CYBER 9/12 STRATEGY CHALLENGE
Atlantic Council
25 YEARS GCSP Geneva Centre for Security Policy

2020 Cyber 9/12 Strategy Challenge

Intelligence Report I

Competition Instructions

Your team will take on the role of experienced cyber policy experts invited to brief the Political and Security Committee of the European Union which has been called to address an evolving cyber crisis. **For the purposes of this exercise**, the Political and Security Committee is made up of European leaders (including heads of state, heads of government, ministers of defence and foreign affairs, directors of intelligence services, and representatives from the private sector).[1]

This briefing document contains fictional information on the background and current situation involving a major cyber incident affecting critical infrastructure and services in Europe. The incident notionally takes place in May and June 2021. The scenario presents a fictional account of political developments and both public and private reports on the cyber incident.

The parties to this fictional cyber incident are:

- The fictional state of the Republic of Nistria;
- The fictional state of the Federal Republic of Mustelus;
- The European Union.

<u>The Republic of Nistria</u>

The Republic of Nistria is a fictional northern European state on the Eastern border of the EU. It has a highly developed digital commerce industry and society has accepted e-governance without issue. Its primary industrial base, however, is energy production. The state-owned energy company, NisPower, maintains a monopoly on energy production in the country resulting in low energy costs for its citizens.

Until 2010, Nistria was the 12th federal state of Mustelus. It gained independence following a fiercely fought, highly politicised and highly emotive referendum. At the time and since the referendum, much of the anti-independence movement stemmed from ethnic Mustelans living in Nistria. In addition, Nistria also has large deposits of natural resources and the Mustelan government wished to maintain control of these assets.

Since gaining independence, Nistria has become the 28th member of the EU, further antagonising their Mustelan neighbours. Nistria takes an active role in EU politics but has found itself the subject of antitrust investigations given its state-owned energy company –

[1] The Political and Security Committee in reality is made up of EU Ambassadors representing their countries. More information can be found here https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/political-security-committee/

NisPower – is taking advantage of EU economic regimes and is operating as a private company in several European countries. It has purchased energy production and supply companies and expanded its facilities to include gas supply, electricity production and several nuclear reactors.

On 14th May 2021 NisPower executed a planned upgrade of its SCADA and computer network systems. The objective was to bring all its entities – state-owned and private – into a single unified computer network with full control abilities from its home network in Nistropolis, the Nistrian capital city. The upgrade failed with catastrophic consequences. NisPower requested additional assistance from an external cyber forensics company, the fictional CyberSec Systems Inc, who carried out an examination of the network failures, reporting its findings on the 28th May.

The Federal Republic of Mustelus

The second fictional state is the Federal Republic of Mustelus. This is a federal country made up of 11 states. Unlike Nistria, Mustelus is NOT a member of the European Union.

Mustelus has a highly developed economy focused around its vast natural resources, particularly oil and gas. Due to its Baltic coastline, Mustelus maintains a substantial naval presence and has a large merchant fleet for exporting its raw commodities, particularly for the energy industry. Mustelus is also a digitised society and boasts a highly developed computer games industry with a particular speciality being MMPORGs

Although the Mustelan government lost the referendum on Nistrian independence in 2010, it has pushed for reunification. It seeks to exercise influence over Nistrian politics through various means, including economic and customs unions, trade and commodities agreements and speaking directly to the Mustelan diaspora in Nistria.

Some of the most popular computer games are MMPORGs with the strategic goal of reunification of separatist entities. There have also been unsubstantiated allegations of Mustelan government entities fomenting unrest in this diaspora community. This routinely occurs annually during Mustelan National Day celebrations on the 8th May.

The European Union

In the universe in which this exercise is situated, the EU is a union of 28 member states, with the Republic of Nistria being the newest, 28th member. The EU's security crisis policy and strategy are directed by the Political and Security Committee.

The Political and Security Committee of the EU

The Political and Security Committee (PSC), is a body of the *Council of the European Union*. As such it upholds a consensus-based approach amongst member state representatives to devise pan-European responses to potential crises.

The PSC is responsible for the EU's Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP). The Committee therefore actively:

- monitors the international situation;
- recommends strategic approaches and policy options to the Council;
- provides guidance to EU crisis entities such as the Committee for Civilian Aspects of Crisis Management (CIVCOM), the European Union Military Committee (EUMC), the European Union Institute for Security Studies (EUISS);
- and ensures political control and strategic direction of crisis management operations.

The PSC meets at least twice a week to keep track of the international situation. In a crisis, the PSC can hold significant authority. The Council may authorise decision-making capabilities to the Committee throughout the duration of a crisis management operation. One of the ways the PSC can exercise this authority is to adopt EU Decisions under the CFSP framework. EU Decisions are a specific type of EU legislation which are only binding on the specific Member State or entity to which they refer.

In the universe of the 2020 Cyber 9/12 Strategy Challenge, the Council has authorised the PSC to choose a course of action on behalf of the EU to ensure the EU's security. In addition, f*or the purposes of the 2020 Cyber 9/12 Strategy Challenge in Geneva, the PSC is made up of heads of state and government, as well as subject matter experts, whereas in reality the PSC meets at the EU-ambassador level. All other political and security concerns reflect the EU's actual, real-life situation.*

The Exercise

Your team needs to provide information on the full range of policy response alternatives available to respond to this crisis, and has been tasked to develop 2-4 policy recommendations to present to the task force. You are to consider as facts the following pages in formulating your response.

You will use the fictional scenario material presented to perform three tasks:

1. **Written Policy Brief:** Write a 500-word brief discussing the key elements and security concerns that the task force must understand. The written task is meant to not only test your team's ability to summarise the scenario, but more importantly to explain the reasons and confidence levels behind your analysis of the key issues and implications of the ongoing cyber incident.
2. **Oral Policy Brief:** Prepare a ten-minute oral presentation outlining possible policy options and recommending one to the task force.
3. **Decision Document:** Teams will also be required to submit a "decision document" accompanying their oral presentation at the beginning of the competition round. The "decision document" will be maximum one page outlining the team´s policy response options, decision process, and recommendations. The teams should note that the document is not intended to summarise every detail of the recommendations, but to help the judges follow the oral presentation. Judges will be given only 2 minutes to read the document before the presentation begins.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- **Don't fight the scenario**. Assume all scenario information presented is possible, observed, or reported as written. Use your energy to explore the implications of that information, not the plausibility.
- **Think multi-dimensionally**. When analysing the scenario, remember to consider implications for other organisations and domains (e.g. private sector, military, law enforcement, information operations, diplomatic, etc.) and incorporate these insights along with cyber security.
- **Be creative**. Cyber policy is an evolving discourse, and there is no single correct policy response option to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- **Analyse the issues**. The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various official publications from entities such as the European Union or derived from original news sources while others have been invented by the authors. All scenario content is intended for academic, simulation purposes and is not meant to represent the views of the competition organisers, authors, or any affiliated or named organisation, actual or fictional.

Briefing

From: The Political and Security Committee of the European Union

Re: Escalating disruption to pan-EU energy and electricity supply following failed NisPower IT Upgrade

Date: June 2nd, 2021

The Political and Security Committee of the European Union has established an international and multi-stakeholder task force and is contacting your team to solicit policy solutions to respond to an evolving cyber incident. The Task Force is made up of national security advisors from the governments of European countries, representatives from European Union security and foreign policy agencies and as well as private-sector representatives.

Given the nature of this cyber incident, this group of European leaders wants to assemble a range of possible policy response alternatives before determining a course of action to announce in the next task force meeting at **8:00am on 2 July 2021**. Your oral policy brief recommendations must analyse the possible strengths, weaknesses, opportunities and threats of each proposed policy response alternative before recommending the one best course of action. To do so, you will apply your understanding of cyber security, national and international law, foreign policy, and security theory to synthesise useful policy measures from limited information.

When generating each of your policy response alternatives, the task force requests that you consider the following potentially conflicting interests at the national, EU and NATO level. These are provided as suggested starting points and are not meant to limit your policy responses.

Immediate Response vs. Delayed Response
What actions should be considered, if any, if there exists the possibility of European agencies' involvement? What actions should to be taken immediately after the incident versus those that should be taken later?

Government Response vs. Private-Sector Response
What actions should be led by the private sector in response to the reports and incidents and what actions should be under government leadership? Actions to consider may include public acknowledgements, preventive and pre-emptive defensive actions, and offensive actions.

Unilateral Response vs. Multilateral Response
Should there be a unilateral or multilateral response within Europe? What about international organisations like the United Nations or NATO?

Direct Response vs. Indirect Response
If action is to be taken, should it be a direct or indirect response to the incident? Should those responding act in secret, or reveal their cyber capabilities? Should no action be taken?

Additionally, this message is accompanied by several documents that may assist your team in preparing its policy response alternative recommendations for the task force:

Appendix 1- Recommendation from the European Commission on cyber security in the energy sector

Appendix 2- Internal memo from CyberSec Systems digital forensics teams examining NisPower's failed IT upgrade

Appendix 3- Email chain between the Chair of NisPower's Board and the Nistrian Deputy Prime Minister

Appendix 4- News report regarding pro-Mustelan nationalist protests

Appendix 5- Twitter exchange regarding pro-Mustelan protests

Appendix 6- European Commission Press Release stating NisPower is subject to an antitrust investigation from EU competition regulators.

Appendix 1[2]

European
Commission

Brussels, 3.4.2019
C (2019) 2400 final

COMMISSION RECOMMENDATION

Of 3.4.2019

on cybersecurity in the energy sector

{SWD(2019) 1240 final}

[2] Source for this recommendation can be found here https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

COMMISSION RECOMMENDATION

of 3.4.2019

on cybersecurity in the energy sector

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

(1) The European energy sector is undergoing an important change towards a decarbonised economy, while ensuring security of supply and competitiveness. As part of that energy transition and the related decentralisation of power generation from renewable sources, technological progress, sector coupling, and digitalisation are turning Europe's power grid into a "smart grid". At the same time, this also brings new risks as digitalisation increasingly exposes the energy system to cyberattacks and incidents which may jeopardize the security of energy supply.

(2) The adoption of all eight legislative proposals[3] of the 'Clean Energy for all Europeans' Package including the Energy Union Governance as stepping stone, allows to create a favourable environment for the digital transformation of the energy sector. It also acknowledges the importance of cybersecurity in the energy sector. In particular, the recast of the Regulation on the Internal Market for Electricity[4] provides for the adoption of technical rules for electricity such as a Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, on common minimum requirements, planning, monitoring, reporting and crisis management. The Regulation on Electricity Risk Preparedness[5] broadly follows the approach chosen in the Regulation on Security of Gas Supply[6]; stressing the need to properly assess all risks, including those related to cybersecurity, and proposing to adopt measures to prevent and mitigate those identified risks.

(3) When the Commission adopted the EU Cybersecurity Strategy[7] in 2013, it identified strengthening the Union's cyber-resilience as a priority. One of the key deliverables of the Strategy is the Directive on Security of Network and Information Systems[8] (hereafter, the "NIS

[3] Directive (EU) 2018/2001; Directive (EU) 2018/2002; Regulation (EU) 2018/1999; Directive (EU) 2018/844. The European Parliament confirmed the political agreements reached with the Council on Electricity Market Design proposals (Risk-Preparedness Regulation, Regulation for the Agency for the Cooperation of Energy Regulators (ACER) and the Electricity Directive and the Electricity Regulation at the plenary session of March 2019. The Council formal adoption is expected to take place in April; the publication of the legal text in the OJ will follow soon thereafter.

[4] COM/2016/0861

[5] COM/2016/0862

[6] Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply, OJ L 280, 28.10.2017, p. 1.

[7] JOIN(2013) 1

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1.

Directive"), which was adopted in July 2016. As the first piece of horizontal EU legislation on cybersecurity, the NIS Directive boosts the overall level of cybersecurity in the Union through the development of national cybersecurity capabilities, the increase of EU- level cooperation and the introduction of security and incident reporting obligations for companies referred to as 'operators of essential services'. Incident reporting is mandatory in key sectors, including the energy sector.

(4) When implementing preparedness measures in cybersecurity, the relevant stakeholders, including operators of essential services in energy as identified under the NIS Directive, should take into account the horizontal guidance issued by the NIS Cooperation Group established under Article 11 of the NIS Directive. That Cooperation Group, which is composed of representatives of Member States, the European Agency for Cybersecurity (ENISA) and the Commission, has adopted guidance documents concerning security measures and incident notification. In June 2018, that Group created a dedicated work stream on energy.

(5) The 2017 Joint Communication on Cybersecurity[9] acknowledges the importance of sector specific considerations and requirements at EU level, including in the energy sector. Cybersecurity and possible policy implications have been the subject of a comprehensive discussion process in the Union over the recent years. Consequently, there is rising awareness today that individual economic sectors face specific cybersecurity issues and, therefore, need to develop their own sectoral approaches in the wider context of general cybersecurity strategies.

(6) Information sharing and trust are key elements in cybersecurity. The Commission aims to increase the sharing of information among the relevant stakeholders by organising dedicated events, as for examples, the high-level roundtable on cybersecurity in energy organised in Rome in March 2017 and the high-level conference on cybersecurity in energy organised in Brussels in October 2018. The Commission also wants to enhance the cooperation between relevant stakeholders and specialised entities such as the European Energy Information Sharing and Analysis Centre.

(7) The Regulation on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act Regulation[10]") will strengthen the mandate of the EU Agency for Cybersecurity so as to better support Member States in tackling cybersecurity threats and attacks. It also creates a European cybersecurity framework for the certification of products, processes and services that will be valid throughout the Union and is of particular interest for the energy sector.

(8) The Commission has put forward a Recommendation[11] addressing cybersecurity risks in the 5th generation (5G) of network technologies by setting out guidance on appropriate risk analysis and management measures at national level, on developing a coordinated European risk analysis and on establishing a process to develop a common toolbox of best risk management measures. Once rolled out, 5G networks will form the backbone for a wide range of services essential for the functioning of the internal market and operation of vital societal and economic functions such as energy.

(9) This Recommendation should provide non-exhaustive guidance to Member States and relevant stakeholders, in particular network operators and technology suppliers, for achieving

[9] JOIN(2017) 450

[10] The Cybersecurity Act was adopted by the European Parliament in March 2019. The Council formal adoption is expected to take place in April; the publication of the legal text in the OJ will follow soon thereafter.

[11] C(2019)2335

a higher level of cybersecurity in view of the specific real-time requirements identified for the energy sector, cascading effects and the combination of legacy and state-of-the-art technologies. This guidance aims at helping stakeholders keep in mind the specific requirements of the energy sector when implementing internationally recognised cybersecurity standards[12].

(10) The Commission intends to regularly review this Recommendation based on the progress made across the Union in consultation with Member States and relevant stakeholders. The Commission will continue its efforts to strengthen cybersecurity in the energy sector, notably through the NIS Cooperation Group, which ensures strategic cooperation and exchange of information among Member States in cybersecurity.

(11) The Commission recognises the vulnerability of the energy sector to interference from non-EU state actors seeking to disrupt energy supply. However, given that EU citizens are the ultimate end-users of energy supply, care should also be taken to mitigate the potential impact of criminal entities, internal to the EU or external, on an uninterrupted energy supply.

HAS ADOPTED THIS RECOMMENDATION:

SUBJECT MATTER

(1) This Recommendation sets out the main issues related to cybersecurity in the energy sector, namely real-time requirements, cascading effects and combination of legacy and state-of-the-art technology and identifies the main actions for implementing relevant cybersecurity preparedness measures in the energy sector.

(2) In applying this Recommendation, Member States should encourage the relevant stakeholders to build up knowledge and skills related to cybersecurity in the energy sector. Where appropriate, Member States should also include these considerations into their national cybersecurity framework, notably through strategies, laws, regulations and other administrative provisions.

REAL-TIME REQUIREMENTS OF ENERGY INFRASTRUCTURE COMPONENTS

(3) Member States should ensure that the relevant stakeholders, notably energy network operators and technology suppliers, and in particular operators of essential services identified under the NIS Directive, implement the relevant cybersecurity preparedness measures related to real-time requirements in the energy sector. Some elements of the energy system need to work under "real time", that is to say reacting to commands within a few milliseconds, which makes it difficult or even impossible to introduce cybersecurity measures due to a lack of time.

(4) In particular, energy network operators should:

[12] International Standardisation Organisations have published various cybersecurity (ISO/IEC 27000: Information Technologies) and risk management standards (ISO/IEC31000: Implementation of risk management). A specific standard for the energy sector (ISO/IEC 27019: Information security controls for the energy utility industry) was issued as part of the ISO/IEC 27000 series in October 2017.

(a) apply the most recent security standards for new installations wherever adequate and consider complementary physical security measures where the installed base of old installations cannot be sufficiently protected by cybersecurity mechanisms;

(b) implement international standards on cybersecurity and adequate specific technical standards for secure real-time communication as soon as respective products become commercially available;

(c) consider real-time constraints in the overall security concept for assets, especially in asset classification;

(d) consider privately owned networks for tele-protection schemes to ensure the quality of service level required for real-time constraints; when using public communication networks, operators should consider ensuring specific bandwidth allocation, latency requirements and communication security measures;

(e) split the overall system into logical zones and within each zone, define time and process constraints in order to enable the application of suitable cybersecurity measures or to consider alternative protection methods.

(5) Where available, energy network operators should also:

(a) choose a secure communication protocol, taking into consideration real-time requirements, for example between an installation and its management systems (Energy Management System – EMS / Distribution Management System - DMS);

(b) introduce an appropriate authentication mechanism for machine-to-machine communication, addressing real-time requirements.

CASCADING EFFECTS

(6) Member States should ensure that the relevant stakeholders, notably energy network operators and technology suppliers, and in particular operators of essential services identified under the NIS Directive, implement the relevant cybersecurity preparedness measures related to cascading effects in the energy sector. Electricity grids and gas pipelines are strongly interconnected across Europe and a cyber-attack creating an outage or disruption in a part of the energy system might trigger far-reaching cascading effects into other parts of that system.

(7) In applying this Recommendation, Member States should evaluate the interdependencies and criticality of power generation and flexible-demand systems, transmission and distribution substations and lines, and the associated impacted stakeholders (including cross-border situations) in case of a successful cyber-attack or cyber incident. Member States should also ensure that energy network operators have a communication framework with all key stakeholders to share early warning signs and cooperate on crisis management. There should be structured communication channels and agreed formats in place in order to share sensitive information with all relevant stakeholders, Computer Security Incident Response Teams, and relevant authorities.

(8) In particular, energy network operators should:

(a) ensure that new devices, including Internet of Things devices, have and will maintain a level of cybersecurity appropriate to a site's criticality;

(b) adequately consider cyber-physical effects when establishing and periodically reviewing business continuity plans;

(c) establish design criteria and an architecture for a resilient grid, which could be achieved by:

- putting in place in-depth defence measures per site, tailored to a site's criticality;
- identifying critical nodes, both in terms of power production capacity and customer impact; Critical functions of a grid should be designed to mitigate risk that can cause cascading effects by considering redundancy, resilience to phase oscillations and protections against cascaded load cut-off;
- collaborating with other relevant operators and with technology suppliers to prevent cascading effects by applying appropriate measures and services;
- designing and building communication and control networks with a view to confining the effects of any physical and logical failures to limited parts of the networks and to ensuring adequate and swift mitigation measures.

LEGACY AND STATE-OF-THE-ART TECHNOLOGY

(9) Member States should ensure that the relevant stakeholders, notably energy network operators and technology suppliers, and in particular operators of essential services identified under the NIS Directive, implement the relevant cybersecurity preparedness measures related to the combination of legacy and state-of-the-art technology in the energy sector. Indeed, two different types of technologies co-exist in today’s energy system: an older technology with a lifespan of 30 to 60 years, designed before cybersecurity considerations, and modern equipment, reflecting state-of-the-art digitalisation and smart devices.

(10) In applying this Recommendation, Member States should encourage energy network operators and technology suppliers to follow the relevant internationally accepted standards on cybersecurity wherever possible. Meanwhile, stakeholders and customers should adopt a cybersecurity-oriented approach when connecting devices to the grid.

(11) In particular, technology suppliers should provide tested solutions for security issues in legacy or new technologies free of charge and as soon as a relevant security issue becomes known.

(12) In particular, energy network operators should:

(a) analyse the risks of connecting legacy and Internet of Things concepts and be aware about internal and external interfaces and their vulnerabilities;

(b) take suitable measures against malicious attacks originating from large numbers of maliciously controlled consumer devices or applications;

(c) establish an automated monitoring and analysis capability for security-related events in legacy and Internet of Things environments, such as unsuccessful attempts to log-in, door alarms for cabinet opening or other events.

(d) conduct on a regular basis specific cybersecurity risk analysis on all legacy installations, especially when connecting old and new technologies; since the legacy installations often represent a very large number of assets, risk analysis might be done by asset classes;

(e) update software and hardware of legacy and Internet of Things systems to the most recent version whenever adequate; in so doing, energy network operators should consider complementary measures such as system segregation or adding external security barriers where patching or updating would be adequate but is not possible, for instance unsupported products;

(f) formulate tenders with cybersecurity in mind, that is to say demand information about security features, demand compliance with existing cybersecurity standards, ensure continuous alerting, patching and mitigation proposals if vulnerabilities are discovered, and clarify vendor liability in the event of cyber-attacks or incidents;

(g) collaborate with technology suppliers to replace legacy systems whenever beneficial for security reasons but take into account critical system functionalities.

MONITORING

(13) Member States should communicate to the Commission, within 12 months after the adoption of this Recommendation, and every two years thereafter, detailed information regarding the state of implementation of this Recommendation through the NIS Cooperation Group.

REVIEW

(14) On the basis of the information submitted by the Member States, the Commission will review the implementation of this Recommendation and assess whether further measures are required as appropriate in consultation with the Member States and the relevant stakeholders.

ADDRESSEES

(15) This Recommendation is addressed to the Member States.

Done at Brussels, 3.4.2019

Appendix 2[13]

CyberSec Systems

Memo

To: Jaime Tomsoni – Chairman of the Board, NisPower
From: Dr. Victoire Baezner
cc: Augustine Bonfantini, Deputy Prime Minister, Republic of Nistria
Date: May 28, 2021
Re: Digital Forensic Examination of NisPower Network Update Failure

CONFIDENTIAL REPORT TO NISPOWER EXECUTIVES

Report from CyberSec Systems on issues relating to the planned upgrade and consolidation of NisPower computer networks and SCADA systems

Investigator	**CyberSec Systems Inc.**
	HQ: 1 Cyber Lane
	Berkley, CA USA
Digital Forensics Examiner	**Dr. Victoire Baezner**
	CISO CyberSec Systems
	Badge # 2548
Subject	**NisPower Ltd**
	1 Power Lane
	Nistropolis
Subject Entity	**State-owned energy monopoly**

CyberSec Systems Inc.

CyberSec Systems Inc. is a specialist network security and digital forensics company based in the United States. It specialises in providing support to entities operating in the critical and industrial infrastructure sector. Its USP is that it provides holistic situation reports examining

[13] Although this report is ENTIRELY FICTIONAL elements of it have been drawn from an original report by Symantec. The original source can be found here https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

the totality of an incident including physical impacts, in addition to its highly advanced digital forensic analysis.

Case Background

NisPower is a large state-owned electricity and energy production and distribution company, headquartered in Nistropolis, the capital city of the Republic of Nistria. Although it is wholly owned by the Nistrian government, it operates as a private-sector company in a number of European states. It has a acquired a substantial number of private-sector energy companies across the EU. These private-sector subsidiaries and satellite entities operate energy production sites including renewables, gas- and coal-fired power stations and nuclear facilities.

NisPower executives planned to upgrade and update the computer and supervisory control and data acquisition (SCADA) systems across its entire network – the Nistrian home network and those of its subsidiaries outside Nistria. A number of these subsidiaries operated using decades-old computer systems and legacy networks which were in urgent need of upgrade, not only to be compliant with EU regulations on energy systems, but also to avoid the possibility of catastrophic failure.

The objectives of the update were:

- To upgrade the legacy systems of NisPower's private-sector acquisitions to ensure compliance with EU regulation. A number of systems, including backup and redundancy networks, had not been maintained or updated for several years;
- To create a more resilient system of SCADA networks to avoid cascading failures and maintain energy production and distribution across Nistria and the EU;
- Streamline computer network and SCADA oversight;
- Reduce its security landscape;
- Increase network efficiency;
- To create a single global NisPower network and consolidate SCADA and network oversight processes to create a central commercial entity based at the parent company in Nistropolis.

The upgrade and network consolidation were carefully planned over a period of several months with CISO and CEO involvement. It took place at midnight on May 14, 2021.

By 3:00am on May 15th systems engineers overseeing the consolidation noticed several errors in the home network, as well as acquired satellite and legacy systems going offline.

By 6:00am on May 15th it was clear that a major catastrophic failure had occurred:

- Connections had been lost to three of the five nuclear power stations in France;
  - Backup systems are temporarily operational for a maximum of 12 hours;
- Connections were lost to gas supplies bringing in fuel from Eastern Europe including
  - Pipeline distribution centres;
  - Gas storage facilities and strategic nodes.
- Telephone lines were not functioning due to the switch from copper lines to VOIP in most European countries. Technicians were relying on mobile networks;
- Commands from the central hub in Nistropolis were not being received in former legacy systems.

For several days NisPower systems engineers attempted to restore the network but were unable to do so. When intermittent contact with the satellite systems was finally restored, local engineers informed NisPower engineers in Nistropolis that the systems were not only disconnected from the parent network but had in some cases shut down.

The consequence of this was that some energy distribution facilities were operating on backup redundant systems which had not been upgraded in several years and were reaching critical levels. Systems in Polish, French and Belgian subsidiaries were required to be shut down, and have subsequently failed to restart. In other cases, the redundancy systems failed to initiate, or the primary networks were not able to switch to the redundancies. NisPower computer engineers have been unable to identify a logical reason for this.

Following the failure, on May 21st NisPower executives reached out to CyberSec Systems to conduct a thorough forensic examination of its networks to identify any root cause.

Analysis

Following examination, efforts to remedy network failures and return NisPower to a full-supply situation are being hampered by two primary non-ICT issues.

1. The complexities of operating in a multi-entity and multinational commercial environment. In Nistria, NisPower is a public entity wholly owned by the Government of Nistria. In the wider European Union, however, NisPower operates as a private-sector entity, holding several commercial subsidiaries. This complex network of public and private entities supporting the critical infrastructure of the EU member states creates additional political issues as well as practical problems in ensuring continuous energy supply;
2. Most of NisPower's storage nodes have been built in remote locations to save land-purchase costs. Several of these areas have little to no cellular phone coverage which is hampering efforts to communicate given that the VOIP systems, which are linked to NisPower's computer network, have also failed.

ICT Analysis

Malware detection

Dr Baezner identified the presence of a malware family, **FriendlyPixie,** within the unified NisPower network (home and satellite).

FriendlyPixie exploited a 0-day vulnerability in win32k.sys, used for local privilege escalation. The vulnerability resides in code that calls a function in a function pointer table; however, the index into the table is not validated properly, allowing code to be called outside of the function table.

The installation routine in Export 15, extracts and executes Resource 250, which contains a DLL that invokes the local privilege escalation exploit. The DLL contains a single export—Tml_1. The code first verifies that the execution environment isn't a 64-bit system and is Windows XP or Windows 2000.

If the snsm7551.tmp file exists execution ceases, otherwise the file ~DF540C.tmp is created, which provides an in-work marker.

Next, win32k.sys is loaded into memory and the vulnerable function table pointer is found. FriendlyPixie will then examine the DWORDs that come after the function table to find a suitable DWORD to overload as a virtual address that will be called. When passing in an overly large index into the function table, execution will transfer to code residing at one of the DWORDs after the function table. These DWORDs are just data used elsewhere in win32k.sys, but hijacked by FriendlyPixie. For example, if the ASCII string ‘aaaa’ (DWORD 0x60606060) is located after the function table, FriendlyPixie will allocate shellcode at address 0x60606060 and then pass in an overly large function table index that points to the DWORD ‘aaaa’ (0x60606060).

Because the available space at the address (in the above example 0x60606060) may be limited, FriendlyPixie uses a two-stage shellcode strategy. Memory is allocated for the main shellcode and at the chosen hijacked address, FriendlyPixie places only a small piece of shellcode that will jump to the main shellcode.

Next, FriendlyPixie drops a malformed keyboard layout file into the Temp directory with the file name ~DF<random>. tmp. The malformed keyboard layout file contains a byte that will result in the overly large index into the function table. NtUserLoadKeyboardLayoutEx is called to load the malformed keyboard layout file successfully invoking the exploit. The original keyboard layout is restored and then the malformed keyboard layout file is deleted.

The shellcode then loads the main FriendlyPixie DLL in the context of CSRSS.EXE.

Load Point

FriendlyPixie drops Resource 242 MrxCls.sys via Export 16. MrxCls is a driver digitally signed with a compromised Realtek certificate that was revoked on July 16, 2008 by Trusign. A different version of the driver was also found signed by a different compromised digital certificate from ZMicrox.

Mrxcls.sys is a driver that allows FriendlyPixie to be executed every time an infected system boots and thus acts as the main load-point for the threat. The driver is registered as a boot start service creating the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\”ImagePath” = “%System%\drivers\mrxcls.sys” and thus loading early in the Windows boot process.

The goal of the driver is to inject and execute copies of FriendlyPixie into specific processes.

The driver contains an encrypted data block. After decryption, this block contains (among others) a registry key/ value pair, which is normally HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MrxCls\“Data”.

The driver reads this binary value (previously set by FriendlyPixie during the installation process). The value is decrypted. It contains a list of pairs (target process name, module to inject):

- services.exe —• %Windir%\inf\oem7A.PNF
- S7tgtopx.exe —• %Windir%\inf\oem7A.PNF
- CCProjectMgr.exe —•%Windir%\inf\oem7A.PNF
- explorer.exe —• %Windir%\inf\oem7m.PNF

The services.exe, s7tgtopx.exe (Simatic manager) and CCProjectMgr.exe (WinCC project manager) will be injected with oem7a.pnf, which is a copy of the main FriendlyPixie DLL. Once injected, FriendlyPixie executes on the compromised computer.

Explorer.exe is injected with oem7m.pnf, an unknown file, which does not appear to be dropped by FriendlyPixie.

Summary of Findings on Digital Forensic Examination

This report has identified information relating to the case of the failed update of NisPower SCADA and network systems.

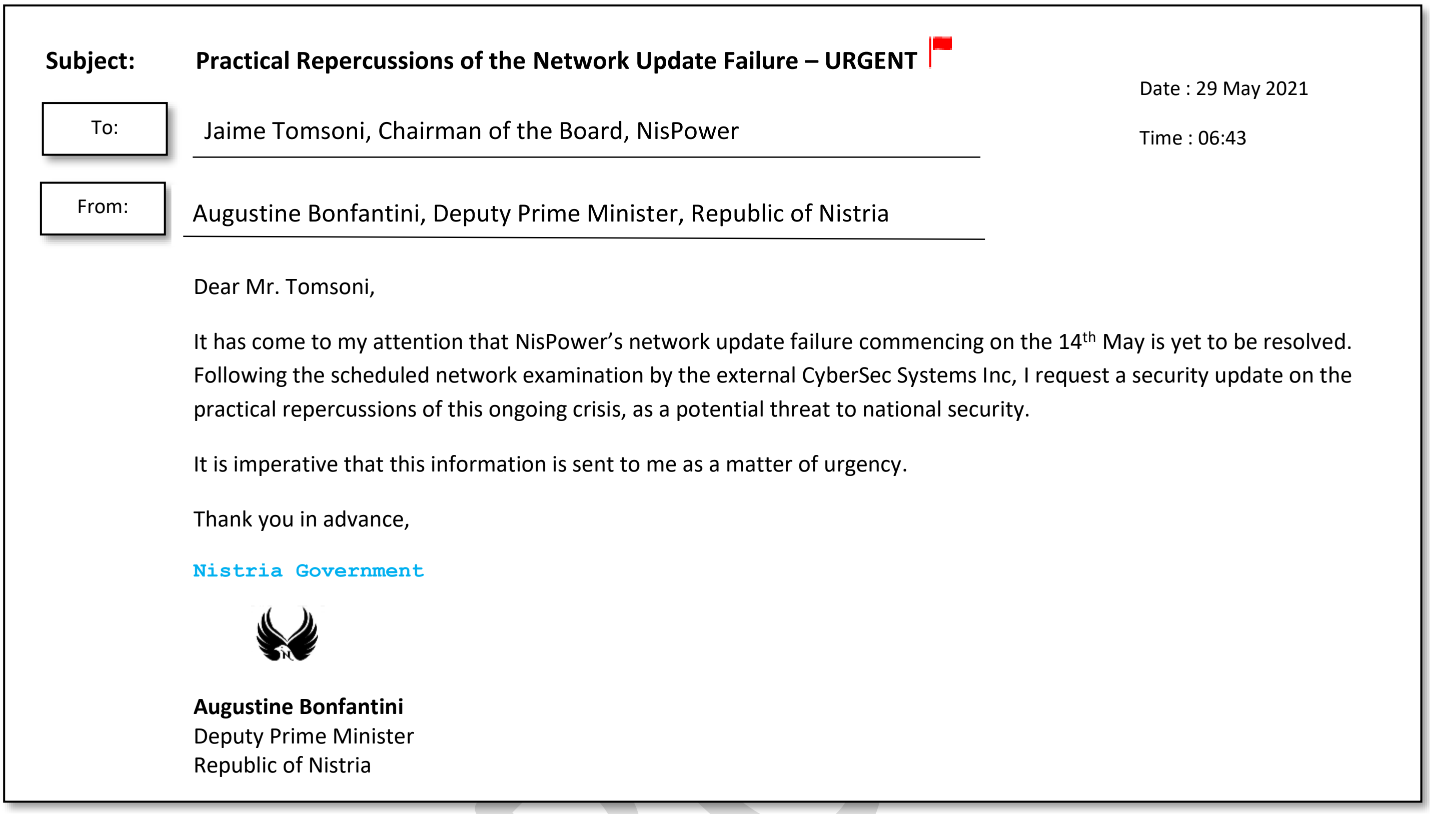
The team deployed by CyberSec Systems and led by Dr Baezner carried out an extensive digital forensic examination of NisPower systems and discovered the presence of a malware tool. This malware, from the FriendlyPixie family, is designed with multiple payloads. The first payload corrupts SCADA systems, rendering them non-operational. The second payload locks infected systems out of redundancies, preventing the bootup of backup systems or a return to pre-event status quo.

FriendlyPixie is a family of malware well-known to the penetration (PEN)-testing community. It has been found to target corporations and state-owned entities. Sophisticated international criminal organisations have deployed FriendlyPixie to target financial institutions and government economic centres for financial gain. So-called “eco-warriors” have also targeting fossil fuel entities to disrupt production and energy supply.

Although the malware is commercially available on the dark web, it is sophisticated, suggesting a certain level of resources on the part of the perpetrator. Due to the speed with which the malware spread, the initial infection appears to have been in the NisPower home network based in its Nistropolis headquarters. This suggests that NisPower assets and networks were the intended target. The malware has been customised to have the maximum effect on energy distribution and control systems. The customisation, although minimal use of syntax and coding language, is most often found in the Mustelan gaming industry.

It is now up to the board of NisPower and the Nistrian government to determine the value of this report, and to decide on appropriate follow-up action. It is important to note that there was no evidence pointing to a specific perpetrator or origin location. The examination found only the malware that caused the systemic failure.

Appendix 3



Subject: **Practical Repercussions of the Network Update Failure – URGENT** 🚩

Date : 29 May 2021

Time : 06:43

To: Jaime Tomsoni, Chairman of the Board, NisPower

From: Augustine Bonfantini, Deputy Prime Minister, Republic of Nistria

Dear Mr. Tomsoni,

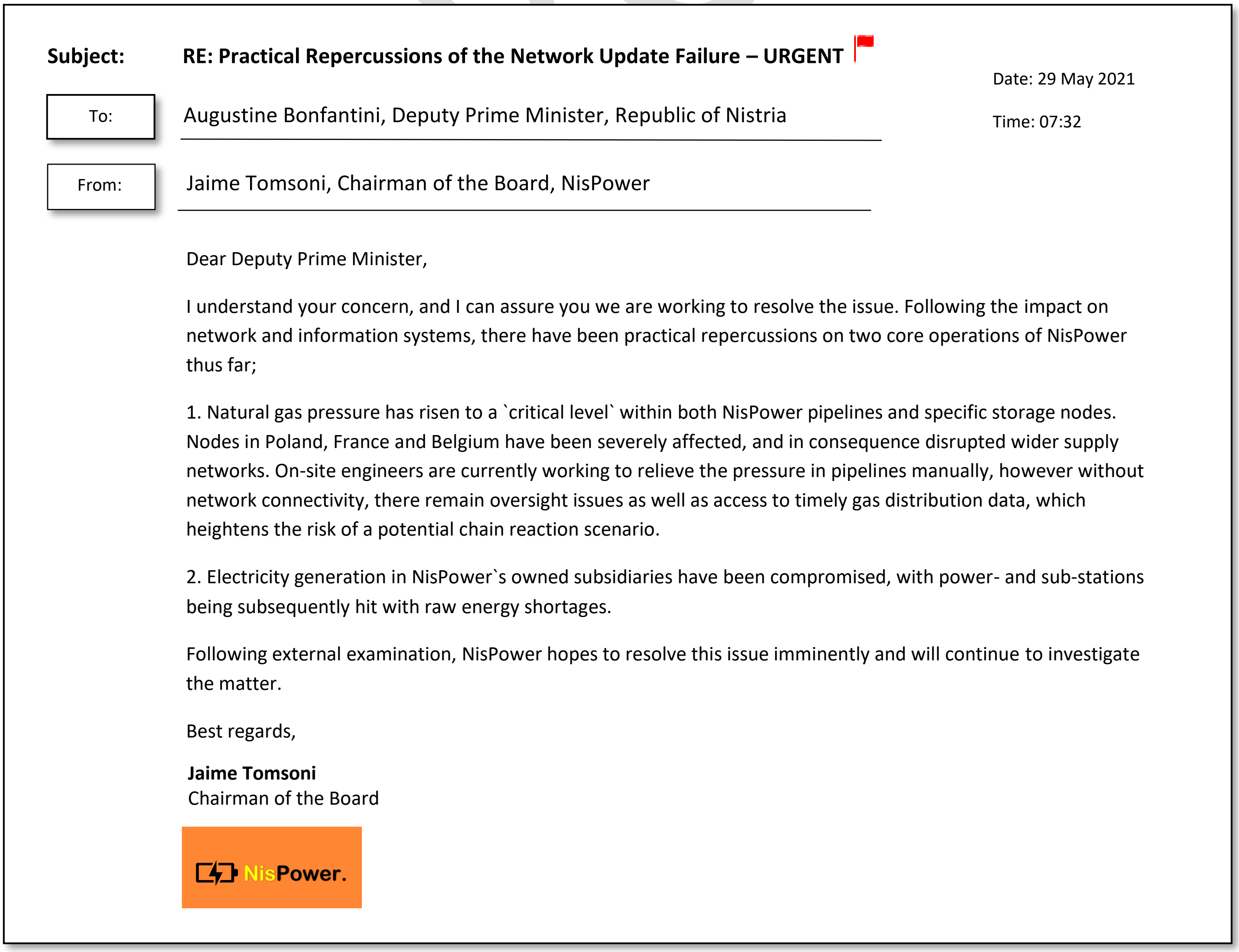
It has come to my attention that NisPower's network update failure commencing on the 14th May is yet to be resolved. Following the scheduled network examination by the external CyberSec Systems Inc, I request a security update on the practical repercussions of this ongoing crisis, as a potential threat to national security.

It is imperative that this information is sent to me as a matter of urgency.

Thank you in advance,

Nistria Government

Augustine Bonfantini
Deputy Prime Minister
Republic of Nistria



Subject: **RE: Practical Repercussions of the Network Update Failure – URGENT** 🚩

Date: 29 May 2021

Time: 07:32

To: Augustine Bonfantini, Deputy Prime Minister, Republic of Nistria

From: Jaime Tomsoni, Chairman of the Board, NisPower

Dear Deputy Prime Minister,

I understand your concern, and I can assure you we are working to resolve the issue. Following the impact on network and information systems, there have been practical repercussions on two core operations of NisPower thus far;

1. Natural gas pressure has risen to a `critical level` within both NisPower pipelines and specific storage nodes. Nodes in Poland, France and Belgium have been severely affected, and in consequence disrupted wider supply networks. On-site engineers are currently working to relieve the pressure in pipelines manually, however without network connectivity, there remain oversight issues as well as access to timely gas distribution data, which heightens the risk of a potential chain reaction scenario.

2. Electricity generation in NisPower`s owned subsidiaries have been compromised, with power- and sub-stations being subsequently hit with raw energy shortages.

Following external examination, NisPower hopes to resolve this issue imminently and will continue to investigate the matter.

Best regards,

Jaime Tomsoni
Chairman of the Board

NisPower.

Subject: **RE: Practical Repercussions of the Network Update Failure – URGENT**

Date : 29 May 2021

Time : 07:59

To: Jaime Tomsoni, Chairman of the Board, NisPower

From: Augustine Bonfantini, Deputy Prime Minister, Republic of Nistria

Dear Mr. Tomsoni,

I appreciate your timely response.

Given the nature of the situation, I will need to relay this to the EU's Political and Security Committee considering the potential security repercussions on not only Nistria energy, but as you inferred, other European states and third parties.

It is imperative that the Nistria Government is directly updated with NisPower`s network developments and risk assessments during this time. Please contact myself as soon as information becomes available.

Thank you in advance,

Nistria Government

Augustine Bonfantini
Deputy Prime Minister
Republic of Nistria

Appendix 4[14]

theguardian

TEMPERS FLARE AT NATIONAL DAY CELEBRATIONS

Ethnic Mustelans celebrating Mustelan National Day on 8th May clash with Nistrian Police.

The annual Mustelan National Day celebrations in the east of the Republic of Nistria turned violent as ethnic Mustelans clashed with police amid allegations of racial interference. In the eastern town of Bromli, close to the Nistrian-Mustelan border, Nistrian police broke up a large crowd of revellers based on public order concerns. A number of arrests were made for public order offences such as public intoxication and resisting arrest, when a makeshift bonfire threatened to blow out of control and was extinguished by Nistrian police. The dousing of the bonfire sparked anti-police chants accusing authorities of racial prejudice and seeking to quell ethnic Mustelan free speech.

Since the Republic of Nistria became independent from Mustelus in 2010 following a fiercely fought referendum, ethnic Mustelans living in Nistria have celebrated their connection to what they perceive as their homeland in largely peaceful displays of national pride. However, tempers tend to flare around the 8th May, Mustelus's National Day. In the east of Nistria, the region closest to Mustelus, demonstrations and pro-Mustelus parades are a frequent occurrence. Most pass peacefully but in recent years violence has broken out amid concerns that Nistrian authorities are being heavy-handed in their dealings with the Mustelan diaspora, as well as allegations of Mustelan government interference and deliberate incitement to violence. Pro-Mustelan social media campaigns spike dramatically in the run-up to Mustelan National Day.

Shaun Codri, 28, the son of Mustelan immigrants who witnessed the clashes said "yes, some people were drunk, but we were simply celebrating our national and cultural heritage. The police had no right to stop us from doing that. Sure, some people drank too much but that happens every weekend and the police don't care. Why should today be different?"

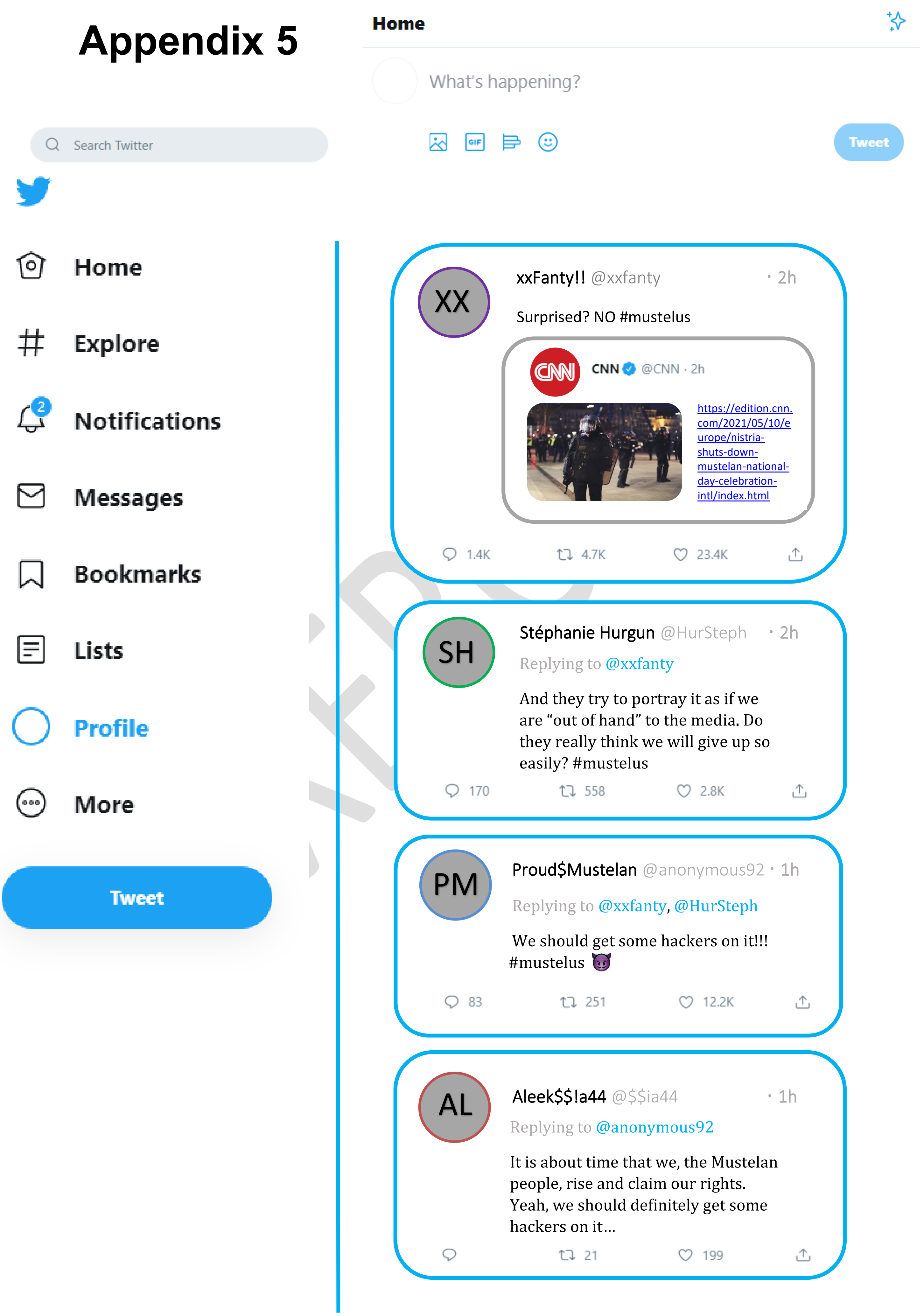
Elena Hordvig, the mayor of the east-Nistrian town of Bromli responded to the allegations of heavy-handed policing by saying "we are proud of our shared cultural history and every year we encourage Mustelans and those descended from Mustelans to celebrate their heritage. It is a shame that a few bad apples are spoiling the festivities for everyone by letting things get out of hand. The police have a

[14] All written material here is FICTIONAL. Original source for graphics can be found here https://www.theguardian.com/world/2020/jan/28/french-police-clash-with-firefighters-during-paris-protest

responsibility to protect everyone, Nistrians and Mustelans alike, and I am proud of the job that they do."

Responding to unconfirmed reports that Mustelan government-backed militia had crossed the border in civilian clothing during the night of 7th and 8th May in order to incite anti-Nistrian violence, Mayor Hordvig acknowledged that she had heard these reports but refused to be drawn on them.

Appendix 5



xxFanty!! @xxfanty · 2h

Surprised? NO #mustelus

CNN @CNN · 2h

https://edition.cnn.com/2021/05/10/europe/nistria-shuts-down-mustelan-national-day-celebration-intl/index.html

1.4K 4.7K 23.4K

Stéphanie Hurgun @HurSteph · 2h

Replying to @xxfanty

And they try to portray it as if we are "out of hand" to the media. Do they really think we will give up so easily? #mustelus

170 558 2.8K

Proud$Mustelan @anonymous92 · 1h

Replying to @xxfanty, @HurSteph

We should get some hackers on it!!! #mustelus 😈

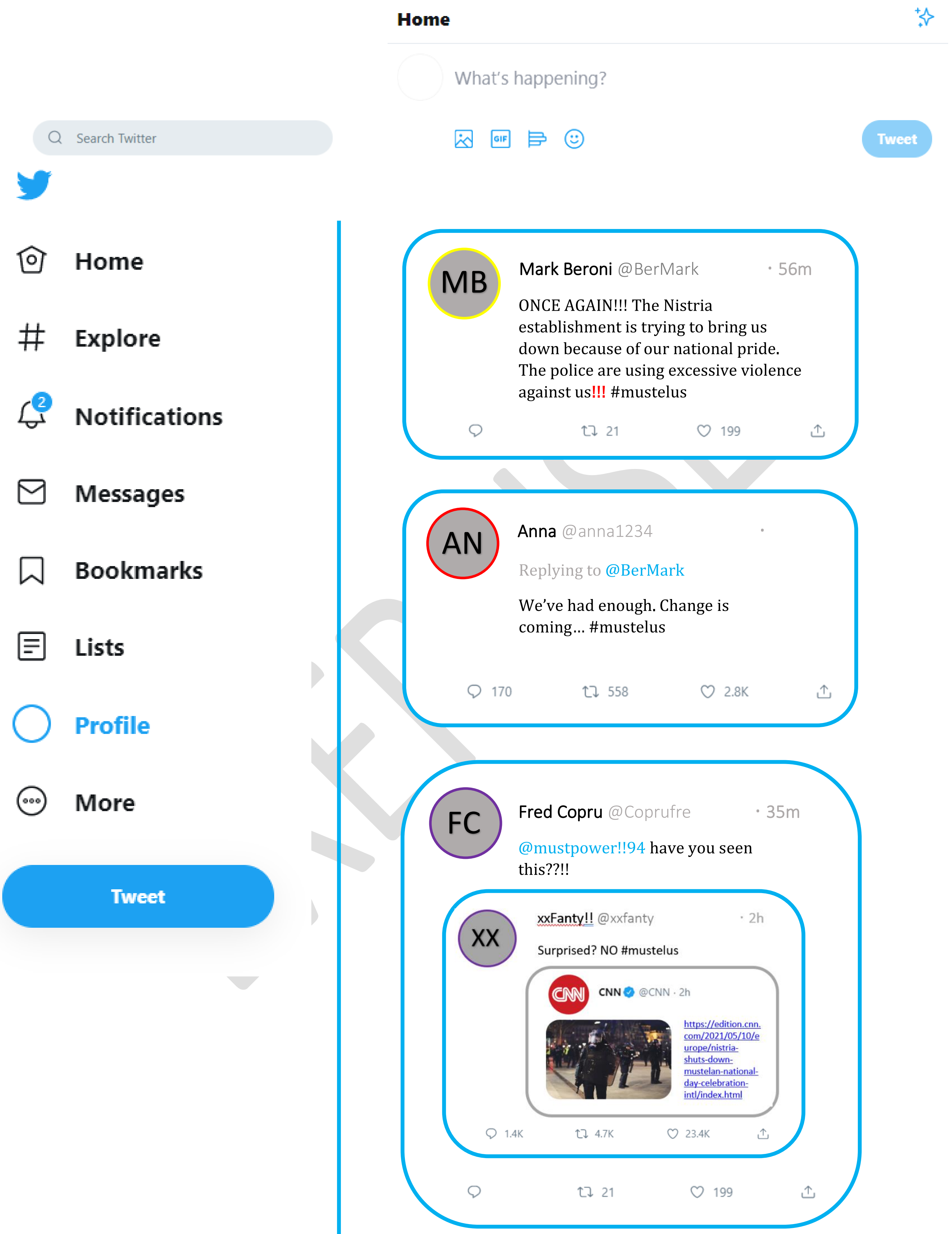
83 251 12.2K

Aleek$$!a44 @$$ia44 · 1h

Replying to @anonymous92

It is about time that we, the Mustelan people, rise and claim our rights. Yeah, we should definitely get some hackers on it…

21 199



Mark Beroni @BerMark · 56m

ONCE AGAIN!!! The Nistria establishment is trying to bring us down because of our national pride. The police are using excessive violence against us!!! #mustelus

21 199

Anna @anna1234 ·

Replying to @BerMark

We've had enough. Change is coming… #mustelus

170 558 2.8K

Fred Copru @Coprufre · 35m

@mustpower!!94 have you seen this??!!

xxFanty!! @xxfanty · 2h

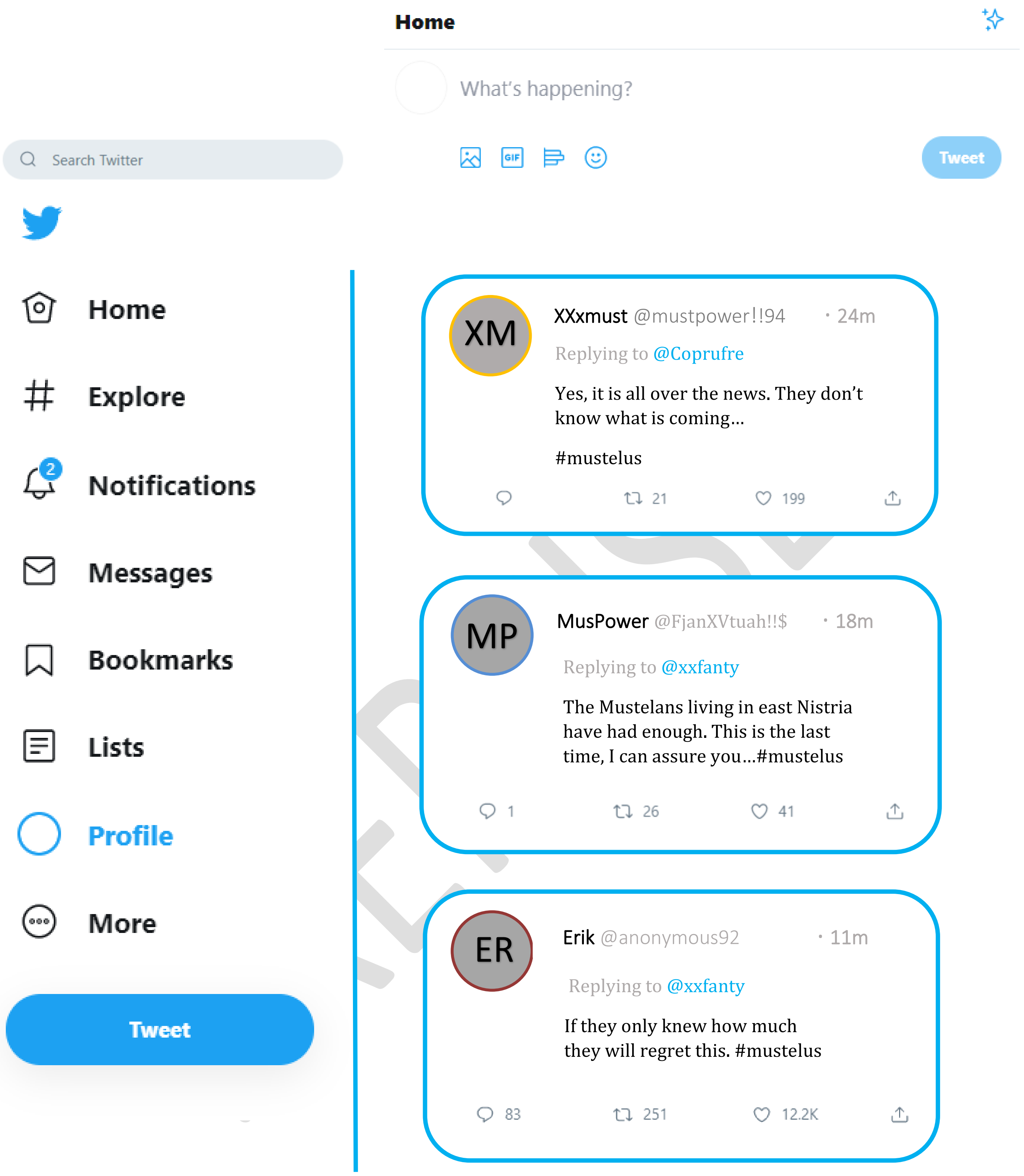
Surprised? NO #mustelus

CNN @CNN · 2h

https://edition.cnn.com/2021/05/10/europe/nistria-shuts-down-mustelan-national-day-celebration-intl/index.html

1.4K 4.7K 23.4K

21 199



XXxmust @mustpower!!94 · 24m

Replying to @Coprufre

Yes, it is all over the news. They don’t know what is coming…

#mustelus

MusPower @FjanXVtuah!!$ · 18m

Replying to @xxfanty

The Mustelans living in east Nistria have had enough. This is the last time, I can assure you…#mustelus

Erik @anonymous92 · 11m

Replying to @xxfanty

If they only knew how much they will regret this. #mustelus

Appendix 6[15]

European Commission

European Commission - Press release

Antitrust: Commission opens investigation into possible anti-competitive conduct of NisPower

Brussels, 31 March 2021

The European Commission has opened a formal antitrust investigation to assess whether NisPower's purchase of several European energy companies is in breach of EU competition rules.

Commissioner Magdalene **Brach**, in charge of competition policy, said: *"European consumers are increasingly becoming concerned about where their energy comes from. E-commerce has boosted retail competition and brought more choice and better prices in the energy sector. We need to ensure that large corporations operating as monopolies don't eliminate these benefits through anti-competitive behaviour such as buying up independent companies to create monopolies. I have therefore decided to take a very close look at NisPower's business practices and its dual role as producer and retailer, to assess its compliance with EU competition rules."*

NisPower has numerous roles as a platform: (i) it sells energy to consumers as a retailer; (ii) it sells energy to consumers via a network of wholly-owned subsidiaries; (iii) it produces energy and sells it to other utility companies; (iii) it operates as a state-owned enterprise in Nistria; and (iv) it operates as a private entity in a number of other European states in addition to its subsidiaries. This can cause confusion and a lack of choice.

When providing energy to consumers and non-subsidiary entities, a marketplace for independent sellers, NisPower continuously collects data about corporate and private customers. Based on the Commission's preliminary fact-finding, NisPower appears to use competitively sensitive information – on marketplace sellers, their products and transactions.

As part of its in-depth investigation the Commission will look into:

- the **standard agreements between NisPower and downstream distributors**, which allow NisPower's retail business to analyse and use third party seller data. In particular, the Commission will focus on whether and how the use of accumulated marketplace seller data by NisPower as a retailer affects competition;
- the role of data in the purchase of **wholly-owned subsidiaries.**

If proven, the practices under investigation may breach EU competition rules on anticompetitive agreements between companies (Article 101 of the Treaty on the Functioning of the European Union (TFEU)) and/or the abuse of a dominant position (Articles 102 TFEU).

The Commission will now carry out its in-depth investigation as a matter of priority. The opening of a formal investigation does not prejudge its outcome.

[15] This press release has been adapted from an official EU publication. The original source can be found here https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291

Background

Article 101 of the TFEU prohibits anticompetitive agreements and decisions of associations of undertakings that prevent, restrict or distort competition within the EU's Single Market.

Article 102 of the TFEU prohibits the abuse of a dominant position. The implementation of these provisions is defined in the Antitrust Regulation (Council Regulation No 1/2003), which can also be applied by the national competition authorities.

Article 11(6) of the Antitrust Regulation provides that the opening of proceedings by the Commission relieves the competition authorities of the Member States of their competence to apply EU competition rules to the practices concerned. Article 16(1) further provides that national courts must avoid adopting decisions that would conflict with a decision contemplated by the Commission in proceedings it has initiated.

The Commission has informed NisPower and the competition authorities of the Member States that it has opened proceedings in this case.

There is no legal deadline for bringing an antitrust investigation to an end. The duration of an antitrust investigation depends on several factors, including the complexity of the case, the extent to which the undertakings concerned cooperate with the Commission and the exercise of the rights of defence.

More information on the investigation will be available on the Commission's competition website, in the public case register under case number AX.5248.

IP/19/4291

CYBER 9/12 STRATEGY CHALLENGE

Atlantic Council

25 YEARS GCSP Geneva Centre for Security Policy

2020 Cyber 9/12 Strategy Challenge

Intelligence Report II

Competition Instructions

Your team will take on the role of experienced cyber policy experts invited to brief the Political and Security Committee of the European Union which has been called to address an evolving cyber crisis. **For the purposes of this exercise**, the Political and Security Committee is made up of European leaders (including heads of state, heads of government, ministers of defence and foreign affairs, directors of intelligence services, and representatives from the private sector).[16]

This briefing document contains fictional information on the background and current situation involving a major cyber incident affecting critical infrastructure and services in Europe. The incident notionally takes place in **June and July 2021**. The scenario presents a fictional account of political developments and both public and private reports on the cyber incident.

Your team needs to provide information on the full range of policy response alternatives available to respond to this crisis, and has been tasked to develop 2-4 policy recommendations to present to the task force. You are to consider as facts the following pages in formulating your response.

You will use the fictional scenario material presented to perform two tasks:

1. **Oral Policy Brief:** Prepare a ten-minute oral presentation outlining possible policy options and recommending one to the task force.
2. **Decision Document:** Teams will also be required to submit a “decision document” accompanying their oral presentation at the beginning of the competition round. The “decision document” will be maximum one page outlining the team’s policy response options, decision process, and recommendations. The teams should note that the document is not intended to summarise every detail of the recommendations, but to help the judges follow the oral presentation. Judges will be given only 2 minutes to read the document before the presentation begins.

Keep these tips in mind as you are reading and considering your policy response alternatives:

[16] The Political and Security Committee in reality is made up of EU Ambassadors representing their countries. More information can be found here https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/political-security-committee/

- **Don’t fight the scenario**. Assume all scenario information presented is possible, observed, or reported as written. Use your energy to explore the implications of that information, not the plausibility.
- **Think multi-dimensionally**. When analysing the scenario, remember to consider implications for other organisations and domains (e.g. private sector, military, law enforcement, information operations, diplomatic, etc.) and incorporate these insights along with cyber security.
- **Be creative**. Cyber policy is an evolving discourse, and there is no single correct policy response option to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- **Analyse the issues**. The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various official publications from entities such as the European Union or derived from original news sources while others have been invented by the authors. All scenario content is intended for academic, simulation purposes and is not meant to represent the views of the competition organisers, authors, or any affiliated or named organisation, actual or fictional.

Briefing

From: The Political and Security Committee of the European Union

Re: Escalating disruption to pan-EU energy and electricity supply following failed NisPower IT Upgrade

Date: 2nd July, 2021

The date is the 2nd July, 2021, and your team has recently presented policy recommendations to the European task force. Since then, there has been increasing cyber disruption across Europe, affecting energy infrastructure and services. This disruption in connected to the failed upgrade of NisPower's central networks. Given the growing urgency of the situation, the chairman of the task force has asked your team to consider the latest information available and develop additional policy response options to present at the next task force meeting tomorrow morning, at **9:10am on 3 July, 2021.**

Your oral policy brief recommendations must analyse the possible strengths, weaknesses, opportunities, and threats of each proposed policy response alternative before recommending the one best course of action. To do so, you will apply your understanding of cyber security, law, foreign policy, civil aviation and security theory to synthesise useful policy measures from limited information.

When generating each of your policy response alternatives, the task force requests that you consider the following potentially conflicting interests at the national, EU and NATO level. These are provided as suggested starting points and are not meant to limit your policy responses.

Immediate Response vs. Delayed Response

What actions should be considered, if any, if the possibility exists of European agencies' involvement? What actions should be taken immediately after the incident versus those that should be taken later?

Government Response vs. Private Sector Response

What actions should be led by the private sector in response to the reports and incidents and what actions should be under the government's leadership? Actions to consider may include public acknowledgements, preventive and pre-emptive defensive actions, and offensive actions.

Unilateral Response vs. Multilateral Response

Should there be a unilateral or multilateral response within Europe? What about international organizations like the United Nations and NATO?

Direct Response vs. Indirect Response

If action is to be taken, should it be a direct or indirect response to the incident? Should no action be taken?

Additionally, this message is accompanied by several documents that may assist your team in preparing its policy response alternative recommendations for the task force:

Appendix 1- Letter from NisPower to the European Commission regarding the escalating situation

Appendix 2- Republic of Nistria formal request for resources from Europol

Appendix 3- BBC news article on energy security

Appendix 4- NATO intelligence report

Appendix 5- AP news report on Mustelan troop movements.

Appendix 1

European Commission

To: European Commission
From: Jaime Tomsoni, Chairman of the Board, NisPower
Date: 30 June, 2021

NisPower hereby wishes to inform the European Commission of the prevailing situation following our failed network update on the 14 June 2021.

The urgent situation and practical impacts following NisPower's failed network update has created an unsustainable situation in which NisPower cannot further guarantee energy supply to affected European countries. NisPower's electricity grids and gas pipelines are strongly interconnected across Europe, and the digital incident on the 14 June generated a severe disruption to the energy system and is likely to trigger cascading effects. We are highly concerned that the consequences will be of such nature that large parts of our receiving countries will be unable to obtain their requested energy supply for a prolonged period of time.

In addition to energy supply and distribution, NisPower also wishes to stress the potential physical consequences this situation could impose on the concerned infrastructure. An investigation conducted by CyberSec Systems Inc. found a number of critical risks that could develop within the next few days. It is of high importance that the European Commission is informed of these risks by reason of the European dimension of Nispower's operations.

The following risks have been identified as high-level:

1. Two of NisPower's three nuclear power plants in France, which were disrupted by the failed network update, are in danger of going into imminent meltdown, which in turn will affect widespread European energy supply.
2. Three gas pipeline hubs are now critically overloaded and could result in a potential explosive chain reaction if a solution is not reached urgently. NisPower is currently working on assuring the safety of our staff at the affected facilities and surrounding areas.

3. Electricity supplies to Nistria and neighbouring countries are severely disrupted with reports today of localised blackouts. This is of high concern for critical infrastructure solely reliant on NisPower supply.

As of today, NisPower will act in full cooperation with both the Government of Nistria and the EU to resolve this matter.

Jaime Tomsoni

NisPower.

Appendix 2

MEMO

Classified TOP SECRET

Official Request for Investigative Resources from THE GOVERNMENT OF THE REPUBLIC OF NISTRIA to the EUROPEAN CYBERCRIME CENTRE at EUROPOL

Date: 2 July 2021

Time: 19.27 pm

The Government of the Republic of Nistria herewith requests investigative resources from the European Cybercrime Centre (EC3) at Europol.

This request concerns the current situation of NisPower's failed network update on 14 June. NisPower contracted CyberSec Systems Inc. to conduct a digital forensic examination relating to the issues faced by the planned upgrade and consolidation of the company's computer network and SCADA systems.

Findings of the initial examination on the 28 June 2021 concluded the presence of a tool from the FriendlyPixie malware family. The malware inherits two payloads — the first one corrupts SCADA systems, rendering them non-operational, while the other payload locks infected systems out of redundancies, preventing the bootup of backup systems or a return to status quo. It remains unknown as to how and when this malware appeared in the network, and as to why it activated during NisPower's network update.

Following the first digital forensic examination and the provided report, NisPower and the Nistrian government have issued a second request to CyberSec Systems Inc. to further investigate the origin location and possible perpetrator of the malware. It is imperative to all relevant entities that this information is obtained, in order for NisPower and the Republic of Nistria to act upon the current system failures.

The Government of Nistria hereby requests assistance from Europol through the formation of a joint team with CyberSec Systems Inc, to support a second digital forensics report. The nature of this crisis, and the practical energy impacts across Europe, calls for Europol and the

European Cybercrime Centre’s most sophisticated tools and resources to move forward on this matter.

We look forward to your cooperation.

Nistria Government

Augustine Bonfantini
Deputy Prime Minister
Republic of Nistria

Appendix 3

NisPower's Network Update Failure Threatens Europe's Energy Security

NisPower, the Nistrian state-owned energy production and distribution company faces major challenges in the aftermath of its failed network update, threatening energy security across Europe.

NisPower's planned and failed update of their SCADA systems across its entire network — both the Nistrian home network and its subsidiaries abroad — is having increasingly negative effects on energy production and distribution across the whole of Europe.

As NisPower, according to its own sources, is working intensively to solve the issue, several real-world consequences have appeared.

Most concerning of which is that two nuclear power plants in Northern France that were cut-off during the update, are considered to almost be at a complete 'meltdown' level. Gas supplies to European states have also been affected, with pipelines reportedly at risk of explosion. NisPower has yet to clarify if this poses a risk to nearby towns or public sites, or even directly notify the countries in which the pipelines currently run.

Some neighbouring countries dependent on Nistrian energy are already reporting disruptions and localised blackouts.

BBC NEWS

If this continues, millions of households could lose their electricity supply, considered even more pressing for critical national infrastructure with some states, particularly France, already consulting crisis management experts.

Other energy companies, particularly those in the energy-rich Federal Republic of Mustelus, whilst outside the EU, have publicly reached out as potential new suppliers to mitigate the potential crisis and longer-term effects.

Although NisPower's failed network update is an eye-opening event itself, more interesting is that the company and the state have still yet to identify who or what is behind this failure — whether it was an internal systematic error or a potentially malicious state-supported attack to cause widespread damage to the energy giant.

Crowds of people in affected countries have shown their dissatisfaction with the situation over social media, demanding answers and reparations by the company. BBC News sought NisPower's CEO for a response, but he declined to comment.

Europe continues to look at NisPower and the Nistrian government for further clarity and confirmation on what could be expected in days to come.

2 July, 2021, 19:51

Appendix 4

SECRET NATO Joint Security Awareness Report

NATO
OTAN
NORTH ATLANTIC TREATY ORGANIZATION

DE RFG NR 208
IMMEDIATE
R 20210702Z JUL
FM NATO CYBER OPS CEN
TO NATO CSOC DISTRO
SIC WDR GFR
KJ
NATO SECRET

SUBJECT 1: OBSERVATION OF NATIONALIST, ANTI-NISTRIAN CHATTER IN DIGITAL FORA DISCUSSING TARGETING OF NISTRIAN ENERGY ASSETS

SUBJECT 2: INCREASED AVAILABILITY OF FRIENDLYPIXIE MALWARE ON SITES VISITED BY MUSTELAN NATIONALISTS

IN LIGHT OF THE CURRENT SITUATION ON NISPOWER'S FAILED NETWORK UPDATE AND THE SUBSEQUENT NATIONAL AND EUROPEAN IMPACT, THE CYBER OPERATIONS CENTRE HAS GATHERED INTELLIGENCE IDENTIFYING A NUMBER OF OPERATIONS BELIEVED TO BE OF RELEVANCE TO THE PARTIES INVOLVED IN THE CRISIS.

SUBJECT 1:

THE CYBER OPERATIONS CENTRE HAS IN RECENT WEEKS OBSERVED ALARMING INFORMATION EXCHANGE BETWEEN SEVERAL INDIVIDUALS IN THE HIGHLY INTERACTIVE AND SOCIETAL MUSTELEAN GAMING COMMUNITY. PREVIOUS NATO INTELLIGENCE OPERATIONS HAVE DEMONSTRATED HOW THE COMPUTER GAMES ARE MMPORGS WITH THE STRATEGIC GOAL OF REUNIFICATION OF SEPARATIST ENTITIES. THE INFORMATION EXCHANGES OF CONCERN INVOLVE COMPREHENSIVE INFORMATION ON HOW TO ACCESS THE MALWARE, WHAT SPECIFIC CONSEQUENCES IT IS SOUGHT TO GENERATE, AND HOW TO IMPLEMENT IT SUCCESSFULLY. IN ADDITION TO THE CHATTER INVOLVING INFORMATION ON HOW TO USE THE MALWARE, NATO HAS IDENTIFIED MULTIPLE ACTORS DISCUSSING THE TARGETING OF NISTRIAN ENERGY ASSETS.

SUBJECT 2:

THE MALWARE, WHICH IS BELIEVED TO BE THE CAUSE OF THE FAILED UPDATE, IS PART OF THE MALWARE FAMILY FRIENDLYPIXIE. THIS SPECIFIC MALWARE FAMILY IS EASILY AVAILABLE ON THE DARK WEB FOR ANY PERPETRATOR TO PURCHASE AND

EMPLOY FOR CRIMINAL PURPOSES. CERTAIN KNOWLEDGE IS REQUIRED TO SUCCESSFULLY ADOPT THE MALWARE INTO THE INTENDED TARGET. ACCORDING TO OUR INTELLIGENCE, SITES REGULARLY USED BY MUSTELAN NATIONALISTS HAVE BEEN THE PREVAILING PLATFORM FOR SUCH KNOWLEDGE SHARING. NATO HAS ALSO RECOGNIZED AN INCREASED AVAILABILITY OF THE MALWARE AT THE SITES ON THE DARK WEB WHICH ARE COMMONLY USED BY THE MUSTELAN NATIONALISTS.

KJ
NNN

Appendix 5

AP

BREAKING NEWS
2 July, 2021, 20:21

NISTROPOLIS (AP) - There are unconfirmed reports of Mustelan troop movements on the border of the Republic of Nistria. Speculation is mounting that these exercises were timed to coincide with the recent failed update of state-owned NisPower’s computer network systems.

Sources in the Mustelan government have denied there is any connection, claiming that the troop movements are part of the Mustelan Armed Forces’ annual spring exercises. They deny any planned aggression.

Nevertheless, there remains speculation that the cyber operations targeting Nistrian power supplies are a precursor to an escalation of conflict. Sources close to the NisPower network failure state that the highly sophisticated nature of the cyber operation implies state-sponsorship.

Nistria was a former federal state of Mustelus until it gained independence in 2010. Since then, a sizeable minority of ethnic Mustelans have been pushing for reunification, and the right-wing Mustelan media continues to not recognise Nistria’s independence. Up until now, any hostilities have remained political, but observers have noted the similarities between the Nistrian infrastructure failure and the historic use of cyber operations as preludes to conventional military assualts.

More details soon

2020 Cyber 9/12 Strategy Challenge

Intelligence Report III

Competition Instructions

Your team will take on the role of experienced cyber policy experts invited to brief the Political and Security Committee of the European Union which has been called to address an evolving cyber crisis. **For the purposes of this exercise**, the Political and Security Committee is made up of European leaders (including heads of state, heads of government, ministers of defence and foreign affairs, directors of intelligence services, and representatives from the private sector).[17]

This briefing document contains fictional information on the background and current situation involving a major cyber incident affecting critical infrastructure and services in Europe. The incident notionally takes place in **June and July 2021**. The scenario presents a fictional account of political developments and both public and private reports on the cyber incident.

Your team needs to provide information on the full range of policy response alternatives available to respond to this crisis, and has been tasked with developing a holistic policy recommendation to present to the task force. You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform one task:

1. Oral Policy Brief: Prepare a ten-minute oral presentation outlining possible policy options and recommend one to the task force.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- **Don't fight the scenario**. Assume all scenario information presented is possible, observed, or reported as written. Use your energy to explore the implications of that information, not the plausibility.
- **Think multi-dimensionally**. When analysing the scenario, remember to consider implications for other organisations and domains (e.g. private sector, military, law enforcement, information operations, diplomatic, etc.) and incorporate these insights along with cyber security.
- **Be creative**. Cyber policy is an evolving discourse, and there is no single correct policy response option to the scenario information provided. There are many ideas to experiment with in responding to the crisis.

[17] The Political and Security Committee in reality is made up of EU Ambassadors representing their countries. More information can be found here https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/political-security-committee/

- **Analyse the issues**. The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various official publications from entities such as the European Union or derived from original news sources while others have been invented by the authors. All scenario content is intended for academic, simulation purposes and is not meant to represent the views of the competition organisers, authors, or any affiliated or named organisation, actual or fictional.

Briefing

From: The Political and Security Committee of the European Union

Re: Escalating disruption to pan-EU energy and electricity supply following failed NisPower IT Upgrade

Date: July 3, 2021

The date is the 3rd July, 2021 and since you last presented your policy recommendations to the European task force, we have witnessed some major incidents affecting energy infrastructure and services, as well as an escalating political situation regarding attribution. These pose an imminent threat to Europe and neighbouring regions. Given the urgency of the situation, the chairman of the task force has asked your team to consider the latest information available and develop additional policy response options to present at the next task force meeting in **15 minutes**.

Your recommendation must analyse the possible strengths, weaknesses, opportunities, and threats of each proposed policy response alternative before recommending the best course of action. To do so, you will apply your understanding of cybersecurity, law, foreign policy, civil aviation and security theory to synthesize useful policy measures from limited information.

When generating your response, the task force requests that you consider the following potentially conflicting interests at the national, EU and NATO level. These questions are provided as suggested starting points and are not meant to limit your policy responses.

1. **What should be the highest priority when responding?**
2. **Who is best placed to respond?**
3. **What should be the nature of that response?**

Additionally, this message is accompanied by several documents that may assist your team in preparing its policy response for the task force:

Appendix 1 – Serious and Organised Crime Threat Assessment report on malware origin and perpetrator(s)

Appendix 2 – News Report regarding pan-European electricity and gas supply crisis

Appendix 3 – DG Connect Memo from European Commission to NisPower Executive regarding national energy protocol and guideline adherence

Appendix 4 – Breaking News of criminal arrest.

Appendix 1

EU CONFIDENTIAL

DATE: 3rd July 2021

Serious and Organised Crime Threat Assessment: Report from Europol on NisPower`s computer network and SCADA system update failure and malware detection.

The SOCTA Methodology

The SOCTA analyses and explores criminal markets and crime areas in the EU; the organised crime groups (OCGs) or individuals carrying out these criminal activities; as well as factors in the broader environment that shape the nature of serious and organised crime within Europe. This assessment explores a particular family of malware, FriendlyPixie, that has proven popular in the PEN-testing community, is commercially accessible online via the dark web, and has previously been utilised to target corporations and state-owned entities by OCGs. It has recently been detected as the primary source of an energy company system failure that has required further analysis.

This report summarises the investigation carried out by the Joint Technical Team (EC3-CyberSec) on the failed network upgrade and subsequent FriendlyPixie malware detection within the state-owned NisPower, an energy company based in Nistria that also privately operates across Europe. This JTT assessment contributes to previous reports, initiated with the external cyber forensic examination by the U.S.-based CyberSec Systems on the 28th June 2021. This has been referred to Europol following a formal request from the Government of the Republic of Nistria for the European Cyber Crime Centre (EC3) to provide investigative support, in partnership with CyberSec Systems.

Initial Reports

The initial CyberSec ICT analysis found the presence of the malware tool, FriendlyPixie, within the combined home and satellite network. The complexity of the malware indicated this was a malicious act customised to produce maximum damage to energy production and distribution control systems, implying a perpetrator with a high degree of knowledge and capability.

Prior investigation confirmed many elements of the code were popular amongst the gaming industry and demonstrated Mustelan hallmarks. NATO had also picked up chatter on potential Mustelan nationalist involvement. Whilst these lack political attribution, current political circumstances and CyberSec Systems' request have warranted further multilateral investigation by the JTT into the malware origin, network failure and perpetrator(s).

Investigation

I. Origin of Malware

Corresponding with prior reports, forensic examination of the FriendlyPixie's source code revealed Mustelan digital "accents" – idiosyncrasies in the syntax and programming code used to write the malware. By tracking multiple packets previously identified, the location of the insertion of FriendlyPixie into NisPower's network was traced by the JTT to the computer systems of a NisPower satellite company, FRASATCo, a small, private company bought by NisPower in August 2018, located in France.

The upload of the malware has been sourced to a command and control node in a power station in Amiens, accessed via the user credentials of ***Ms B Novak*****, on the 16th August 2018 at 16:55**.

II. Network Failure

The malware remained in FRASATCo's system, but was effectively dormant. NisPower firewalls had blocked transmission into the home network during initial connection. However, during the company-wide NisPower network system upgrade on the 14th June 2021, the firewalls were temporarily disabled to enable integration. The FriendlyPixie tool was able to exploit the outdated computer systems and legacy servers of NisPower`s acquired entities, causing the malware to spread and in turn leading to subsequent system failures.

III. Perpetrator(s)

Ms Novak has been identified as the former Network Security Manager at FRASATCo, and a Mustelan emigrant living in France. Further investigation into the company has shown that shortly after the NisPower takeover, the former network security team of FRASATCo were made redundant, including Ms Novak, with their contracts terminated on the 16th August 2018.

The evidence collected during the forensic investigation and included in this report, strongly suggests that the individual user is highly involved. Both the FriendlyPixie tool, which is accessible online, and the capabilities required to tailor and upload the malware may be of a similar skillset expected of a Network Security Manager. If subsequent law enforcement investigations confirm that the insertion was deliberate, this would constitute a criminal act.

Although reminiscent of the Mustelan malware, the JTT concludes there remains insufficient evidence to attribute state involvement. Furthermore, this assessment does not confirm the company or entity acting as the primary target of this potentially malicious attack.

The JTT has provided the origin of the NisPower malware and user information to the Government of the Republic of Nistria and the relevant law enforcement community to take next steps in light of this new evidence.

Appendix 2[18]

le News
SWISS NEWS IN ENGLISH

Deadly pipeline explosion in Nistria and rolling blackouts across Europe following powerplant shutdowns.

Two people dead and 34 injured in Nistria gas pipeline explosion. Towns in blackout following power station shutdowns in Northern France, with more to be expected.

July 2nd, 2021, 06:12

Flames from the explosion that ripped through a gas pipeline in southern Nistria this morning. Photograph: Nonstopnews via AP

NisPower, the controversial state-owned energy production and distribution company that operates privately across Europe has reaped chaos following its failed security update on the 14th June.

An explosion and fire ripped through a gas pipeline in southern Nistria killing two people and injuring 34 others this morning. Among the wounded were NisPower employees from six neighbouring countries, with two Mustelan nationals confirmed dead at the scene. Footage on social media this morning showed a large column of fire in the distance, requiring over 250 firefighters. NisPower said the associated hub has been completely shut down and the blaze is now extinguished.

The destroyed pipeline was a major regional transfer node distributing natural gas to several dependent Northern European states, including Denmark, Finland, Sweden, and the Baltic

[18] Fictional material adapted from source and original graphics from https://www.irishtimes.com/news/world/europe/deadly-blast-at-austrian-pipeline-hub-cuts-gas-flow-to-italy-1.3324388

states. News of the blast has sent gas prices in Europe soaring within a few hours over fear of imminent restrictions.

Today also marks the complete shutdown of NisPower's three major nuclear power stations in Northern France, which have been at risk of meltdown since the intended system update. Despite causing widespread electricity shortages and power-cuts, the shutdown was necessary in order to "protect the integrity of the network", a spokesman has said. Further shutdowns of NisPower's plants located across Europe are expected, with 'rolling' blackouts a new reality for states dependent on the energy-rich Nistrian company.

Rolling blackouts occur when demand for electricity exceeds the supply. As both the producer and supplier of electricity, NisPower alters generation to ensure electricity supply meets the exact level of demand. Yet, with company-wide control systems still down, an unbalanced frequency at hours of peak demand has been causing, and will continue to cause, power outages across the whole of Northern Europe.

It has been suggested the supply could fall short of up to 10% of some states' energy requirements. The cut-off is expected to have a detrimental impact on state functioning as well as critical national infrastructure, with severe disruptions already reported in France, and a blackout in southern Belgium lasting over six hours yesterday evening. Moreover, with Northern European states suffering both gas and electricity shortages, several are on the verge of declaring national states of emergency.

The simultaneous actions have exacerbated concerns over NisPower's monopoly on Northern European energy, and its attribution to the Nistrian state. NisPower had previously identified these on-site risks to the EU in a safety assessment following the update failure, which begs the question, did NisPower do enough to prevent this? But even more so, in this unprecedented transnational crisis, what can the EU do to help?

Appendix 3

DG Connect Memo

To: NisPower Executive

From: Digital Society, Trust & Cybersecurity (Directorate H), European Commission

Date: July 2, 2021 11.59pm

Following Nistria's lack of clarification on vendor liability in the event of a cyberattack or incident, this memo serves as notification to follow protocols and guidelines explicitly stated in both the *Directive on Security of Network and Information Systems* (hereafter the "NIS" Directive)[19] and *Commission Recommendation SWD(2019) 1240 final*, and to act on the requirement to communicate implementation through the NIS Cooperation Group.

The Commission wishes to consult and re-inform NisPower and the Nistria government, as acting *energy network operators*, of EU cybersecurity recommendations and obligations in the energy sector at both a stakeholder and member state capacity.

National implementation of the NIS Directive was due on May 9, 2018.

After review of Nistria compliance, the Commission notes only four network security standards within the energy sector were adopted by the state prior to the scheduled system update on June 14, 2021.

On April 3, 2019, the EU issued its Commission Recommendation on cybersecurity in the energy sector, including (i) real-time requirements, (ii) the risk of cascading effects, and (iii) the combination of legacy systems with new technologies. The Recommendations identify necessary steps to enhance cybersecurity preparedness.

In consideration of the current energy climate, the Commission is not confident that adequate steps and risk evaluations were taken by NisPower prior to the scheduled system update, specifically regarding outdated servers and legacy systems of recently acquired subsidiaries. In accordance with the Recommendations, energy network operators should (4a) *apply the most recent security standards for new installations wherever adequate and consider complementary physical security measures where the installed base of old installations cannot be sufficiently protected by cybersecurity mechanisms*, as well as (12d) *conduct on a regular basis specific cybersecurity risk analysis on all legacy installations, especially when connecting old and new technologies.* The Commission is unaware of any action taken by NisPower to ensure cybersecurity of the new subsidiaries operating on identified "outdated legacy servers".

Energy network operators should *analyse the risks of connecting legacy concepts and be aware of the internal and external interfaces and their vulnerabilities*. In April 2019, EU institutions reached an agreement on the Cybersecurity Act, creating certification schemes to provide energy companies an opportunity to certify their ICT products, services or processes. The Commission notes this was not adopted by NisPower to secure subsidiary services, including for the transmitting, storing, retrieving or processing of information via network and information systems. It is recommended to utilise such initiatives as a private entity and a member state, particularly for transnational services across Europe.

The Commission also highlights Nistria's absence of a Regulation on Risk Preparedness of the Electricity Sector plan, as part of the Union's sector specific legislation. This preparedness plan takes into account cybersecurity and guarantees system stability against potential threats. Similarly, there is no indication of Nistria's adoption of the requirement to provide Gas Security of Supply Regulation, to incorporate cybersecurity within regional and national risk assessments. The current energy situation further suggests that

[19] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1.

the design criteria for a resilient grid, including the identification of critical nodes, defence measures per site and mitigation measures, was not sufficiently institutionalised prior to the system failure.

The Commission urges NisPower and the Nistria government, as an operator of essential services in energy, to take into account the horizontal guidance issued by the NIS Cooperation Group established under Article 11 of the NIS Directive. It is of high importance that NisPower reports its forthcoming restorative actions, from the date of this memo, to both the NIS Cooperation Group and the European Energy Information Sharing and Analysis Centre to monitor cascading effects.

The Director General highly recommends Nistria ensure the implementation of relevant cybersecurity preparedness measures related to real-time requirements in the energy sector to prevent reoccurrence in additional subsidiaries.

Appendix 4[20]

BREAKING NEWS: Woman arrested over NisPower system update failure; the cause of current electricity blackouts and gas shortages sweeping across Europe.

© picture alliance/AP Photo/L. Notarianni

A woman has been arrested today for the modification and insertion of a malicious piece of malware with intent to damage the computer's network system.

Following investigation carried out at both the national and transnational level, with extensive EU involvement, the woman has been identified as Belle Novak, a former Network Security Manager of one of NisPower's subsidiaries, FRASATCo in Amiens, Northern France. Sources close to the investigation report that Ms Novak — a Mustelan national with an extensive background in computer games software engineering — was made redundant following FRASATCo's takeover by Nistrian energy company NisPower in 2018. Union representatives involved in the takeover negotiations claim that NisPower executives promised there would be no redundancies, but once the takeover was finalised, they proceeded to cut staff, citing "market conditions". Many employees voiced their anger on social media at the time.

It is alleged that Ms Novak inserted a computer virus into FRASATCo's control systems as a parting gesture, which remained unidentified for almost three years until the recent failed network consolidation carried out by NisPower. Approximately one hour ago, Ms Novak was contacted by French Police at her house near Amiens and served with an arrest warrant for disruption of computer functionality and criminal damage.

In a separate development, Mustelan troops conducting exercises close to the Nistrian border have withdrawn to the capital. Sources close to the Mustelan Ministry of Defence have stated that planned exercises were completed early, and the withdrawal was not related to the current political situation between Mustelus and Nistria.

Follow our live updates to stay informed.

Updated on 3rd July 2021, 7.30 CEST.

FRANCE 24

[20] Image from https://www.dw.com/en/macron-anti-terror-law-replaces-french-state-of-emergency/a-41191947