing minor fluctuations in power output and occasional safety system activations. Your initial diagnostics haven't revealed any clear software or hardware faults.

However, a deep dive into the system logs has uncovered traces of what appears to be a sophisticated, custom-made malware designed to create small, hard-to-detect disruptions.

1. ***What immediate actions should NREC take in response to this situation?***
2. ***How might this situation escalate, and what preventive measures can be implemented?***
3. ***How can NREC address this potential cybersecurity threat without causing unnecessary downtime in its power generation capabilities?***

Exercise – a fictive scenario

Inject 2. 5 - Economic

Unusual fluctuations in the energy market are causing unexpected financial strain on NREC's daily power trading activities as well as long-term contracting arrangements.

Analysis suggests possible market manipulation, but the source and mechanism are unclear. Simultaneously, you've received confidential intelligence that a state actor may be using economic warfare tactics to undermine renewable energy initiatives in the region.

Your financial team has also noticed a series of sophisticated phishing attempts targeting your traders and financial analysts.

1. ***What immediate actions should NREC take in response to this situation?***
2. ***How might this situation escalate, and what preventive measures can be implemented?***
3. ***How can NREC protect its financial interests and market position while navigating these complex and potentially manipulated market conditions?***

Tabletop Exercise (TTX)

Stage Information Package, #3

#3

TTX Stage Information Package: #3

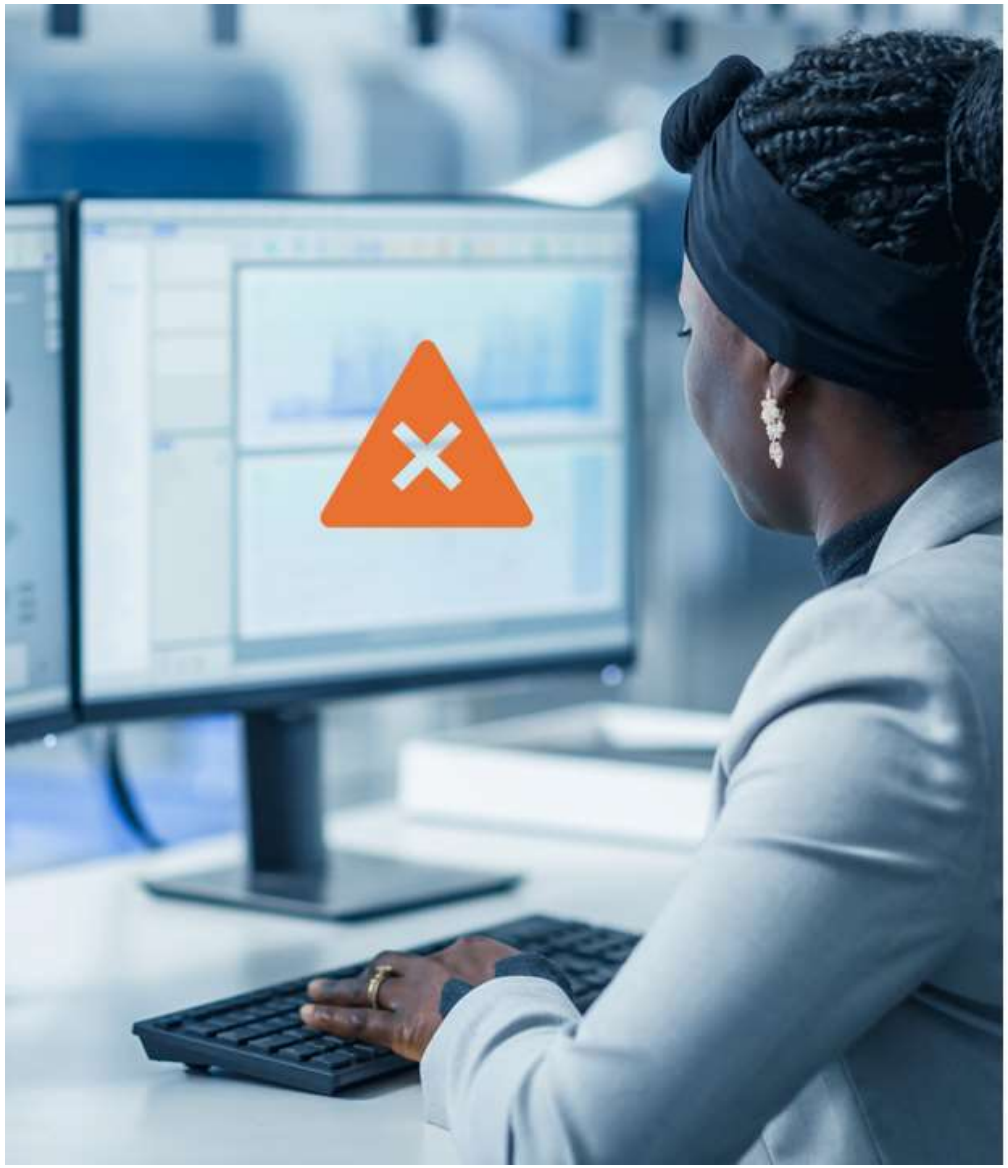
Content

- Stage Instructions
- Inject 2.4 Cyber
- Inject 2.5 Supply Chain + Appendix "Economic Analysis Report"

Stage instructions

- Take part, and read *the Stage Information package,* including.:
    - Two (2) Injects + appendixes
- Discuss solutions to the Injects presented.
- Fill in the *Inject Response Form*
- Be prepared to receive and mange additional injects
- Be prepared to present your Response/Lessons Identified, **<2min.**
- **Keep the time**

*O*ver time, write down comments, feedback associated to the exercise in *the Feedback form*



Exercise – a fictive scenario

Inject 2.4 – Cyber

Your operations team has reported erratic behaviour in the control systems of several offshore wind turbines.

The issues seem to be intermittent and subtle, causing minor fluctuations in power output and occasional safety system activations. Your initial diagnostics haven't revealed any clear software or hardware faults.

However, a deep dive into the system logs has uncovered traces of what appears to be a sophisticated, custom-made malware designed to create small, hard-to-detect disruptions.

Exercise – a fictive scenario

Inject 2. 5 - Economic

Unusual fluctuations in the energy market are causing unexpected financial strain on NREC's daily power trading activities as well as long-term contracting arrangements.

Analysis suggests possible market manipulation, but the source and mechanism are unclear. Simultaneously, you've received confidential intelligence that a state actor may be using economic warfare tactics to undermine renewable energy initiatives in the region.

Your financial team has also noticed a series of sophisticated phishing attempts targeting your traders and financial analysts.

Tabletop Exercise (TTX)

Stage Information Package, #4

#4

TTX Stage Information Package: #4

Content

- Stage Instructions
- Scenario Overview – Phase 3 Crisis Point
- Inject 3.1 Cyber
- Inject 3.2 Supply Chain

Stage instructions

- Take part, and read *the Stage Information package,* including.:
    - Two (2) Injects
- Discuss solutions to the Injects presented.
- Fill in the *Inject Response Form*
- Be prepared to receive and mange additional injects
- Be prepared to present your Response/Lessons Identified, **<2min.**
- **Keep the time**

*O*ver time, write down comments, feedback associated to the exercise in *the Feedback form*

Exercise – a fictive scenario

Phase 3 - Crisis Point

As NREC, you now find yourself at the peak of the crisis, eight months into your offshore wind farm projects.

The situation has escalated dramatically on multiple fronts. International tensions are at a breaking point, with the neighbouring state's military exercises causing significant concern and edging closer to your operational areas. Your new offshore wind farm project is nearing completion, but the challenges you face have grown exponentially.

The cyber threats you've been battling have evolved into full-scale attacks, your supply chain is in disarray, and public opinion has turned sharply against you.

As the Strategic Planning and Response Team, you're now in crisis management mode. The decisions you make in this phase will be critical not just for NREC's survival, but potentially for the energy security and stability of the entire region. You must act swiftly and decisively, balancing short-term crisis response with long-term strategic considerations.

Exercise – a fictive scenario

Inject 3.1 - Cyber

A sophisticated cyberattack has breached your SCADA systems, causing widespread disruption across your wind farm network.

Multiple turbines are behaving erratically, with some shutting down completely and others operating outside safe parameters. The situation is ongoing and cascading, with more systems being disrupted.

There's a significant risk of equipment damage and power supply disruptions. Initial analysis suggests the attack may have exploited the vulnerabilities introduced by the earlier intrusion into your project management system.

Exercise – a fictive scenario

Inject 3.2 – Supply Chain

A series of coordinated protests have erupted at existing NREC facilities, such as boats, onshore substations, headquarters and regional offices across the region, effectively blocking access and disrupting operations.

While some protesters appear to be genuine environmental activists, intelligence suggests that others may be paid actors with ties to foreign interests.

Simultaneously, you've received reports of suspicious drones flying near your offshore installations, and there are unconfirmed sightings of unmarked submarines in the vicinity of your undersea cables.

Tabletop Exercise (TTX)

Stage Information Package, #5

#5

TTX Stage Information Package: #5

Content

- Stage Instructions
- Scenario Overview – Phase 3 Crisis Point
- Inject 3.3 Information + two (2) appendixes.
- Inject 3.4 Cyber

Stage instructions

- Take part, and read *the Stage Information package,* including.:
    - Two (2) Injects + appendixes
- Discuss solutions to the Injects presented.
- Fill in the *Inject Response Form*
- Be prepared to receive and mange additional injects
- Be prepared to present your Response/Lessons Identified, **<2min.**
- **Keep the time**

*O*ver time, write down comments, feedback associated to the exercise in *the Feedback form*

Exercise – a fictive scenario

Phase 3 - Crisis Point

As NREC, you now find yourself at the peak of the crisis, eight months into your offshore wind farm projects.

The situation has escalated dramatically on multiple fronts. International tensions are at a breaking point, with the neighbouring state's military exercises causing significant concern and edging closer to your operational areas. Your new offshore wind farm project is nearing completion, but the challenges you face have grown exponentially.

The cyber threats you've been battling have evolved into full-scale attacks, your supply chain is in disarray, and public opinion has turned sharply against you.

As the Strategic Planning and Response Team, you're now in crisis management mode. The decisions you make in this phase will be critical not just for NREC's survival, but potentially for the energy security and stability of the entire region. You must act swiftly and decisively, balancing short-term crisis response with long-term strategic considerations.

Exercise – a fictive scenario

Inject 3.3 – Information

A deepfake video has surfaced showing NREC's CEO apparently admitting to bribing government officials to fast-track wind farm approvals and cover up environmental damages. The video is spreading rapidly across social media and being picked up by mainstream news outlets.

Simultaneously, a whistleblower has come forward claiming to have documents that support some of the allegations in the video. Your initial analysis suggests the video is fake, but the documents appear to be a mix of genuine internal communications taken out of context and sophisticated forgeries.

Exercise – a fictive scenario

Deepfake Video

Deepfake Video Transcript and Document Analysis

Transcript of Deepfake Video:
Video Title: NREC CEO Confession
Duration: 3:45 minutes
Transcript:

- **[00:00 - 00:30]**
  - CEO: "We've managed to fast-track the approvals for our wind farm projects by providing certain incentives to government officials."
- **[00:31 - 01:15]**
  - CEO: "Environmental concerns were becoming a major roadblock, but we took care of it discreetly to avoid any delays."
- **[01:16 - 02:00]**
  - CEO: "Our strategy included convincing the inspectors to overlook some minor violations in exchange for future benefits."
- **[02:01 - 03:00]**
  - CEO: "This approach has been crucial in maintaining our project timelines and financial targets."
- **[03:01 - 03:45]**
  - CEO: "Ensuring the success of our operations sometimes requires unconventional methods, and we are prepared to do what's necessary."

Annotations, highlighting potential manipulations:
[00:10 - 00:20]: Unnatural lip movement and inconsistent audio quality.
[00:35 - 00:40]: Sudden change in lighting and shadows on the CEO's face.
[01:00 - 01:05]: Audio artifacts suggesting splicing of different audio clips.
[02:15 - 02:20]: Mismatch between lip sync and spoken words.
[03:10 - 03:20]: Visible digital artifacts around the CEO's mouth, indicating possible deepfake technology.

Nordic Pine 2024

Exercise – a fictive scenario

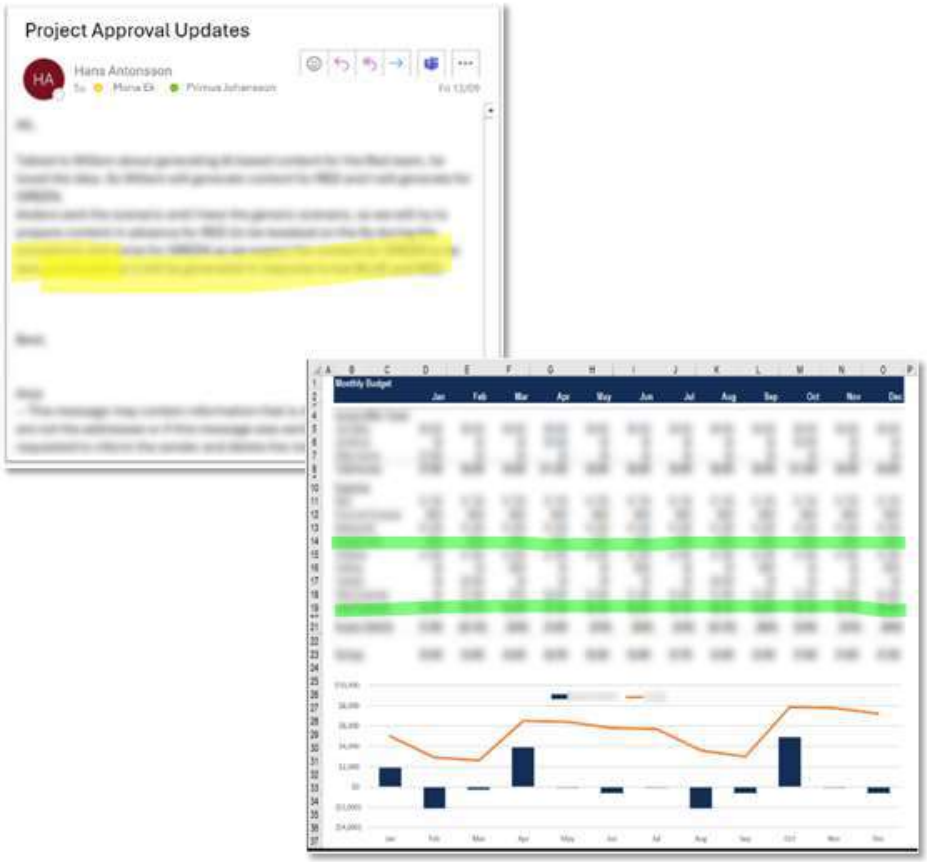
Whistleblower's Documents

Preliminary Analysis of Whistleblower's Documents:

1. Document 1: Internal Email Communication
   - Subject: "Project Approval Updates"
   - Content: Discussion on meeting project deadlines and regulatory hurdles.
   - Analysis: Genuine internal communication, but statements are taken out of context to suggest unethical behavior.

2. Document 2: Financial Report Excerpt
   - Subject: "Expense Allocation for Q2"
   - Content: Budget allocations for project-related expenses.
   - Analysis: Contains some genuine financial data, but additional lines have been inserted to imply bribes and illicit payments.

3. Document 3: Environmental Impact Summary
   - Subject: "Environmental Compliance Status"
   - Content: Summary of environmental impact assessments and mitigation measures.
   - Analysis: Mix of authentic and forged content, with manipulated sections to exaggerate environmental violations.



Exercise – a fictive scenario

Inject 3.4 – cyber

Your emergency communication systems are experiencing a massive distributed denial-of-service (DDoS) attack, severely hampering your ability to coordinate responses to the ongoing crises.

Simultaneously, you've detected unauthorized access attempts to your backup communication channels.

Your IT team suspects that the attackers may have gained access to your emergency protocols through the earlier breach of your project management system.

Tabletop Exercise (TTX)

Stage Information Package, #6

Nordic Pine 2024 – 24-26th Sep

#6

TTX Stage Information Package: #6

Content

- Stage Instructions
- Scenario Overview – Phase 4 Response and Mitigation
- Scenario Overview – Phase 5 Recovery and Lessons Learned

Stage instructions

- Take part, and read *the Stage Information package,* including.:
    - Two (2) Scenario Overview.
- Discuss solutions to Phase 4 and Phase 5.
- Fill in the *Inject Response Form*
- Be prepared to present your Response/Lessons Identified.
- Keep the time

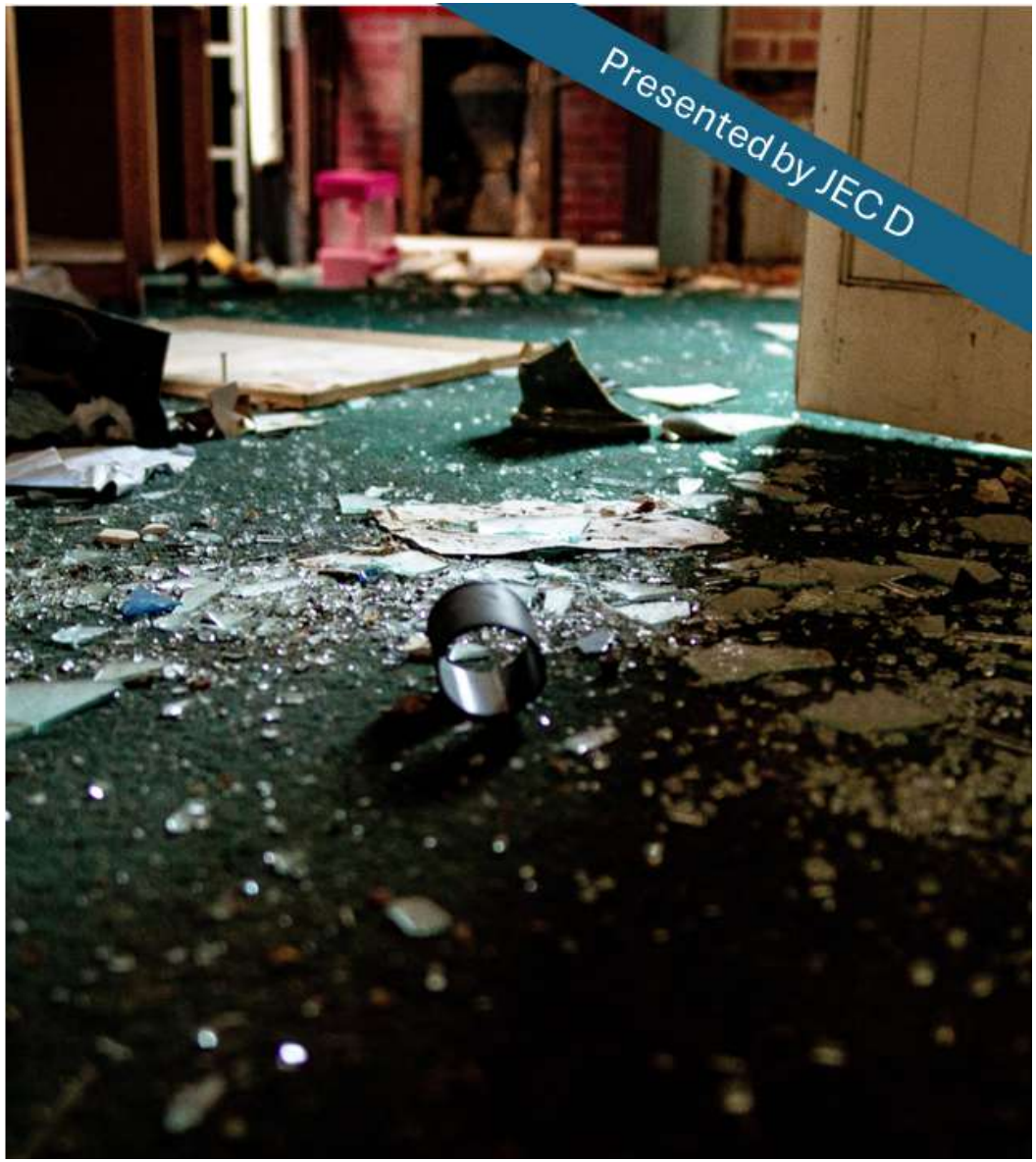
Exercise – a fictive scenario

Phase 4 - Response and Mitigation

As NREC, you've weathered the peak of the crisis and are now ten months into your turbulent journey. The immediate storm has passed, but you're far from calm waters. Your operational offshore wind farm project, while operational, is running at reduced capacity due to the recent attacks and disruptions.

The global situation remains volatile, with increased scrutiny on the energy sector and your operations. As the Strategic Planning and Response Team, your focus has shifted from crisis management to damage control, reputation rebuilding, and long-term resilience planning.

The decisions you make in this phase will be crucial for NREC's recovery and future stability. You must balance the need for transparency with security concerns, address the lingering effects of the crisis, and prepare for potential future threats, all while working to restore normal operations and rebuild trust with stakeholders.



Exercise – a fictive scenario

Phase 5 - Recovery and Lessons Learned

As NREC, you've reached the twelve-month mark of this tumultuous journey.

The acute crisis has passed, but its effects continue to ripple through your organization and the broader energy sector. Your offshore wind farm project is fully operational yet operating in a new reality of heightened security concerns and public scrutiny.

The global situation has stabilized somewhat, but a new normal of increased vigilance and complex geopolitical manoeuvring has set in. As the Strategic Planning and Response Team, your focus now is on long-term recovery, implementing lessons learned, and preparing for future challenges.

The decisions you make in this phase will shape NREC's resilience and adaptability in the face of evolving threats. You must balance the need for increased security with operational efficiency, rebuild trust with stakeholders, and position NREC as a leader in secure and sustainable energy production.

Inject handouts

- Inject 2.3 Financial Intelligence Report
- Inject 2.5 Economic Analysis Report
- Inject 3.5 PM Legal Brief and appendix and supply chain appendix
- Inject 4.3 Confidential Intelligence Brief
- Inject 4.5 Financial Analysis Report
- Inject 5.5 Risk Assessment Report
- Cyber injects

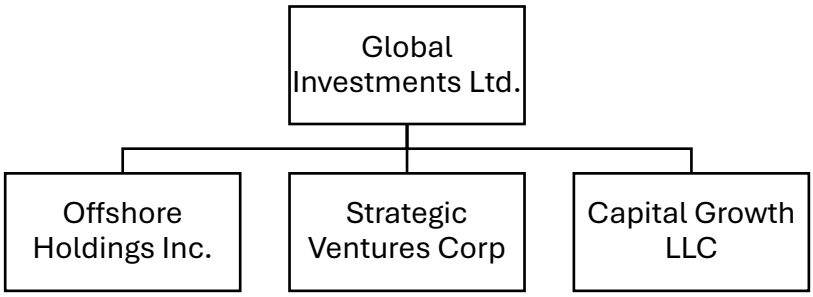
Financial Intelligence Report to NREC

Complex Ownership Structure of Foreign Investment Firm and Recent Acquisitions

1. Summary

This report outlines the findings related to a foreign investment firm that has been acquiring shares in several key component suppliers for our wind farm project. The ownership structure of the firm is complex and obscured by multiple layers of shell companies and offshore accounts. Recent acquisitions and subtle quality issues in component shipments raise concerns about potential supply chain vulnerabilities.

2. Ownership Structure:



Global Investments Ltd. Cayman Islands. Investment and holdings

Offshore Holdings Inc. British Virgin Islands. Major shareholder in Global Investments Ltd.

Strategic Ventures Corp. Luxembourg. Subsidiary of Offshore Holdings Inc.

Capital Growth LLC Delaware, USA. Minor shareholder in Global Investments Ltd.

3. Recent Acquisitions:

Supplier A:

Company Name: WindTech Components
Shares Acquired: 25%
Date of Acquisition: 8 August 2024
Acquisition Method: Direct purchase through Global Investments Ltd.

Supplier B:

Company Name: GreenEnergy Supplies
Shares Acquired: 30%
Date of Acquisition: 15 July 2024
Acquisition Method: Acquired via Strategic Ventures Corp.

Supplier C:

Company Name: EcoParts Manufacturing
Shares Acquired: 20%
Date of Acquisition: 25 July 2024
Acquisition Method: Indirect purchase through Capital Growth LLC

4. Concerns and Observations:

Opaque Ownership

The true ownership of Global Investments Ltd. is obscured by multiple shell companies and offshore accounts, making it difficult to ascertain the ultimate beneficial owners.

Quality Issues

Recent shipments from WindTech Components and GreenEnergy Supplies have shown subtle quality issues, raising suspicions about potential tampering or cost-cutting measures.

Supply Chain Vulnerability

The acquisitions, while legal, suggest a strategic interest in key suppliers that could lead to potential manipulation or disruption of our supply chain.

NREC Internal Economic Analysis Report

Unusual Market Fluctuations and Suspected Economic Warfare Tactics

1. Summary

This report details the recent unusual fluctuations in the energy market that are causing unexpected financial strain on NREC's operations. Analysis indicates possible market manipulation. Concurrently, confidential intelligence suggests a state actor may be employing economic warfare tactics to undermine renewable energy initiatives in the region. Additionally, there have been sophisticated phishing attempts targeting NREC's traders and financial analysts.

2. Market Fluctuations

2.1. Electricity Prices

Significant price spikes observed over the past three weeks.

Volatility index has increased by 35% compared to the previous quarter.

2.2. Renewable Energy Credits

Unusual trading volumes, with large buy and sell orders executed within short periods.

Prices of renewable energy credits have dropped by 20% unexpectedly.

2.3. Supply and Demand:

Reports of sudden changes in energy demand forecasts from major consumers.

Supply chain disruptions in key component deliveries have affected production stability.

3. Potential Market Manipulation Indicators

3.1. Trading Patterns

Identified patterns suggest coordinated trading activities designed to create artificial volatility.

Large trades executed during low liquidity periods to maximize market impact.

3.2. Entities Involved

Several new, previously unknown entities have entered the market, executing large volume trades.

These entities are linked to offshore accounts and shell companies, making it difficult to trace ownership.

4. Suspected Economic Warfare Tactics

4.1. Confidential Intelligence Brief

Intelligence indicates a state actor is using economic tactics to destabilize renewable energy markets.

Methods include market manipulation, spreading disinformation about renewable energy reliability, and cyber-attacks on financial systems.

4.2. Targeted Phishing Attempts

Sophisticated phishing emails have been sent to NREC's traders and financial analysts.

Emails appear to come from legitimate market analysts and contain malware designed to capture sensitive financial information.

5. Impact Assessment

5.1. Financial Strain

Increased volatility has led to higher operational costs and financial uncertainty.

Potential loss of investor confidence in renewable energy projects.

5.2. Operational Risks

Supply chain disruptions and market instability could delay ongoing projects.

Manipulated market conditions could force NREC to sell energy at a loss.

Legal Brief to Strategic Planning and Response Team (SPRT)

Summary of Lawsuits Filed Against NREC

1. Summary

This brief provides an overview of the recent lawsuits filed against NREC in multiple jurisdictions, alleging environmental and health damages related to our wind farm projects. The timing and similarity of these lawsuits, along with the seizure of critical component shipments, suggest a potential coordinated effort to undermine our operations.

2. Lawsuit Details

Jurisdiction: Country A
Case Number: 12345/2024
Plaintiffs: Local Residents Association
Claims: Environmental pollution, noise pollution, adverse health effects
Status: Filed, awaiting court hearing

Jurisdiction: Country B
Case Number: 67890/2024
Plaintiffs: Environmental Advocacy Group
Claims: Destruction of natural habitats, violation of environmental regulations
Status: Filed, preliminary injunction granted

Jurisdiction: Country C
Case Number: 11223/2024
Plaintiffs: Coastal Community Coalition
Claims: Impact on marine life, water contamination, respiratory issues
Status: Filed, discovery phase

3. Common Themes in Lawsuits

Environmental Impact:

- Allegations of pollution and destruction of natural habitats.
- Claims of non-compliance with environmental regulations.

Health Concerns:

- Accusations of causing respiratory issues and other health problems among local populations.
- Reports of noise pollution affecting mental health and well-being.

Regulatory Violations:

- Assertions that NREC has bypassed or violated local and international environmental laws.
- Claims of insufficient environmental impact assessments and mitigation measures.

4. Potential Coordinated Legal Strategy

Simultaneous Filing:

- Lawsuits filed in multiple jurisdictions within a short timeframe.
- Similar language and claims used across different cases.
-

Plaintiff Networks:

- Coordination among various local and international advocacy groups.
- Use of shared legal resources and representation.
-

Public Relations Campaign:

- Efforts to amplify legal actions through media coverage and public campaigns.
- Aim to damage NREC's reputation and stall project progress.

5. Implications for NREC

Project Delays:

- Legal battles and customs issues could significantly delay project completion.
- Potential financial losses due to halted operations and contractual penalties.

Reputational Damage:

- Negative publicity from lawsuits and seized shipments may affect stakeholder confidence.
- Risk of losing investor support and market credibility.

Increased Scrutiny:

- Heightened regulatory and public scrutiny on NREC's operations and compliance practices.
- Possible future restrictions and tougher regulatory requirements.

Legal Brief to Strategic Planning and Response Team (SPRT)

Summary of Lawsuits Filed Against NREC

1. Summary

This brief provides an overview of the recent lawsuits filed against NREC in multiple jurisdictions, alleging environmental and health damages related to our wind farm projects. The timing and similarity of these lawsuits, along with the seizure of critical component shipments, suggest a potential coordinated effort to undermine our operations.

2. Lawsuit Details

Jurisdiction: Country A
Case Number: 12345/2024
Plaintiffs: Local Residents Association
Claims: Environmental pollution, noise pollution, adverse health effects
Status: Filed, awaiting court hearing

Jurisdiction: Country B
Case Number: 67890/2024
Plaintiffs: Environmental Advocacy Group
Claims: Destruction of natural habitats, violation of environmental regulations
Status: Filed, preliminary injunction granted

Jurisdiction: Country C
Case Number: 11223/2024
Plaintiffs: Coastal Community Coalition
Claims: Impact on marine life, water contamination, respiratory issues
Status: Filed, discovery phase

3. Common Themes in Lawsuits

Environmental Impact:

- Allegations of pollution and destruction of natural habitats.
- Claims of non-compliance with environmental regulations.

Health Concerns:

- Accusations of causing respiratory issues and other health problems among local populations.
- Reports of noise pollution affecting mental health and well-being.

Regulatory Violations:

- Assertions that NREC has bypassed or violated local and international environmental laws.
- Claims of insufficient environmental impact assessments and mitigation measures.

4. Potential Coordinated Legal Strategy

Simultaneous Filing:

- Lawsuits filed in multiple jurisdictions within a short timeframe.
- Similar language and claims used across different cases.
-

Plaintiff Networks:

- Coordination among various local and international advocacy groups.
- Use of shared legal resources and representation.
-

Public Relations Campaign:

- Efforts to amplify legal actions through media coverage and public campaigns.
- Aim to damage NREC's reputation and stall project progress.

5. Implications for NREC

Project Delays:

- Legal battles and customs issues could significantly delay project completion.
- Potential financial losses due to halted operations and contractual penalties.

Reputational Damage:

- Negative publicity from lawsuits and seized shipments may affect stakeholder confidence.
- Risk of losing investor support and market credibility.

Increased Scrutiny:

- Heightened regulatory and public scrutiny on NREC's operations and compliance practices.
- Possible future restrictions and tougher regulatory requirements.

Exercise – a fictive scenario

Inject 3.5 – Supply Chain

Critical component shipments for your nearly-completed wind farm project have been seized by customs officials in a transit country, citing vague "security concerns." This delay threatens to derail your entire project timeline.

Simultaneously, you've received intelligence that suggests this may be part of a coordinated effort to undermine renewable energy projects in the region.

You have received corroborating details from peer firms in the Nordics, who are experiencing similar component seizures, which might amplify the risk in the region.

Your legal team has also alerted you to a sudden flurry of lawsuits being filed against NREC in multiple jurisdictions, all making similar claims about environmental and health damages.

Confidential Intelligence Brief to Strategic Planning and Response Team (Hardcopy handouts)

Subject: Suspected State-Sponsored Campaign Against Regional Energy Infrastructure

Overview:

This intelligence brief provides an assessment of the recent cyberattacks, disinformation campaigns, and physical disruptions targeting regional energy infrastructure, specifically focusing on NREC due to its innovative technologies and significant regional influence.

RiskSupportIntelligence

Risk Support Intelligence AB
Nordic Pine 2024
Jönköping Sweden

Exercise – a fictive scenario

Exercise – a fictive scenario

Key Findings:

- **State Actor Involvement:**
  - Intelligence sources indicate a coordinated effort by [Redacted] to destabilize the region's energy infrastructure.
  - The campaign is believed to be part of a broader strategy to undermine renewable energy initiatives and maintain regional dominance in traditional energy sectors.
- **Targets and Methods:**
  - NREC was specifically targeted due to its leadership in innovative energy technologies and its influence in the regional market.
  - Tactics employed include sophisticated cyberattacks on SCADA systems, widespread disinformation campaigns, and orchestrated physical disruptions.
- **Objectives:**
  - Disrupt the development and deployment of renewable energy projects.
  - Create public distrust and regulatory challenges for renewable energy companies.
  - Undermine investor confidence and financial stability of key energy firms.

Incident Analysis:

- **Cyberattacks:**
  - Persistent and sophisticated intrusions into project management and SCADA systems.
  - Exploitation of zero-day vulnerabilities and use of advanced persistent threats (APTs).
- **Disinformation Campaigns:**
  - Circulation of deepfake videos and falsified documents to discredit NREC's leadership and operations.
  - Use of social media and mainstream news outlets to spread false information and incite public opposition.
- **Physical Disruptions:**
  - Seizure of critical component shipments by customs officials citing vague "security concerns."
  - Reports of sabotage and unexplained malfunctions in newly installed wind turbines.

Potential Impact

Operational Disruptions:

- Delays and increased costs due to disrupted supply chains and project timelines.
- Risk of equipment damage and reduced operational efficiency.

Reputational Damage:

- Negative public perception and loss of stakeholder confidence.
- Increased scrutiny from regulatory bodies and potential legal challenges.

Diplomatic Repercussions:

- Public disclosure of state actor involvement could escalate international tensions.
- Potential for retaliatory measures affecting broader geopolitical stability.

Nordica Renewable Energy Consortium

NREC Financial Intelligence Report

Economic Attacks on NREC Subsidiaries and Potential Foreign Buyout Attempts

1. Summary

This report outlines the recent economic sabotage targeting NREC's smaller subsidiaries through a combination of cyber attacks, market manipulation, and regulatory pressures. It also details the implications of foreign buyout attempts by an investment firm suspected of seeking access to sensitive technologies.

2. Economic Attacks

Cyber Attacks

- Multiple subsidiaries have experienced sophisticated cyber intrusions aimed at disrupting financial systems and erasing critical data.
- Examples include ransomware attacks, unauthorized access to financial records, and data breaches.

Market Manipulation

- Unusual trading patterns and artificial price drops in the shares of affected subsidiaries.
- Coordinated short-selling activities leading to a significant devaluation of subsidiary stocks.

Regulatory Pressures

- Sudden and unexpected regulatory audits and fines imposed on subsidiaries.
- Increased scrutiny from financial and environmental regulatory bodies, causing operational delays and additional costs.

3. Foreign Buyout Attempts

Investment Firm Activity

- Firm Name: [redacted]
- Ownership: Foreign-owned, with a complex structure of shell companies and offshore accounts.

- Recent Activity: Aggressive acquisition attempts targeting financially distressed subsidiaries.

Subsidiaries Targeted

Subsidiary A: SolarTech Innovations

- Financial Impact: Cyber attack led to temporary shutdown, causing revenue losses.
- Buyout Offer: Below market value, citing financial instability.

Subsidiary B: GreenPower Solutions

- Financial Impact: Market manipulation resulted in a 30% drop in stock price.
- Buyout Offer: Attractive but contingent on access to proprietary technology.

Subsidiary C: EcoEnergy Systems

- **Financial Impact:** Regulatory fines have strained financial resources.
- **Buyout Offer:** Positioned as a rescue operation but with terms favoring the acquiring firm.

4. Potential Implications:

Operational Control:

- Loss of control over strategic assets and sensitive technologies.
- Potential integration of foreign interests into NREC's core operations, posing security risks.

Financial Stability:

- Immediate financial relief from buyouts may lead to long-term vulnerabilities.
- Risk of further market manipulation and economic sabotage if foreign interests gain foothold.

Technological Security:

- Exposure of proprietary technologies and intellectual property to foreign entities.
- Increased risk of industrial espionage and loss of competitive edge.

Nordica Renewable Energy Consortium

Risk Assessment Report on Key Suppliers

Security Concerns Regarding Compromised Suppliers

Summary

As part of our efforts to strengthen the supply chain, we have uncovered evidence suggesting that some longtime suppliers may have been compromised by foreign interests. The nature of the compromise is subtle, indicating the potential for future exploitation or data gathering. This report highlights the potential security concerns associated with these suppliers.

Key Suppliers and Potential Security Concerns:

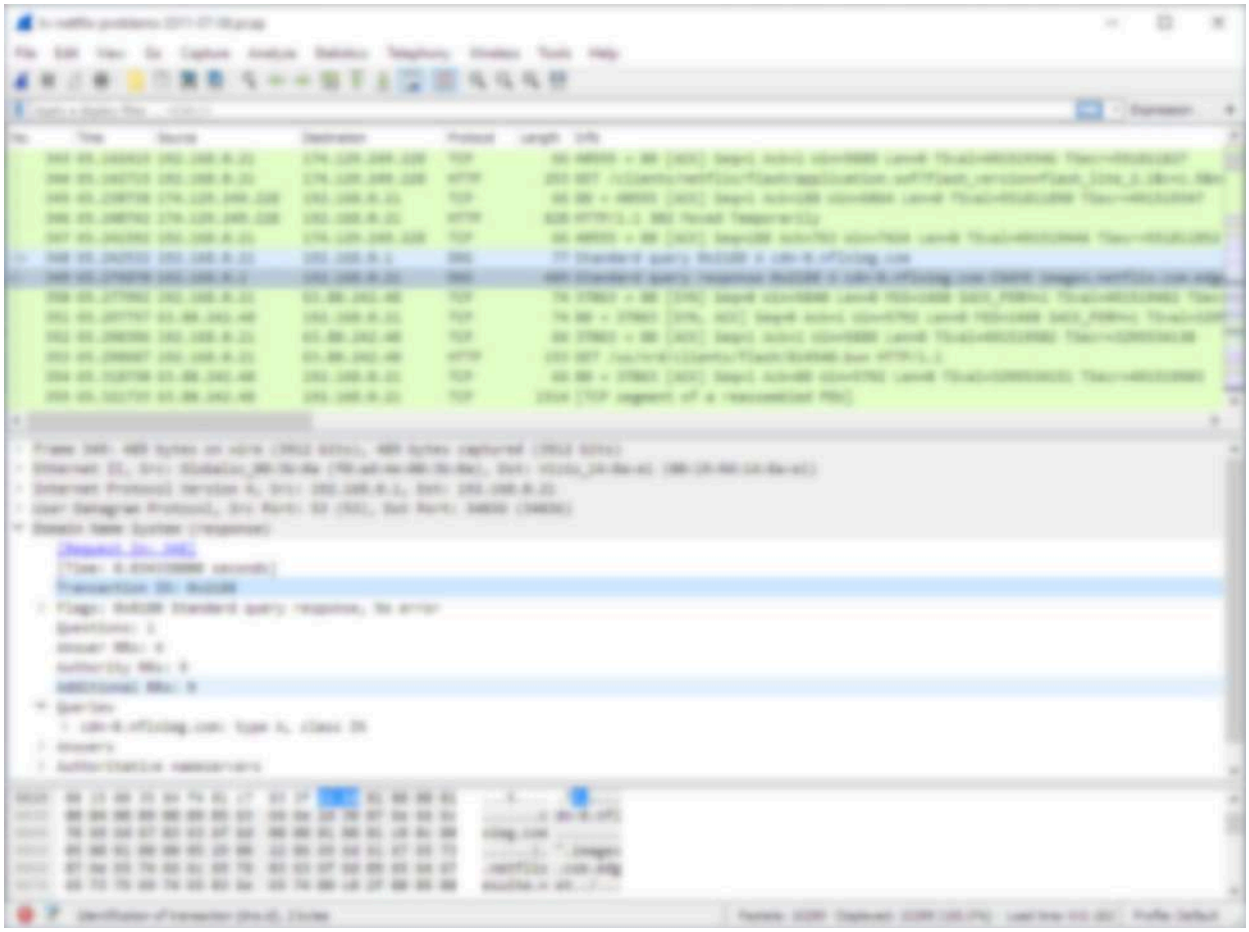
1. **Supplier A: TechParts Ltd.**
   Integration Level: High
   Evidence of Compromise: Unusual data requests and communication patterns.
   Potential Risk: Data leakage and intellectual property theft.
   Impact of Severance: Significant disruption in supply of critical components.

2. **Supplier B: GreenEnergy Solutions**
   Integration Level: Medium
   Evidence of Compromise: Increased third-party subcontracting with foreign entities.
   Potential Risk: Supply chain vulnerability and indirect access to sensitive information.
   Impact of Severance: Moderate disruption, manageable with alternative suppliers.

3. **Supplier C: PowerDynamics Inc.**
   Integration Level: High
   Evidence of Compromise: Suspicious financial transactions and changes in ownership structure.
   Potential Risk: Financial manipulation and operational sabotage.
   Impact of Severance: High disruption, potential delays in project timelines.

Inject 1.1

Network Traffic Log



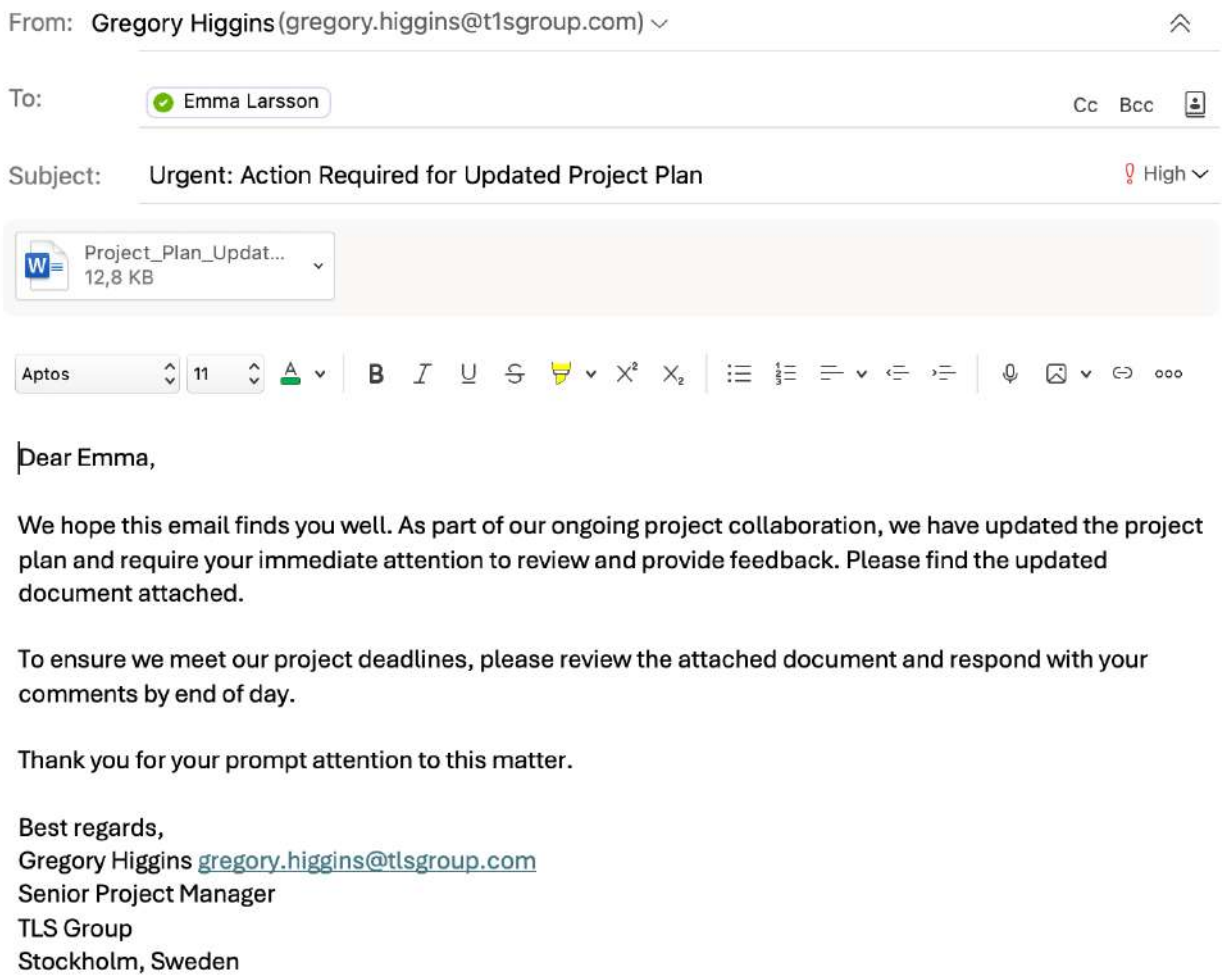
Excerpt:

- **Date/Time:** 10:45:32
    - **Source IP:** 203.0.113.45 … etc
    - **Destination IP:** 10.0.0.5 (Wind Turbine Control Node)
    - **Protocol:** TCP
    - **Port:** 8080
    - **Action:** Denied
    - **Notes:** Multiple attempts from various IP addresses, abnormal traffic pattern
- **Date/Time:** 10:46:15
    - **Source IP:** 198.51.100.23
    - **Destination IP:** 10.0.0.12 (SCADA System)
    - **Protocol:** UDP

    - **Port:** 502
    - **Action:** Denied
    - **Notes:** Unrecognized signature, possible reconnaissance
- **Date/Time:** 10:47:03
    - **Source IP:** 192.0.2.50
    - **Destination IP:** 10.0.0.8 (Wind Turbine Control Node)
    - **Protocol:** TCP
    - **Port:** 443
    - **Action:** Allowed
    - **Notes:** Established connection, duration 15 seconds, then terminated
- **Date/Time:** 10:48:22
    - **Source IP:** 203.0.113.45
    - **Destination IP:** 10.0.0.5 (Wind Turbine Control Node)
    - **Protocol:** TCP
    - **Port:** 8080
    - **Action:** Denied
    - **Notes:** Repeated attempt, consistent with previous patterns
- **Date/Time:** 10:49:01
    - **Source IP:** 198.51.100.23
    - **Destination IP:** 10.0.0.15 (SCADA System)
    - **Protocol:** UDP
    - **Port:** 502
    - **Action:** Denied
    - **Notes:** Persistent probing, no data payload
- **Date/Time:** 10:50:37
    - **Source IP:** 192.0.2.100
    - **Destination IP:** 10.0.0.8 (Wind Turbine Control Node)
    - **Protocol:** TCP
    - **Port:** 443
    - **Action:** Denied
    - **Notes:** Single attempt, matches prior anomaly pattern

Inject 1.4

Phishing Email:



Highlighted Areas of Concern:

1. **From Address:** Although the email appears to come from a trusted partner, the actual email address is slightly altered (e.g., " gregory.higgins@t1sgroup.com " instead of " gregory.higgins@tlsgroup.com ").
2. **Urgency:** The email creates a sense of urgency, which is a common tactic in phishing attempts to prompt quick action without due diligence.
3. **Attachment:** The attached document contains malware capable of exploiting a zero-day vulnerability. Opening this file could lead to system compromise.
4. **Salutation and Signature:** While the names and contact information appear correct, always verify by cross-referencing with known contact details.

Inject 2.1

Cybersecurity Incident Report

Incident Title: Breach in Project Management System

Incident Summary:

- **Detection:** Your cybersecurity team has detected a breach in the project management system.
- **Duration:** The intrusion appears to have been ongoing for several weeks.
- **Affected Data:** Attackers gained access to sensitive data, including wind farm designs and construction schedules.
- **Method:** The method of attack suggests a high level of sophistication.
- **Alterations:** Initial analysis shows potential subtle alterations to technical specifications.

Affected Systems:

1. **Project Management Software:**
    - Accessed Data: Wind farm designs, construction schedules.
    - Alterations Detected: Subtle changes in technical specifications.
    - Vulnerabilities Exploited: Zero-day vulnerability in the software.
2. **Network Infrastructure:**
    - Compromised Nodes: Servers hosting project management software.
    - Data Traffic: Unusual data traffic patterns over the past few weeks.

Preliminary Forensic Analysis:

- **Intrusion Method:**
    - Use of sophisticated phishing emails targeting key personnel.
    - Exploitation of a zero-day vulnerability in the project management software.

- Remote access tools installed to maintain persistence.

- **Indicators of Compromise (IOCs):**
  - Unusual login times and IP addresses.
  - Unauthorized data exports.
  - Unexpected modifications in technical documents.
- **Potential Impact:**
  - Compromised integrity of wind farm design and construction data.
  - Risk of construction delays and cost overruns due to altered specifications.
  - Exposure of sensitive project timelines and strategic information.

Inject 3.1

Real-Time Dashboard: SCADA System Anomalies

Affected Turbines:

1. **Turbine ID:** WT-01
   - **Status:** Shut down
   - **Issue:** Unauthorized remote shutdown command
   - **Risk Level:** High
2. **Turbine ID:** WT-02
   - **Status:** Operating at 150% capacity
   - **Issue:** Over-speed condition
   - **Risk Level:** Critical (imminent equipment failure)
3. **Turbine ID:** WT-03
   - **Status:** Erratic operation
   - **Issue:** Inconsistent power output
   - **Risk Level:** Moderate

4. **Turbine ID:** WT-04
    - **Status:** Operating normally
    - **Issue:** No anomalies detected
    - **Risk Level:** Low

System Anomalies:

- **Unauthorized Commands:**
    - Multiple unauthorized commands detected, originating from compromised SCADA control nodes.
- **Communication Disruptions:**
    - Intermittent communication failures between central control and remote turbines.

- **Data Integrity:**
    - Discrepancies in performance data logs, indicating potential tampering.

Potential Cascade Effects on Power Grid:

1. **Power Supply Disruptions:**
    - Fluctuations in power output causing instability in local grid.
    - Risk of brownouts or blackouts in affected regions.
2. **Equipment Damage:**
    - Over-speed conditions and erratic operations increasing wear and tear on turbines.
    - Potential for long-term damage to turbine components and reduced lifespan.
3. **Operational Impact:**
    - Increased maintenance and repair costs.
    - Downtime affecting overall energy production and revenue.

- .

Inject 5.1

Comprehensive Cybersecurity Audit Report

Date: [Insert Date]

Subject: Key Vulnerabilities in Smart Grid Infrastructure and Proposed Solutions

---

Overview:

This report presents the findings of the post-crisis cybersecurity audit, highlighting several long-standing vulnerabilities within NREC's smart grid infrastructure. These vulnerabilities require urgent attention to prevent potential exploitation, especially considering the recent sophisticated cyberattacks. The report also provides proposed solutions along with associated costs and operational implications.

Key Vulnerabilities:

1. **Legacy Systems:**
    - **Description:** Outdated software and hardware components that lack modern security features.
    - **Potential Impact:** Increased risk of unauthorized access, data breaches, and system failures.
    - **Proposed Solution:** Upgrade to current, secure systems.
    - **Operational Implications:** Temporary downtime during system upgrades, estimated at 48 hours.
2. **Insufficient Encryption:**
    - **Description:** Weak or non-existent encryption protocols for data in transit and at rest.
    - **Potential Impact:** Higher risk of data interception and unauthorized data access.
    - **Proposed Solution:** Implement end-to-end encryption for all data channels.
    - **Operational Implications:** Minor performance degradation during encryption deployment, no expected downtime.

3. **Access Control Weaknesses:**
    - **Description:** Inadequate access control measures and outdated user authentication processes.
    - **Potential Impact:** Unauthorized access to critical systems and sensitive data.
    - **Proposed Solution:** Implement multi-factor authentication and role-based access control.
    - **Operational Implications:** Training required for staff, minor disruption during implementation.
4. **Unpatched Vulnerabilities:**
    - **Description:** Known software vulnerabilities that have not been patched.
    - **Potential Impact:** Increased susceptibility to exploitation through known attack vectors.
    - **Proposed Solution:** Immediate patching of all identified vulnerabilities.
    - **Operational Implications:** Scheduled maintenance windows, possible brief system outages.
5. **Network Segmentation Issues:**
    - **Description:** Poor network segmentation allowing lateral movement within the network.
    - **Potential Impact:** Higher risk of widespread impact from a single point of compromise.
    - **Proposed Solution:** Redesign network architecture to enhance segmentation and isolation.
    - **Operational Implications:** Phased implementation over six months, with minimal disruption to operations.

Operational Implications:

- **Downtime:** Temporary system outages and performance impacts during upgrades and implementations.
- **Training:** Required for staff to adapt to new security measures and protocols.
- **Maintenance:** Increased scheduled maintenance to ensure continued security and functionality.

Nordic Pine Response Form (Your Team's Scenario-based Findings)

Stage Number:

Team Name:

Syndicate/Small Group Response:

- **Actions Taken:**
  - NN
  - NN

- **Outcome:**
  - NN
  - NN

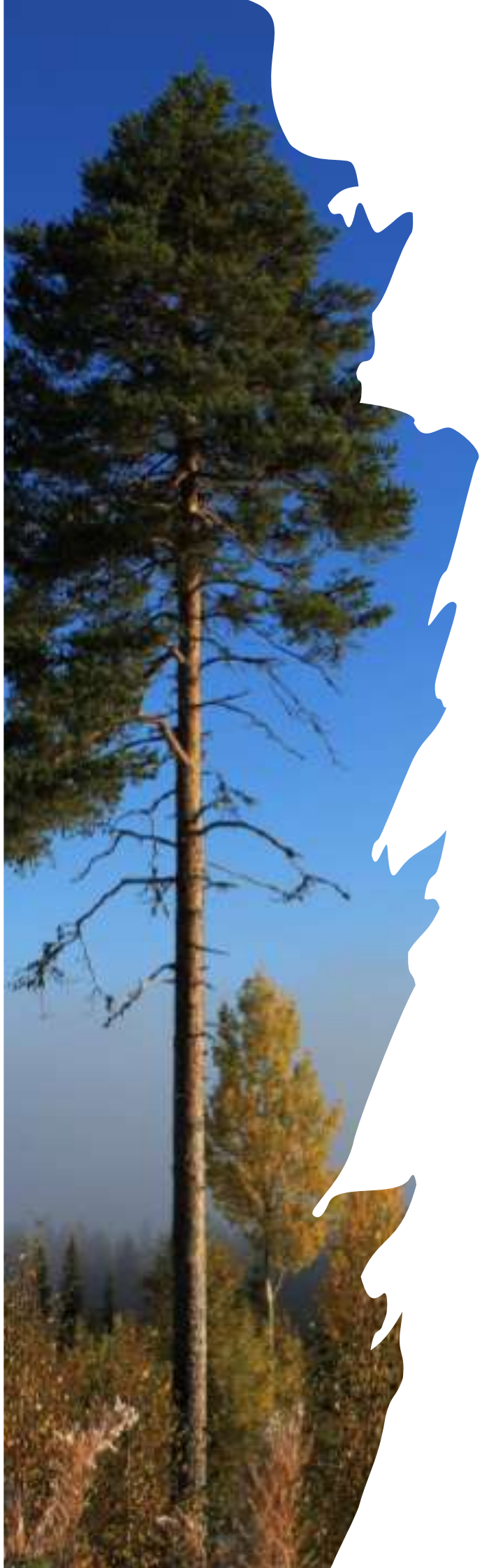
- **Challenges:**
  - NN
  - NN

Lessons Identified / Lessons Learned:

- **Was there a technological solution to this challenge?**
  - If yes, does your organization currently have this technology?
  - What future technology might you envision to address this challenge?

- **Reflections:**
  - NN
  - NN

- **Recommendations for Improvement:**
  - NN
  - NN



Tabletop Exercise (TTX)

Inject Responses, Day 1

Here is a synopsis of the Inject Response forms from the Nordic Pine 2024 TTX, day 1:

Overall Summary:

Common themes include proactive system isolation, thorough investigations, and strategic communication to counter misinformation. The teams also emphasized the importance of quality control, seeking alternative suppliers, and maintaining close dialogue with stakeholders.

Phase 1- Early Warning Signs

Inject 1.1: Cyber

- **Actions Taken:**
  - Ensured that all systems were updated and that firewalls were operational.
  - Investigated suspicious activities, such as specific logs and potential breaches.
  - Isolated the affected parts of the system and checked for vulnerabilities.
  - Shifted remote capabilities to manual operations where necessary.
  - Reported potential issues to cyber authorities and informed stakeholders, including the board and employees.
  - Conducted internal investigations, including checking physical security measures and security camera footage.
  - Ensured the integrity of backups and considered restoring from unbreached backup systems.
  - Implemented technical measures such as Zero Trust principles, user authentication, and improved phishing software.
  - Contacted neighboring companies and local defense forces for information and support.

Inject 1.2: Information

- **Actions Taken:**
  - Communicated scientific data and the truth via press conferences, social media, and company webpages.
  - Engaged with experts, local stakeholders (e.g., fishermen, environmental groups), and mainstream media.
  - Released counter-information and engaged with the local community.
  - Sought help from specialized consultants and industry organizations.
  - Tried to shut down bot accounts spreading misinformation.
  - Prepared for potential escalations, including coordinated attacks and increased public discontent.
  - Engaged with social media influencers and promised health studies to counter misinformation.
  - Centralized media communications with trained communicators and maintained a positive narrative.
  - Used trusted media outlets and prepared incident response plans.
  - Informed local authorities and prepared for potential physical threats and violence.

Inject 1.3: Supply Chain

- **Actions Taken:**

- Sought alternative suppliers and initiated in-house supplies and repairs.
- Audited the quality and checked contracts of current suppliers.
- Conducted thorough quality control of components and previous deliveries.
- Initiated legal actions regarding faulty quality in contracts and prepared to terminate contracts based on quality evidence.
- Maintained close dialogue with suppliers and activated alternative suppliers if available.
- Coordinated with third-party vendors to align cybersecurity protocols.
- Engaged with consortium companies and informed authorities about supply chain disruptions.
- Investigated supply disruptions and quality issues and sent research teams onsite if necessary.

Inject 1.4: Cyber (Continued)

- **Actions Taken:**
  - Addressed email filters and informed internal and external partners about phishing attempts.
  - Checked the integrity of backup systems.
  - Improved email spam filtering and provided spam training for company personnel.
  - Decided whether to block emails from specific companies and informed national cyber authorities.
  - Contacted the product management software company for immediate patches.

Inject 1.5: Information (Continued)

- **Actions Taken:**
  - Investigated affected equipment and engaged with the local community.
  - Went public stating that a third party was hired to investigate the cause.
  - Arranged regular meetings with local stakeholders, such as fishermen's unions.
  - Called national newspapers and local fishermen to discuss concerns.

Phase 2 - Escalation of Threats

Inject 2.1: Cyber

- **Actions Taken:**
  - Isolated the affected system and secured backups.
  - Conducted risk assessments of asset integrity and analysed the extent of breaches.
  - Ensured backup integrity and considered restoring from unbreeched backup systems.
  - Contacted the security operation centre and involved supplier experts for system analysis.
  - Developed patches for servers and improved phishing software.
  - Implemented Zero Trust principles and limited access.
  - Reported to authorities and informed stakeholders about the breach.

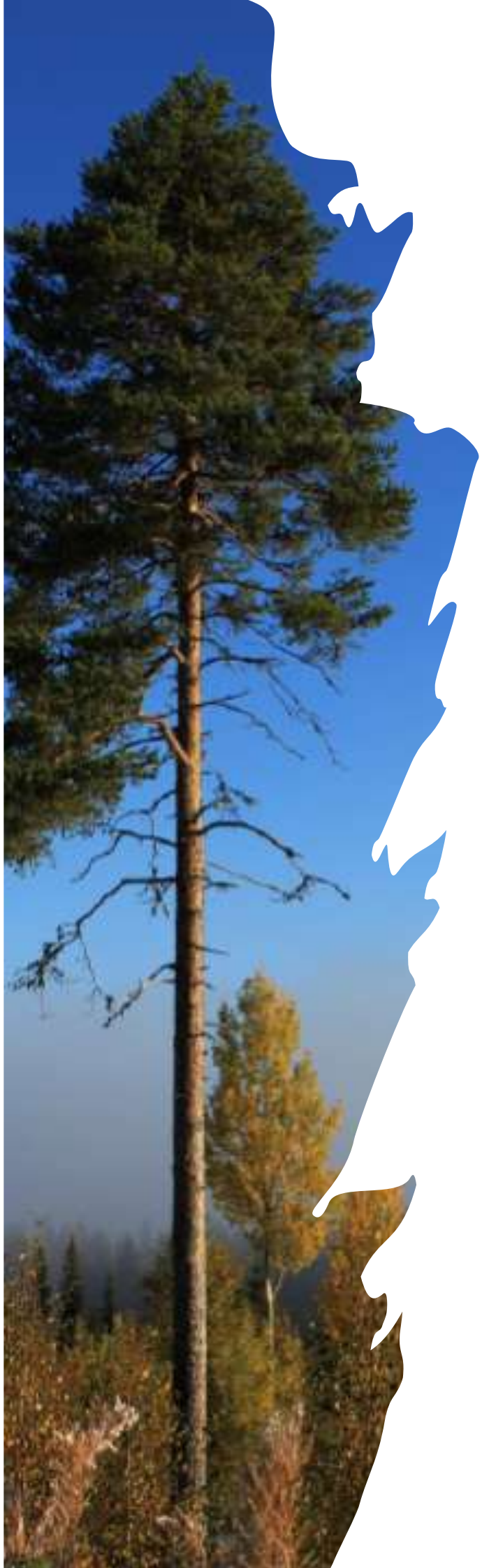
Inject 2.2: Information

- **Actions Taken:**
  - Communicated the truth and facts to counter fake news via press conferences, social media, and company webpages.

- Engaged with experts, politicians, and mainstream media.
- Promised health studies and analysed the data for coordinated disinformation campaigns.
- Outsourced communications and media monitoring temporarily.
- Prepared for potential physical threats and violence.
- Strengthened physical security and informed local authorities.
- Centralized media communications and used trusted media outlets.
- Maintained a positive narrative and strategic communications plan.

Inject 2.3: Supply Chain

- **Actions Taken:**
  - Sought alternative suppliers and initiated in-house supplies and repairs.
  - Conducted thorough quality control of components and monitored ownership changes.
  - Prepared to show evidence of quality issues to terminate contracts.
  - Initiated legal actions regarding faulty quality in contracts and prepared to switch vendors.
  - Maintained close dialogue with suppliers and informed authorities about supply chain disruptions.
  - Coordinated with consortium companies and informed embassies about supply chain issues.
  - Engaged with third-party vendors to align cybersecurity protocols.



Tabletop Exercise (TTX)

Inject Responses, Day 2

Here is a synopsis of the Inject Response forms from the Nordic Pine 2024 TTX, day 2:

Overall Summary:

The Nordic Pine 2024 Tabletop Exercise (TTX) involved a series of scenario-based injects designed to test the response capabilities of various teams to cyber, economic, and supply chain threats affecting wind turbine generators (WTGs) and related infrastructure. The exercise revealed several key actions taken, challenges faced, outcomes, and lessons learned across different stages. The teams focused on isolating affected systems, informing authorities, and improving security measures while managing public communication and stakeholder relations. The emphasis was on rapid incident response, collaboration with national security agencies, and ensuring business continuity.

Inject 2.4: Cyber

- **Actions Taken:**
  - Isolate affected WTGs and the entire wind farm if necessary.
  - Inform authorities and involve cyber security centres.
  - Investigate the extent of the infection using forensic experts.
  - Plan for system restoration and ensure other wind farms are not infected.
  - Contact specialists, manufacturers, and security operations centres.
  - Implement continuity plans and ensure backups and spare parts are available.
  - Manual operations for turbines if necessary.
- **Challenges:**
  - Ensuring the reliability of safety systems.
  - Handling sophisticated attacks potentially from nation-state actors.
- **Lessons Identified:**
  - The need for advanced monitoring of IT and OT networks.
  - Importance of having robust incident response and recovery plans.

Inject 2.5: Economic

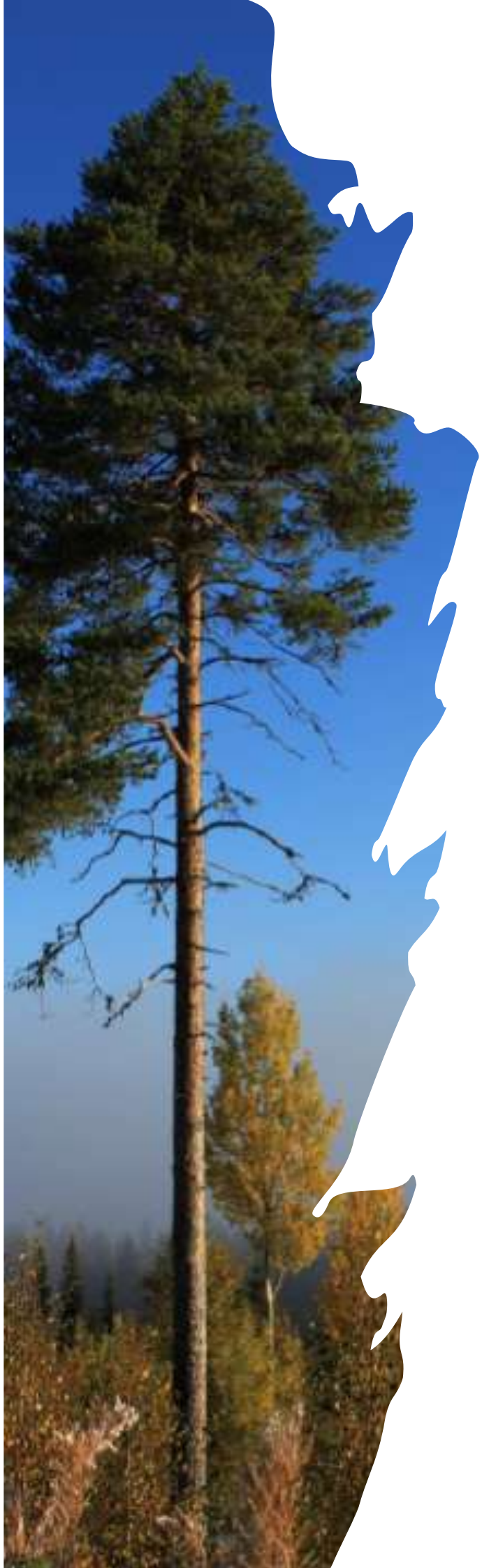
- **Actions Taken:**
  - Update spam filters and inform staff about phishing attempts.
  - Contact authorities and share confidential intelligence.
  - Inform stakeholders and the public about the situation.
  - Investigate and block phishing email senders.
  - Contact energy exchanges and national TSO´s to understand the broader impact.
  - Ensure the company is prepared for financial losses and has enough funding.
  - Act on disinformation by providing correct information through various channels.
  - Prepare internal and external communication plans.
- **Challenges:**
  - Addressing market manipulation and its broader implications.
  - Ensuring quick and effective communication within the company and with the public.
- **Lessons Identified:**
  - The need for preparedness against phishing attacks.
  - Establishing bilateral agreements and alternative partnerships to de-risk electricity trading.

Inject 3.1: Cyber

- **Actions Taken:**
  - Isolate the wind farm and shut down WTGs.
  - Run diagnostics on the wind farm and inform authorities.
  - Prepare for on-site support if remote operations are not feasible.
  - Activate crisis management and SCADA recovery plans.
  - Collaborate with national grids and authorities for shutdown procedures.
  - Use manual operations for turbines if SCADA is unreliable.
- **Challenges:**
  - Managing the crisis when it grows beyond the organization's capabilities.
  - Ensuring timely and coordinated response with national authorities.
- **Lessons Identified:**
  - Importance of having disaster recovery plans and robust backup systems.
  - Ensuring supplier disaster recovery plans are up to date.

Inject 3.2: Supply Chain

- **Actions Taken:**
  - Report to authorities and involve the coast guard.
  - Investigate the integrity of cables and ramp up physical security.
  - Collaborate with police, military, and national agencies for security.
  - Ensure continuous outreach with stakeholders and public communication.
  - Activate communication plans and involve environmental groups.
  - Request assistance for drones and submarines from military and defence forces.
- **Challenges:**
  - Handling physical security threats and the involvement of unmarked submarines.
  - Ensuring the availability of trained security personnel.
- **Lessons Identified:**
  - Necessity of formal verification of safety systems.
  - Importance of having clear policies on drone disruptors and submarine detection.



Tabletop Exercise (TTX)

Inject Responses, Day 3

Here is a synopsis of the Inject Response forms from the Nordic Pine 2024 TTX, day 3:

Overall Summary:

Inject 3.3: Information Response

Actions Taken:

- Educate the public and media about the deepfake video, showing the original to prove authenticity.
- Conduct press events to deny authenticity and state facts about the whistleblower emails.
- Use trusted media to report and explain the deepfake situation.
- Investigate access logs to identify potential insiders.
- Involve legal departments to ensure legal protection and address concerns.
- Publicly explain that the documents were stolen and manipulated, showing verification from the original company.

Inject 3.4: Cyber Response

Actions Taken:

- Contact internet service providers to block malicious traffic from DDoS attacks.
- Use backup communication channels and establish trusted third-party channels.
- Reset administrative accounts and require reauthentication.
- Implement a Zero Trust environment and least privilege access.
- Engage national cyber response teams and report to authorities.
- Enable DDoS protection and conduct log analysis of outbound communications.
- Use secure communication platforms like Signal and Rakel.

Inject 3.5: Supply Chain Response

Actions Taken:

- Contact original suppliers to ship via alternative routes.
- Engage legal teams to address concerns with customs officials.
- Work with national and EU foreign departments to resolve supply issues.
- Communicate openly with stakeholders and adjust project timelines.
- Increase cooperation with competing energy companies regarding supplies.
- Consider diplomatic pressure on countries holding up components.

Phase 4 and 5: Recovery, Mitigation, and Lessons Learned

Actions Taken:

- Secure project management systems and rectify technical specifications.
- Conduct public relations campaigns and establish secure emergency communication channels.
- Retrofit power plant systems and start studies on weak points.
- Involve specialists for focused crisis management and hire external evaluators.
- Return to remote operations for efficiency and establish remote data connections.
- Monitor for changes in the threat landscape and update contingency plans.
- Train personnel on their roles and conduct scenario analysis.
- Ensure secure IT configurations and conduct gap analysis on NIS 2.
- Build relationships with other companies and improve decision-making processes.

- Develop long-term resilience plans, including supply chain diversification and local supplier prioritization.

Outcome:

- Improved crisis management communication channels.
- Enhanced public understanding and trust.
- Increased resilience and preparedness for future threats.
- Stronger relationships with stakeholders, suppliers, and regulatory bodies.

Challenges:

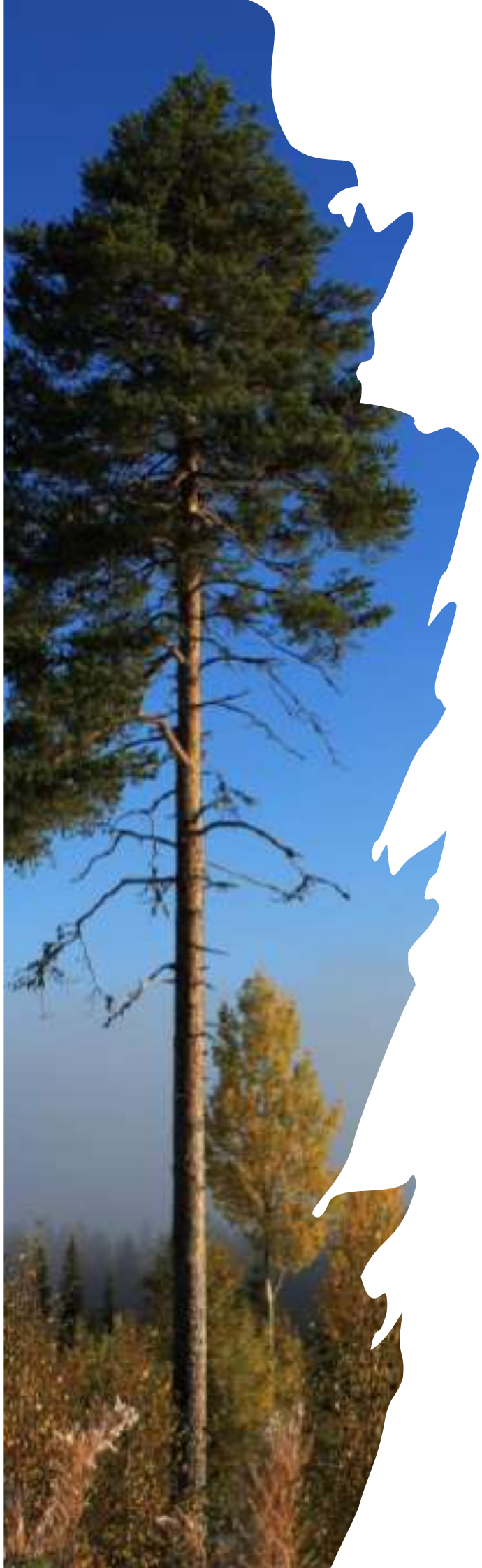
- Managing information and public perception without appearing to cover up issues.
- Addressing geopolitical restrictions and supply chain vulnerabilities.
- Ensuring enough resources and timely decision-making during crises.
- Balancing national security concerns with company priorities.

Reflections:

- External views on crisis management can help rebuild stakeholder trust.
- Preparation for future threats includes maintaining good public relations and securing supply chains.
- Financial resilience involves working with market operators and securing revenue streams.
- Securing human resources through partnerships with universities and joint research.

Recommendations for Improvement:

- Improve stakeholder communication and transparency.
- Continue to strengthen collaborations with competitors and authorities.
- Implement proactive measures for future crisis scenarios.
- Enhance public knowledge about renewable energy and environmental impacts.
- Regularly review and update contingency plans and crisis management strategies.



Tabletop Exercise (TTX)

Summary & Key Takeaways

Here is a synopsis of the Summery and Key Findings from the Nordic Pine 2024 TTX, day 1 -3.

Overall Summary:

This consolidated summary encapsulates the collective actions, reflections, and recommendations from the various teams' responses to the fictive scenario in the Nordic Pine 2024 TTX.

Actions Taken:

- Emphasized the importance of business continuity planning, including clear systems shutdown decision points.
- Considered the implementation of frameworks like ISO 27001 to make attacks more difficult.
- Conducted environmental studies and established clear communication plans.
- Implemented risk-based decision-making models.
- Focused on supplier requirements, management, and audits.
- Ensured the organization rehearsed continuance plans and risk assessments, periodically reviewing them.
- Identified critical suppliers and established supply chain backups.
- Secured contracts and contacts for external experts beforehand.
- Promoted information sharing and collaboration between energy companies and authorities.
- Clarified the chain of command and established single points of contact for different areas.
- Engaged national cyber response teams, enabled DDoS protection, and conducted log analysis of outbound communications.
- Used backup communication channels and secure communication platforms.

Outcome:

- Improved crisis management communication channels.
- Enhanced public understanding and trust.
- Increased resilience and preparedness for future threats.
- Stronger relationships with stakeholders, suppliers, and regulatory bodies.

Challenges:

- Managing information and public perception without appearing to cover up issues.
- Addressing geopolitical restrictions and supply chain vulnerabilities.
- Ensuring enough resources and timely decision-making during crises.
- Balancing national security concerns with company priorities.
- Gathering comprehensive information and recognizing crises early.
- Clarifying authority and communication pathways during incidents.

Lessons Identified / Lessons Learned:

- Questioned the availability and implementation of technological solutions to challenges.
- Explored future technological solutions.
- Emphasized the importance of making or updating contingency plans and practicing them.
- Highlighted the need to spread information about contingency planning and renewable energy infrastructure.
- Increased knowledge of NATO's 7 baseline requirements and the importance of renewable energy.
- Recognized the complexity of cooperation on many levels, including company collaboration, competition, and national and international security aspects.
- Identified the value of Tabletop Exercises (TTX) and the need for agility in response plans.
- Acknowledged the importance of clear reporting pathways and establishing a single point of contact on a national level.

Reflections:

- External views on crisis management can help rebuild stakeholder trust.
- Preparation for future threats includes maintaining good public relations and securing supply chains.
- Financial resilience involves working with market operators and securing revenue streams.
- Securing human resources through partnerships with universities and joint research.
- Recognized the need for clarity on managing risks at national and regulatory levels.
- Emphasized the importance of TTX and strategic foresight.

Recommendations for Improvement:

- Improve stakeholder communication and transparency.
- Continue to strengthen collaborations with competitors and authorities.
- Implement proactive measures for future crisis scenarios.
- Enhance public knowledge about renewable energy and environmental impacts.
- Regularly review and update contingency plans and crisis management strategies.
- Bring scenarios for training purposes and ensure the right team composition.
- Ensure that legal, communication, and cybersecurity departments know their responsibilities.
- Discuss how to elevate issues to a cross-company or cross-country level and move from words to action.