CYBREX
STRAT CHALLENGE

MUNI

2024 CySec Strategy Challenge

Intelligence report I.

CYBREX
STRAT CHALLENGE

Briefing – Intelligence Report I

From: The Political and Security Committee of the European Union

Re: Intelligence Report I

Dear Esteemed Members of the Advisory Board,

I hope this message finds you well. Since our last correspondence, there have been significant developments regarding the Nistrian situation. Finally, we are in a position to provide you with more detailed information. The documents we send you are highly sensitive and confidential, given the nature of the issues at hand. Please handle them with the utmost discretion.

Following extensive negotiations, we have obtained communication from Mrs. Vanheuten, the Nistrian Minister for Health, which sheds light on the nature of the challenges faced. Additionally, we have secured the Investigation and Situational Report on NCH Systems Failure.

Given the tense geopolitical climate in the region, we have also included the Terrorism Situation and Trend report focused on Nistria. It is imperative that you familiarize yourself with the contents of these documents.

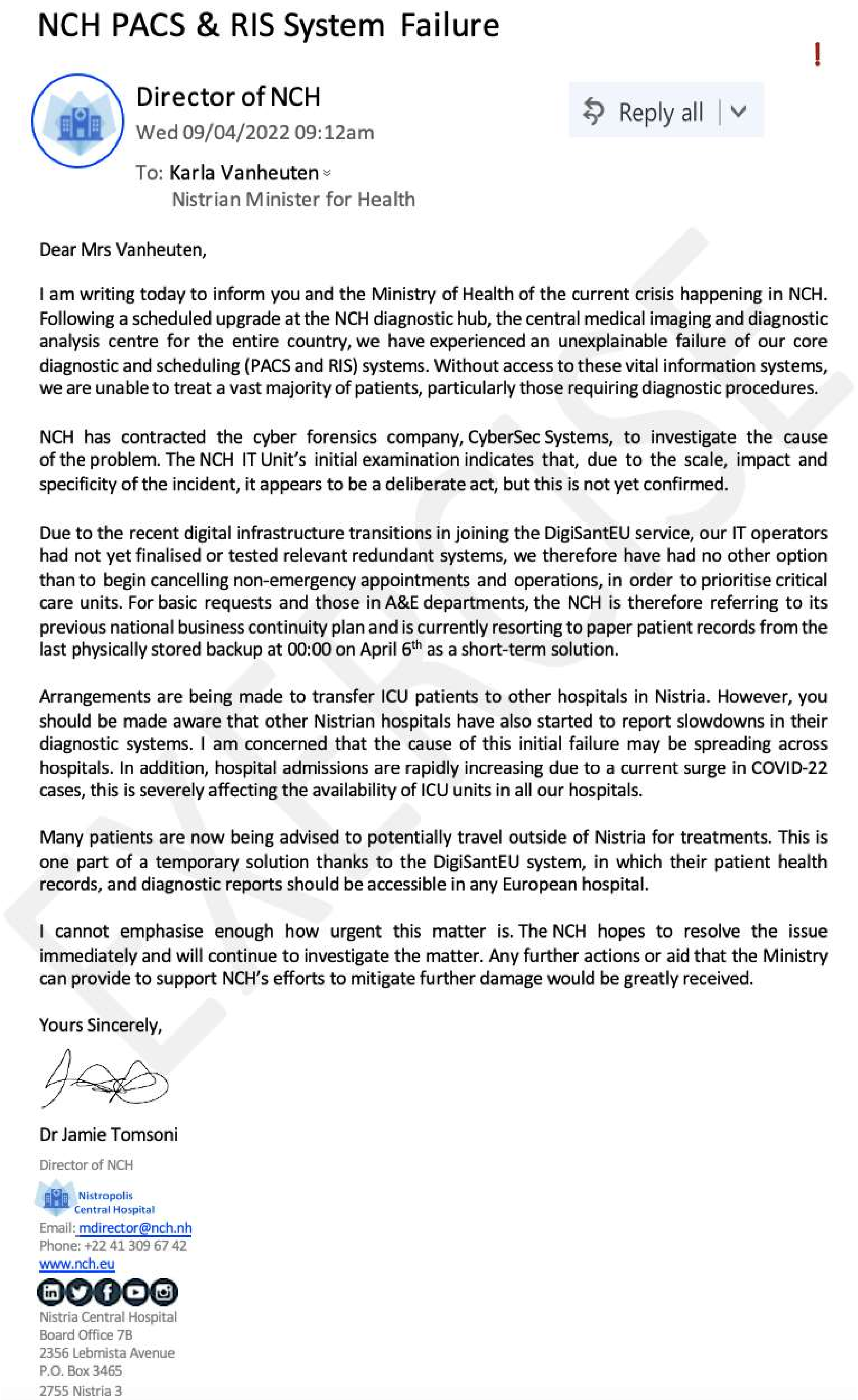
You are hereby tasked with analysing these documents thoroughly. Your expertise and insights will be invaluable in addressing the situation effectively. We kindly request your presence at the Headquarters of the Political and Security Committee, located at the Faculty of Law, Masaryk University, on May 15th, at no later than 13:55. The meeting will take place in rooms 034 and 030. You will find the necessary contact information in the interactive syllabus and the shared folder.

Your contribution to this endeavour is greatly appreciated. Together, we can work towards mitigating the incident and ensuring the stability of the region.

Best regards,

Jakob von Stoupalburg
Vice-president
Political and Security Committee of the European Union

Council of the EU
Rue de la Loi/Wetstraat 175
B-1048 Bruxelles/Brussel
Belgique/België
Tel: +32 22816111
www.consilium.europa.eu



NCH PACS & RIS System Failure

!

Director of NCH
Wed 09/04/2022 09:12am

To: Karla Vanheuten
Nistrian Minister for Health

Dear Mrs Vanheuten,

I am writing today to inform you and the Ministry of Health of the current crisis happening in NCH. Following a scheduled upgrade at the NCH diagnostic hub, the central medical imaging and diagnostic analysis centre for the entire country, we have experienced an unexplainable failure of our core diagnostic and scheduling (PACS and RIS) systems. Without access to these vital information systems, we are unable to treat a vast majority of patients, particularly those requiring diagnostic procedures.

NCH has contracted the cyber forensics company, CyberSec Systems, to investigate the cause of the problem. The NCH IT Unit's initial examination indicates that, due to the scale, impact and specificity of the incident, it appears to be a deliberate act, but this is not yet confirmed.

Due to the recent digital infrastructure transitions in joining the DigiSantEU service, our IT operators had not yet finalised or tested relevant redundant systems, we therefore have had no other option than to begin cancelling non-emergency appointments and operations, in order to prioritise critical care units. For basic requests and those in A&E departments, the NCH is therefore referring to its previous national business continuity plan and is currently resorting to paper patient records from the last physically stored backup at 00:00 on April 6th as a short-term solution.

Arrangements are being made to transfer ICU patients to other hospitals in Nistria. However, you should be made aware that other Nistrian hospitals have also started to report slowdowns in their diagnostic systems. I am concerned that the cause of this initial failure may be spreading across hospitals. In addition, hospital admissions are rapidly increasing due to a current surge in COVID-22 cases, this is severely affecting the availability of ICU units in all our hospitals.

Many patients are now being advised to potentially travel outside of Nistria for treatments. This is one part of a temporary solution thanks to the DigiSantEU system, in which their patient health records, and diagnostic reports should be accessible in any European hospital.

I cannot emphasise enough how urgent this matter is. The NCH hopes to resolve the issue immediately and will continue to investigate the matter. Any further actions or aid that the Ministry can provide to support NCH's efforts to mitigate further damage would be greatly received.

Yours Sincerely,

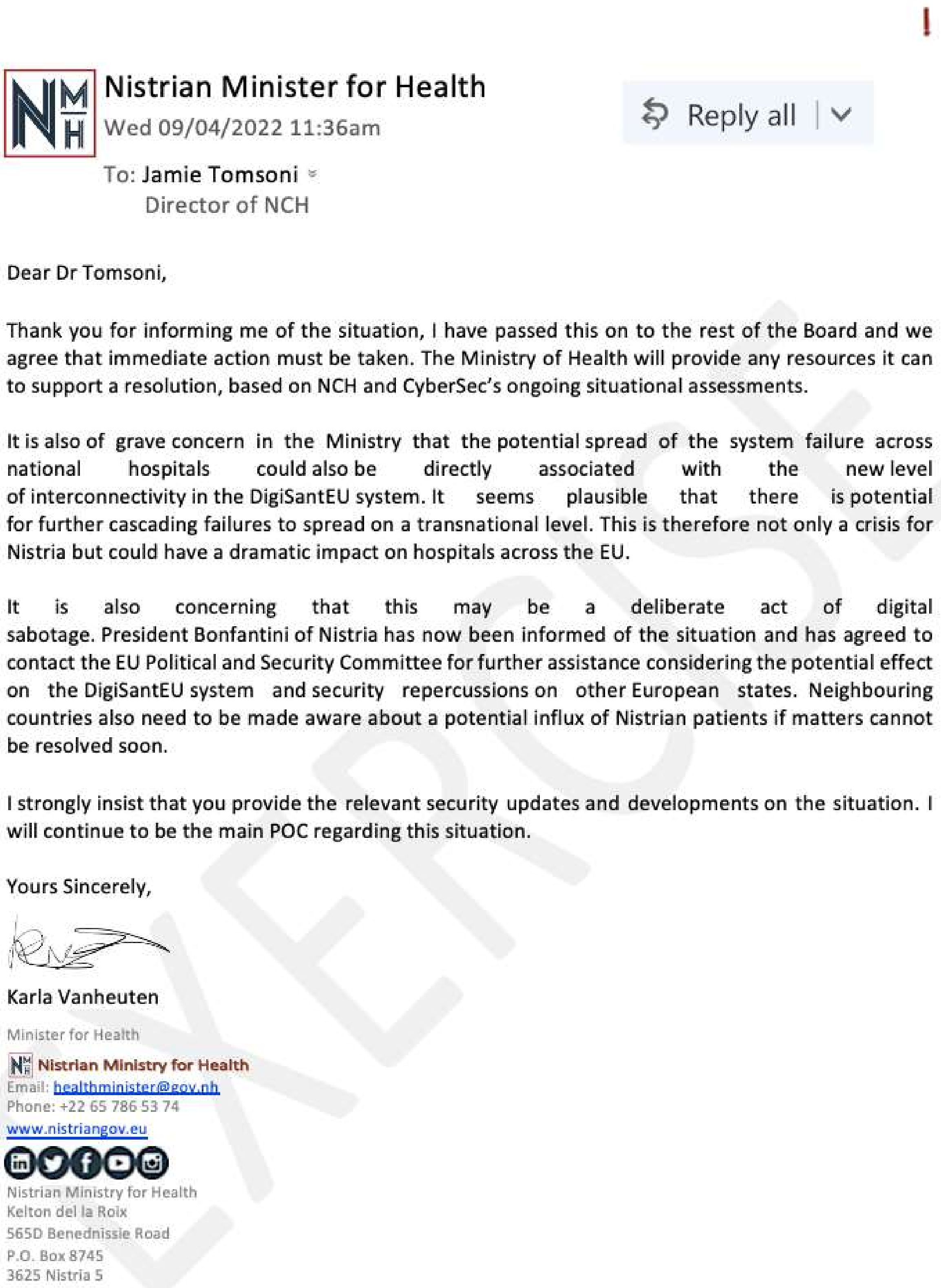
Dr Jamie Tomsoni

Director of NCH

Nistropolis
Central Hospital

Email: mdirector@nch.nh
Phone: +22 41 309 67 42
www.nch.eu

Nistria Central Hospital
Board Office 7B
2356 Lebmista Avenue
P.O. Box 3465
2755 Nistria 3



Nistrian Minister for Health
Wed 09/04/2022 11:36am

To: Jamie Tomsoni
Director of NCH

Dear Dr Tomsoni,

Thank you for informing me of the situation, I have passed this on to the rest of the Board and we agree that immediate action must be taken. The Ministry of Health will provide any resources it can to support a resolution, based on NCH and CyberSec's ongoing situational assessments.

It is also of grave concern in the Ministry that the potential spread of the system failure across national hospitals could also be directly associated with the new level of interconnectivity in the DigiSantEU system. It seems plausible that there is potential for further cascading failures to spread on a transnational level. This is therefore not only a crisis for Nistria but could have a dramatic impact on hospitals across the EU.

It is also concerning that this may be a deliberate act of digital sabotage. President Bonfantini of Nistria has now been informed of the situation and has agreed to contact the EU Political and Security Committee for further assistance considering the potential effect on the DigiSantEU system and security repercussions on other European states. Neighbouring countries also need to be made aware about a potential influx of Nistrian patients if matters cannot be resolved soon.

I strongly insist that you provide the relevant security updates and developments on the situation. I will continue to be the main POC regarding this situation.

Yours Sincerely,

Karla Vanheuten

Minister for Health

Nistrian Ministry for Health
Email: healthminister@gov.nh
Phone: +22 65 786 53 74
www.nistriangov.eu

Nistrian Ministry for Health
Kelton del la Roix
565D Benednissie Road
P.O. Box 8745
3625 Nistria 5

CyberSec Systems Investigation and Situational Report on NCH Systems Failure

To: Jamie Tomsoni – Director of NCH

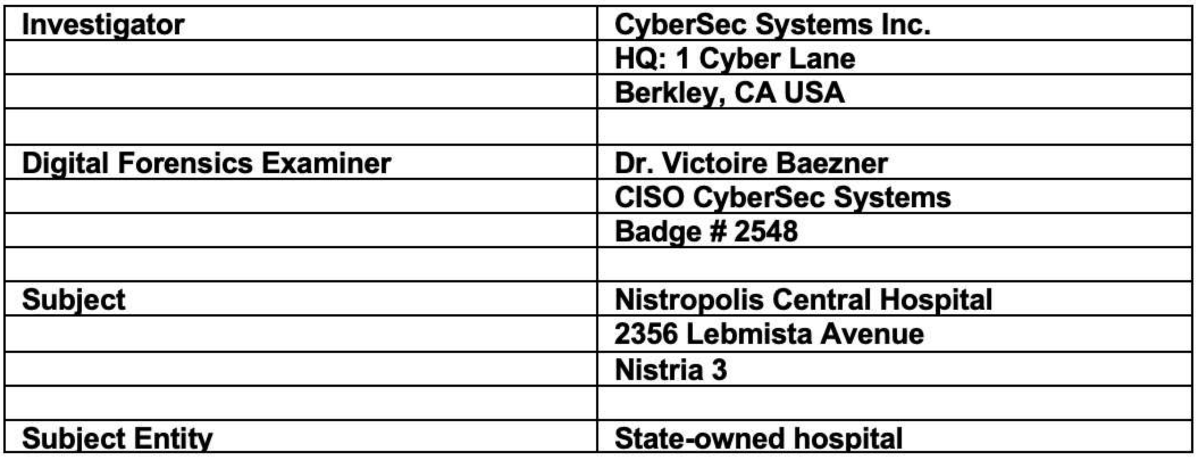
From: Dr. Victoire Baezner

cc: Karla Vanheuten – Minister for Health, Republic of Nistria

Date: April 12th 2022, 08:00

Re: Digital Forensic Examination of NCH System Failures

CONFIDENTIAL REPORT TO NCH EXECUITVES



Investigator	**CyberSec Systems Inc.**
	HQ: 1 Cyber Lane
	Berkley, CA USA
Digital Forensics Examiner	**Dr. Victoire Baezner**
	CISO CyberSec Systems
	Badge # 2548
Subject	**Nistropolis Central Hospital**
	2356 Lebmista Avenue
	Nistria 3
Subject Entity	**State-owned hospital**

Key Terminology:

The terms defined in this section are used throughout the remainder of this document.

- **CyberSec Systems:** Digital forensics and cyber security specialists that provide support and produce situational reports examining the totality of incidents including but not limited to physical impacts and advanced digital forensic analysis.
- **Digital Evidence Specialist:** CyberSec Systems staff with specialized technical expertise to perform digital forensic investigations.
- **Digital Forensics:** The application of digital investigation and analysis techniques to perform a structured examination of a digital storage medium, whilst maintaining a documented chain of evidence, for the purpose of gathering information admissible in evidence in a court of law.

- **Forensics Laboratory:** Isolated, protected offices with restricted access, where digital forensic evidence and work files are stored under a dedicated forensic network.
- **Intrusion Detection System (IDS):** Reports to a central security and control system, detecting suspicious network activity or system threats before they become actual breaches.
- **Hash Value:** A digital fingerprint of the data which helps to verify the integrity of the investigation evidence. It is a fixed length computational result generated from a string of data (e.g. files, directories, an entire hard disk) using a specific mathematical algorithm that creates a unique value.

SUBJECT: System Failures at Nistropolis Central Hospital (NCH)

This report was requested by the Director of Nistropolis Central Hospital following the system failure that took place on the 8th April 2022. As part of the NCH's incident response, CyberSec Systems has been contracted to identify the source of the failure and how the situation transgressed. CyberSec Systems was commissioned and given authority to conduct this digital forensic investigation in a manner that ensures the integrity of the chain of evidence to be admissible in administrative, disciplinary and judicial procedures.

Our investigators were authorised to operate under accordance of Article 4(2) of Regulation (EC) 883/2013, Article 7(1) of Regulation (EC) 2185/96 and Article 103 of Regulation (EU) 2017/745. Due to the large volume of data collected and stored for the purposes of this investigation (including but not limited to personal information), all procedures were conducted in compliance with the GDPR. All data of potential relevance to the investigation was requested, collected and stored within CyberSec Systems' secure forensics laboratory.

Following a three-day investigation, this report provides a preliminary situational report, the forensic analysis findings and scope for further investigation by the CyberSec Systems digital forensics team, led by Dr Victoire Baezner.

Key Findings

- Upgraded diagnostic software has been identified as the digital asset compromised.
- The compromised software led to the system overloading of the picture archiving and communications systems (PACS), which later contributed to the system failure of the central radiology information systems (RIS) scheduling software.
- System failures primarily originated in the NCH's diagnostics laboratory and started to show an impact after the scheduled system upgrades.
- The interconnectivity of systems and analogous software in all Nistrian hospitals suggests the cause of the NCH system slowdowns could also be the cause of increasing diagnostic PACS delays in the additional four main Nistrian hospitals.
- The hallmarks, scale, sophistication and impact of the incident suggests this could have been a deliberately instigated operation targeting upgraded diagnostic software, but this is not yet confirmed.

Situational Report

The situation was reported as follows:

1.1 In accordance with EU membership requirements, Nistrian hospitals were due to complete the final digital service infrastructure upgrades to comply with DigiSantEU service regulations. Whilst already using and connected to DigiSantEU systems since major installations in March 2022, the final stage of this process was the upgrading of diagnostic equipment at Nistria's central diagnostic hub, located at Nistropolis Central Hospital.

1.2 Three upgrades were scheduled to take place: two software and one hardware. The hardware upgrade included DigiSantEU required equipment developed by Simpworth Technology, a specialist medical imaging hardware manufacturer. These upgrades took place at 02:00 April 6th, 2022. This time was chosen to minimize the impact on healthcare provision at NCH. The installation and upgrades took three hours to complete.

2.1 At 11:00 on April 7th, NCH diagnostic staff began reporting severe delays in using the PACS software. Investigations into this revealed that the processing and retrieval of medical images and diagnostic results was running at less than 25% capacity. This resulted in a small backlog of requests. Still operating at a manageable rate, there was no urgency to immediately resolve the issue. However, as per NCH protocol, hospital IT operators were alerted to the situation and tasked with further observation and analysis.

2.2 At 19:00 on April 7th, the slowdown had still not been resolved. The hospital IT technicians could not find any clear issue with the systems or networks and could not trace the origin of the system slowdown.

2.3 During this time, the reduced capacity PACS server continued to accumulate a backlog of requests, which increased due to a sudden spike in Covid-22 related hospital admissions. At 09:32 on April 8th, the diagnostics hub exceeded its manageable capacity and the system became overloaded. This congestion spilled over to the connected RIS scheduling system causing a cascading backlog and system freeze, meaning healthcare providers at the NCH could no longer retrieve patient health records, access diagnostic imagery and results or the scheduling system.

2.4 By the evening of April 8th, operators of the other four main Nistropolis hospitals began reporting diagnostic (PACS) system slowdowns.

2.5 The Head of IT at NCH released a statement that evening voicing his belief that "these failings are the cause of an unidentified malware that is affecting the processing of systems and causing them to shutdown". The Head of IT also disclosed that they have so far been unable to effectively recover from the incident.

2.6 At 21:00 on April 8th, the Director of NCH made a formal announcement that the NCH would now have to delay or cancel a range of non-emergency procedures and operations and would have to drastically reduce new admissions without access to patient information or functioning diagnostic tools.

2.7 At 7:00 on April 9th CyberSec Systems were contacted by the Director of NCH and an in-depth digital forensic investigation began. The complete analysis took three days; all findings, procedures and conclusions have been compiled within this report.

3.1 The NCH does not currently know the financial costs of the system failures. Costs may include cancelled appointments, additional IT support provided by external bodies/IT consultants and the potential cost of restoring data and the systems affected.

Forensic Analysis

The digital forensics team was able to confirm this situation of events following analysis of the systems generated logs and update records. Upon further analysis, the CyberSec Systems team, led by Dr. Victoire Baezner, were able to narrow the cause of the failure further.

1.1 A diagnostic analysis shows that the core system failure originated in the NCH diagnostic laboratory.

1.2 One of the diagnostic software assets upgraded in the NCH diagnostic laboratory appeared to have been severely compromised and corrupted resulting in the following process:

- The software issue prevented the PACS and RIS from effectively communicating, resulting in a cumulative backlog of PACS requests that were unable to be processed;
- As further requests came through the RIS, this gradually resulted in the slowdown of PACS processing capacity to 25%;
- Requests increased at an exponential rate, particularly in response to a spike in COVID-22 related hospital admissions;
- As requests exceeded software capacity, PACS was not able to process further requests. This systematically impacted the RIS management system, causing a cascading stall of software systems;
- This is known as a "freezing by heating" effect, in which the RIS software could not function properly due to being overloaded by the continuous accumulation and backlog of requests for access and information.

1.3 The crippling of this single digital asset has created a cascading failure.

2.1 Upon further analysis, specific hallmarks were identified that suggest this could have been an intentional malicious act, with similar effects to a distributed denial of service (DDoS) operation:

- The damage to the PACS and RIS is so localised and precise that only a highly effective, custom-designed form of malware would have the ability to cause such devastating yet specific damage;
- The highly specific nature and targeted focus of the damage done suggests, if a deliberate act, the potential perpetrator had previous knowledge and intelligence of the systems;
- If a deliberate act, it is possible that the perpetrator had physical or networking access to the PACS server;
- There is no evidence yet to suggest personal data was stolen, however files may have been compromised. It suggests, if a deliberate act, it was intended to cause maximum damage rather than other means such as IP and data theft.

2.2 CyberSec Systems is yet to identify and confirm the presence of malware or deliberate manipulation; investigations are continuing. However, upon forensic examination of the corrupted software it can be noted that:

- Traces of code similar to that used in the 2020 theft of Nistron NH700 FOLD proprietary intellectual property have been identified;
- The NCH's Intrusion Detection System (IDS) did not pick up on any presence of malware or a potential threat in the system suggesting an ability to bypass this protection;
  - These signature-based detection systems can normally identify specific patterns, such as byte sequences in network traffic or malicious intrusion sequences used by malware.
- The results therefore remain inconclusive at this stage.

3.1 Whilst not evidenced in this case, successful infiltration *could* have occurred due to three circumstances:

1. The IDS was outdated, hence malicious code could have evaded detection;
2. Fragmentation and pattern changing evasion could have been used to confuse the transmission control protocol stream of the IDS system. Sophisticated operations can use unknown patterns to evade detection.
3. Encrypted packets of data could not be processed by the hospitals IDS allowing the malware to encrypt the content of the system hard drive. This could have allowed an unauthorized user to gain access to the local network and manipulate the traffic between the PACS and RIS software.

3.2 Evidence Hash → NCH Evidence Items

Below is a detailed log of evidence collected, used and stored for the purposes of this investigation:

Evidence Item	MD5	SHA-1	PATH
PACS Server	fc953eee9 1202475bc fd0394db3 a4459	3636065198ae98a5c34de78ec8301dd7ca4f3e1b	\\.\PHYSICALDRIVE2\BOOTCAMP (3) [43488MB]\NONAME [NTFS]\[root]\[unallocated space]\15025
PACS Osirix DICOM	cb3f67aa7 46b7ddd9a 3c875fe79 cf665	88c4917c7f23ce0bcc0c1e 7e1bdedd4f86ba95e	\\.\PHYSICALDRIVE2\BOOTCAMP (3) [43488MB]\NONAME [NTFS]\ [unallocated space]\15027
PACS Osirix GUI	83194778a 6f2f94df16 5bde3ca3f aac2	ce4cba3f5d4cec71aa2bd9 ab21565ac772f9e6b5	\\.\PHYSICALDRIVE2\BOOTCAMP (3) [43488MB]\NONAME [NTFS]\[root]\ [unallocated space]\15028
PACS Osirix MD	9e27d910d 88b4bf6c0 ba5a20b25 7e26	3f47df5e2a4d3bd4418b16 4186b0c6b6e9297d1	\\.\PHYSICALDRIVE2\BOOTCAMP (3) [43488MB]\NONAME [NTFS]\[root]\ [unallocated space]\15029
DICOM C-Store	5664dsa65 9ad6s3c66 s66f6wrg f6gery	48965ssdf6sr2c6s5f1dsf58 sw54r4f45w5s1s77e	\\.\PHYSICALDRIVE3\GRIDWEB (2) [15568MB]\NONAME [SYS5]\[unallocated space]\17021
DICOM Node	4orps6d 3srt6fd2r2r5g 5ddsf5 51r4e786	5e6r366er2r5958486a19r6 e5w2a1r4241qr56q8	\\.\PHYSICALDRIVE3\GRIDWEB (2) [15568MB]\NONAME [SYS5]\[unallocated space]\17022

RIS Server	1479r6f5e 8r98t5d2r8f fsgt5t77/ d8ftw0	615a51a5r4d2r2a86e518 ds45r5r1s5a65r5a1d5	\\.\PHYSICALDRIVE1\Partition 1 [960MB]\NONAME [FIT32]\[unallocated space]\17082
RIS Clients	9e2e886 wr5w5e6f58w d5r8f4d dsafdae5	6a8784654r5a6rt4655tw 1 s5rt8522864sr531e	\\.\PHYSICALDRIVE1\Partition 1 [960MB]\NONAME [FIT32]\[unallocated space]\17083
OpenRIMS API	2e89t5e45 5r56t3r68tt 8e4t1t8w5 5r5t8	878rs5f1g565yr5a61d51 c5 r5t6a8rat566s4886s	\\.\PHYSICALDRIVE1\Partition 1 [960MB]\NONAME[FIT32]\[unallocated space]\17084
Unix ODBC	7er8t2s52 f14r4t8g4e4 tdfg4485 fdfgsr5	987865dsatrta56dfa4555 4 5s6t48r964strt45a4	\\.\PHYSICALDRIVE3\GRIDWEB (2) [15568MB]\NONAME [SYS5]\[unallocated space]\17023
ODBC Link	383uerwe sk7349dkwo 39kfk9w 4nnsk8	564357484ad5ta54r5t44 86 8a6r7t86a51r65e4r5	\\.\PHYSICALDRIVE3\GRIDWEB (2) [15568MB]\NONAME [SYS5]\[unallocated space]\17024

Future of the Investigation

CyberSec Systems is continuing to work with the Nistrian authorities and its arm's length bodies to monitor and track any changes in NCH systems. Specialised efforts will be focused on further investigations seeking to determine whether the PACS and RIS failures were caused by a specialised type of malware, and establish joint efforts with the criminal investigation team if malicious intentions are further suspected. Depending on the NCH's assessment of this forensic examination, the investigation may be escalated to national security bodies.

Addendum to the report

This information has been provided to the Director of the NCH and relevant Nistrian governing bodies. These details are provided in this report as preliminary information only; further investigation into the system failure is required and is underway.

At this point in time, the issue has not been operationally addressed. Therefore, it is highly recommended that relevant ICT security mechanisms take place to mitigate any further impact on the current systems affected as well as any connected systems. Investigations will continue into the specific cause of the system failures.

Appendix 2[2]

TE SAT

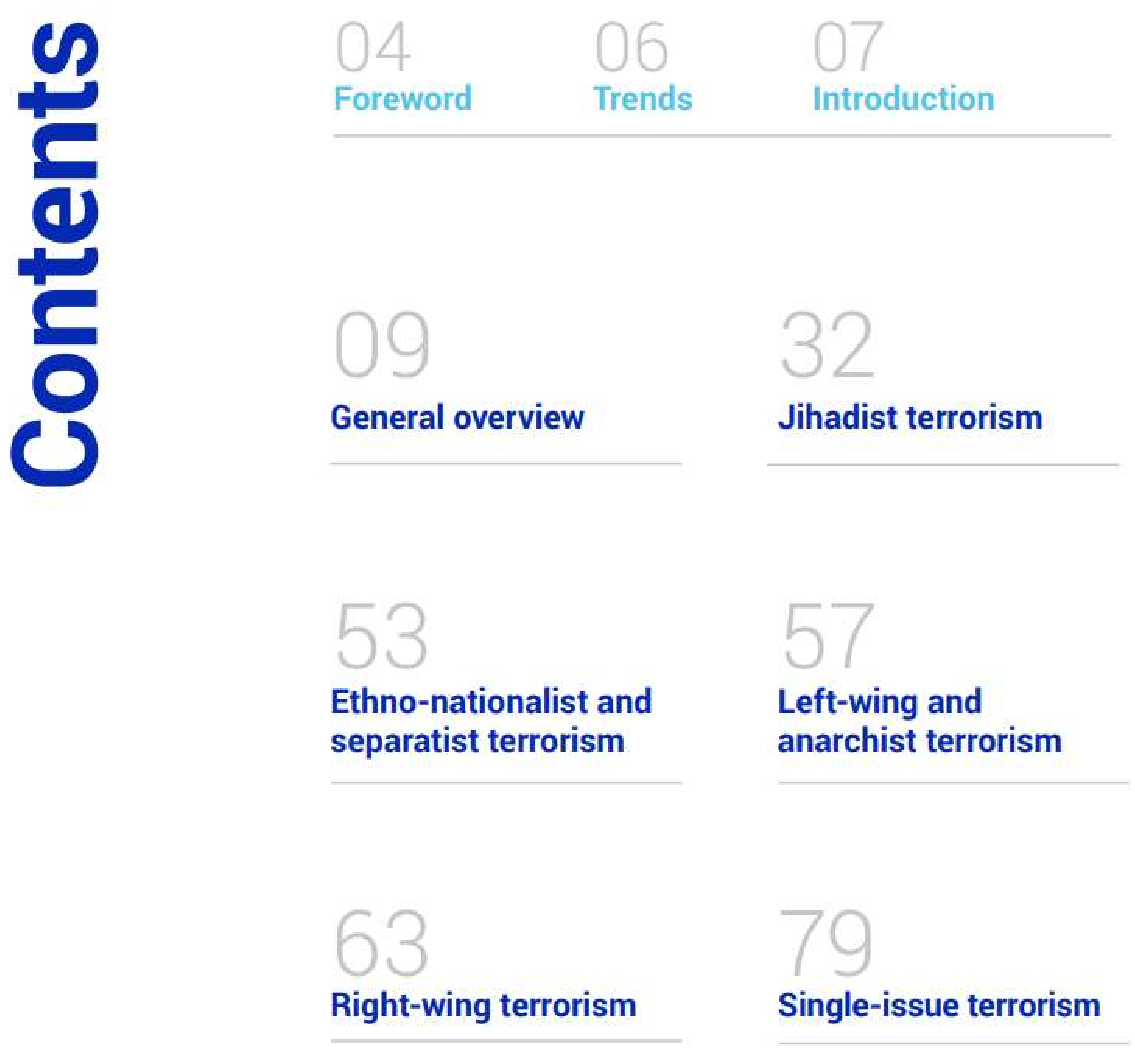
European Union

Terrorism Situation and Trend report

MAY 2022

EUROPOL

[2] Although this report is entirely *fictional,* visuals and content have been drawn from the 2020 Europol TE-SAT Report.



Contents

07 Introduction

The European Union (EU) Terrorism Situation and Trend Report (TE-SAT) 2022 seeks to record basic facts and assemble figures regarding all terrorist attacks and arrests in the EU in the past year April 2021- April 2022.

The shared legal framework created by the EU Directive 2017/541 makes comparing data relating to terrorism from different EU Member States meaningful. On this basis, the TE-SAT provides statistical data on terrorism in EU Member States. On a national level, terrorism legislation varies within the limits set by this Directive, as EU Member States retain flexibility when legislating.

The TE-SAT reflects EU Member States' definitions of terrorist offences according to national legislation. In addition, the TE-SAT mentions specific violent extremist acts and activities, as reported by EU Member States, to provide a more comprehensive picture of the situation. Whereas there is no universally agreed definition of extremism, extremists generally aim to replace the liberal democratic order and alter the fundamental constitutional principles linked to it. Terrorism, therefore, can be considered to be a set of violent tactics employed mainly by extremists.

Terrorism and extremism

In practice, acts which amount to terrorism under national legislation in one EU Member State might not have crossed this line in another. It can be difficult to draw clear distinctions between terrorism and other forms of extremist violence.

The TE-SAT does not require EU Member States to systematically report incidents of violent extremism that are not categorised as terrorism under national law. However, the TE-SAT mentions specific violent extremist acts and activities as reported by EU Member States, when these aim to intimidate a population or compel a government or have the potential to seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country. However, these incidents are not considered in the statistical data on terrorism in this report, which exclusively reflects incidents reported as terrorism by EU Member States.

Not all forms of extremism sanction the use of violence. The TE-SAT refers to non-violent forms of extremism, in particular ideologies inciting hatred of specific groups or populations, as reported by EU Member States, in case these have the potential of inciting acts of terrorism or violent extremism.

Despite the common legal framework embodied by EU Directive 2017/541, discrepancies between what constitutes terrorism persist among EU Member States. The TE-SAT serves as a testimony to these variations. At the same time, the report shows that all EU Member States face similar challenges in defining the line between violent behaviour and terrorism--for example, the role of mental conditions or the role of incitement of lone actor terrorism. Increased law enforcement cooperation and harmonisation of terrorism legislation and jurisprudence among EU Member States will contribute to consolidating the EU's area of freedom, security and justice.

79 Single-issue Terrorism

Single-issue terrorism defined

Single-issue extremist and terrorist groups use criminal means to change a specific policy or practice, as opposed to replacing the entire political, social and economic system in a society. The groups within this category are concerned, for example, with animal rights, environmental protection or anti-abortion campaigns. Examples of groups in this category are the Earth Liberation Front (ELF) and the Animal Liberation Front (ALF).

KEY FINDINGS

› EU Member States thwarted three plots classified single-issue terrorism in 2021.

› Single-issue activists continued to pose a limited threat to public order. Most actions were non-violent.

Single-issue activists continued to pose a limited threat to public order, and most of their actions were non-violent. Their activities included largely peaceful protests, blockades, demonstrations, rallies and camps, in which they advocated for actions against climate change and the protection of animal rights. EU Member States reported a limited number of vandalism cases targeting businesses related to the meat and fur industries.

Single-issue extremist activity by Member State

⇒ **Austria**

⇒ **Belgium**

⇒ **Bulgaria**

⇒ **Croatia**

⇒ **Republic of Cyprus**

⇒ **Czech Republic**

⇒ **Denmark**

⇒ **Estonia**

⇒ **Finland**

⇒ **France**

⇓ **Nistria**

⇒ **Germany**

⇒ **Greece**

⇒ **Hungary**

⇒ **Ireland**

⇒ **Italy**

⇒ **Latvia**

⇒ **Lithuania**

⇒ **Luxembourg**

⇒ **Malta**

⇒ **Netherlands**

In 2018 the paramilitary ecowarrior group 'EcoEarthNow!' was proscribed as an extremist group by the Nistrian government, following reports that law enforcement agents had thwarted a plot to target an unspecified national infrastructure by EcoEarthNow! members.

The group was established in Mustelus in 2015 made up of majority Mustelan paramilitary nationals. To date, many ethnic Mustelans living in Nistria are now reported as heavily involved in the group's activities by the Nistrian government, with some key leaders identified as Nistrian nationals or ethnic Mustelans residing in Nistria. The group's activities have primarily been recorded as non-violent public protests and social media campaigns motivated by the goal of eliminating fossil fuel use across the world.

To date, no other Member State has listed the group as an 'extremist' threat. Many Member States however, have reported their presence at peaceful climate-based protests in their countries. Their presence has also been confirmed outside of the EU, particularly in Mustelus. Mustelus and Nistria act as core EcoEarthNow! membership bases to both plan activities and target institutions and governments, including through online campaigns.

Nistria has been a particular target, as a neighbouring country to Mustelus, due to the current government's approach towards climate change and the use of fossil fuels. As a self-defined paramilitary and 'ecowarrior' group, the threat deemed by Nistria was enough to warrant national monitoring of the group in 2016, with subsequent proscribing of the group as 'extremist' in 2018.

The group has been identified as both militarily and technologically advanced, whilst still utilising more traditional forms of action such as public protests to attract a wider support network.

In 2020, the Nistrian government alleged that a senior EcoEarthNow! leader was a prime suspect of the attempted NH7000 FOLD hack of the state-owned mobile phone brand Nistron. As a Mustelan national residing in Mustelus (a non-EU state) however, Mustelan officials refused to carry out the requested extradition or prosecution processes again the EcoEarthNow! leader.

Since 2016 the Mustelan government has not reciprocated Nistria's requests to monitor the group's activities in their home country. Nistria however, has continued to monitor the activities of members located in Nistria. A high proportion of Nistrian-based members are believed to also identify as Royalists that voted against Nistrian independence from Mustelus in 2013.

Europol has recently confirmed that in early April 2022, the group EcoEarthNow! made substantial online threats towards the Nistrian government on a social media feed. The content, posted by identified leaders of the group, made strong insinuations that if the Nistrian government did not change the nation's plan to reopen four coal-fired power stations across the country, that the group would 'target' one of four critical national infrastructures in Nistria, citing transport, communications, finance or health services. The group's capabilities to execute this type of threat is yet to be verified. The content was later removed from the online platform at the request of the Nistrian government.

The public posts reached a wide audience before their removal. The removal instigated further online campaigns that resulted in the organisation of anti-government protests on 14th-15th April 2022 in the Nistrian capital. The makeup of the crowd was believed to be both EcoEarthNow! representatives and supporters, as well as Royalist group members promoting an anti-government agenda. The Government made no formal response.

No other Member States have encountered such level of activity and have referred to EcoEarthNow! as an environmental activist group only.

⇒ **Poland**

⇒ **Portugal**

⇒ **Romania**

⇒ **Slovakia**

⇒ **Slovenia**

⇒ **Spain**

⇒ **Sweden**