TERROR
Strengthened preparedness and response
to biological and chemical terror attacks

Co-funded by
the Health Programme
of the European Union

Attributes/requirements description of a tangible secure platform for rapid exchange information between sectors.

DELIVERABLE 7.2

This report arises from the TERROR Joint Action, which has received funding from the European Union through the European Health and Digital Executive Agency of the European Commission, in the framework of the Third Health Programme 2014-2020. The European Commission is not responsible for the content of this report. The sole responsibility for the report lies with the authors, and the European Health and Digital Executive Agency is not responsible for any use that may be made of the information contained herein. The authors are not responsible for any further and future use of the report by third parties and third-party translations

Author(s):	Lead author: Stamatis Parissis Co-authors: Dr. Dimitrios Iliopoulos
Date:	04/08/2024
Version History:	Version number 1, 04/08/2024, draft Version number2, 06/05/2024, draft Version number3, 07/22/2024, draft

Project details

Project short name:	JA TERROR
Project full name:	JA TERROR – Strengthened preparedness and response to biological and chemical terror attacks
Grant Agreement no :	101003855
Project duration:	48 months
Project timeframe:	1/1/20 – 12/31/24
Coordinators:	Bengt Skotheim, Bjørn Jarle Wiger

Title:	Attributes/requirements description of a tangible secure platform for rapid information exchange between sectors
Work Package :	WP7
Date of Document	04/08/2024
Reviewing partner:	All

Document details

Status of the Document:	Draft
Dissemination level:	Public

Document history

Revision:	Date	Description
1	04/08/2024	1st Draft
2	06/05/2024	2nd Draft
3	07/22/2024	3rd Draft

List of partners

Partner no	Acronym	Full Name	Country	WP7 Effort
1	HDIR	HELSEDIREKTORATET	Norway	7,2
2	NIPH	FOLKEHELSEINSTITUTTET	Norway	5,04
3	MCA	MINISTRY OF CIVIL AFFAIRS AFFAIRS	Bosnia and Herzegovina	1,08
4	PHI-FBiH	ZAVOD ZA JAVNO ZDRAVSTVO FEDERACIJEBOSNE I HERCEGOVINE	Bosnia and Herzegovina	7,2
5	MoS-BiH	MINISTRY OF SECURITY OF BOSNIA AND HERZEGOVINA	Bosnia and Herzegovina	3,6
6	CIPH	HRVATSKI ZAVOD ZA JAVNO ZDRAVSTVO	Croatia	1,87
7	EODY	National Public Health Organisation	Greece	56,16

8	NNK	NEMZETI NEPEGESZSEGUGYI KOZPONT	Hungary	1,8
9	NIJZ	NACIONALNI INSTITUT ZA JAVNO ZDRAVJE	Slovenia	9,36
10	MoH-ES	MINISTERIO DE SANIDAD	Spain	1,8
11	MoH-MT	Ministry for Health - Government of Malta	Malta	0,9
12	IPHS	INSTITUT ZA ZASTITU ZDRAVLJA SRBIJEDR MILAN JOVANOVIC BATUT	Serbia	10,8

Contents

List of tables

List of figures

Abbreviations

Acronym	Definition
S.I.E.P	Secure Information Exchange Platform
AES	Advanced Encryption Standard
SSL	Secure Socket Layer
TLS	Transport Layer Security
HTTPS	Hypertext Transfer Protocol Secure
CCTV	Closed Circuit Television
GA	Grant Agreement
CORDIS	Community Research and Development Information Service
VPN	Virtual Private Network
MFA	Multi Factor Authentication
IP	Internet Protocol
TCP	Transmission Communication Protocol
WP	Work Package

Executive summary

The purpose of this deliverable (D.7.2.) is to provide a detailed technical document describing all the necessary actions and studies should be taken in mind in order to build a successful Secure Information Exchange Platform (S.I.E.P.) tailored to information exchange needs in case of biological/chemical terror attack. The development of this deliverable focused on satisfying all the necessary requirements based on Grant Agreement in order not only to avoid conflict with other projects but also to provide a complete technique/algorithm to create such a demanding platform. The procedure involved research on the internet and literature to detect if other projects have managed to produce similar outcomes. Also special attention was given on Impress , Proactive and other similar projects and programs in order to avoid duplication. Input from WP4, WP5, WP6, has been reviewed and added accordingly.

After close investigation of all above main input channels WP7 team proceeded to next step determining the basic elements every Secure Information Exchange Platform should include (for example: Encryption, Authentication Mechanisms, Backup Mechanisms and so on.) Lastly combining all previous outcomes WP7 team concluded and finally produced the main outcomes D.7.2 should provide determining the most critical and vital elements such a platform tailored specific to Biological and Chemical Terror Attacks should include like Sentiment Analysis, Safety of Communication Channels, Remote Endpoint Users Connection Protocol and Geolocation Services.

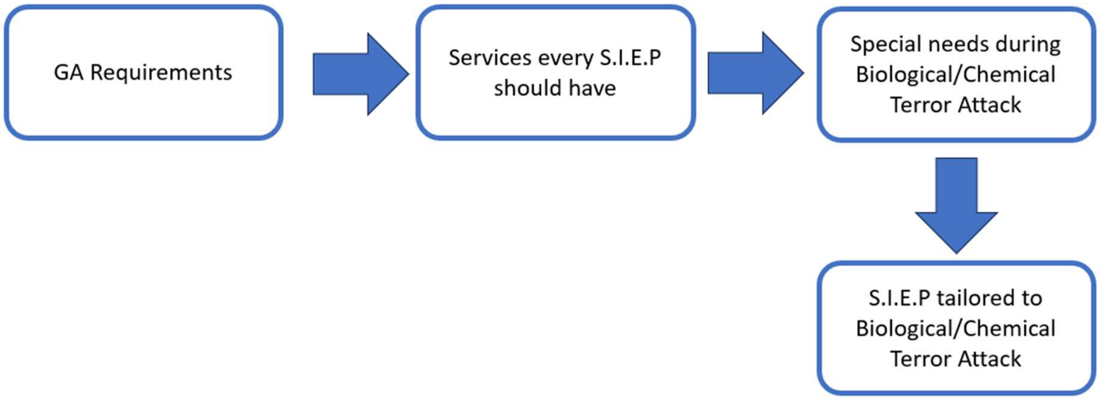

GA Requirements
Services every S.I.E.P should have
Special needs during Biological/Chemical Terror Attack
S.I.E.P tailored to Biological/Chemical Terror Attack

Figure 1. **D.7.2 Production Algorithm**

1. Introduction

1.1 Project Summary

Joint Action Terror is a joint effort by health authorities in European countries to improve health preparedness and cross-sectoral cooperation in the event of a biological or chemical attack. The work of the Joint Action is devided in eight work packages. Four of them are core work packages: coordination, dissemination, evaluation and integration & sustainability and the rest of them are technical work packages addressing the following areas: preparedness and response planning, cross sectorial collaboration, risk and crisis communication and novel threats. In accordance to Grant Agreement one of the requested outcomes was the development of Deliverable 7.2, part of obligation tasks WP7.

1.2. Objectives of WP7

The specific objective of WP7 is to promote the implementation of Risk and Crisis Communication in all stages of risk management on both national and EU level.

The expected results of this Work Package are:

- Provide tools that all collaborating sectors will be able to use, to establish robust communication channels with each other and towards the public, in order to improve preparedness and response during Biological and Chemical terror attacks.

- Present legally and technically tangible solutions for unified platforms to rapidly exchange information between heterogeneous sectors, including potentially classified data.

- Partners, and Member States, will be able to use the experience of already applied community resiliency plans for other health threats and adapt them to the field of biological/chemical terrorist attacks.

1.3. Objectives of Deliverable D.7.2

Deliverable 7.2. is an integral part of the overall deliverables from WP7 with key objectives:

- Provide a technical document describing the attributes/requirements of a tangible secure platform that can be used to rapidly exchange information between sectors at both national and EU level.

- Feasibilty examination aspect linking systems for rapid notifications for law enforcement like SIENA (Europol) and EWRS (EU IHRNFPs).

1.4. Purpose of Deliverable D.7.2.

Technical description of attributes/requirements of tangible secure platform for rapid information exchange between sectors is the main output of D.7.2. While the deliverable focus on providing all the necessary details to fullfill his purpose during completion of all the required tasks to succesfully produce the requested outcome , it is important to note the weight given to AI integration, modular architecture proposed and remote endpoint communication protocol technology used (V.P.N)

1.5. Interaction with Other Work Packages

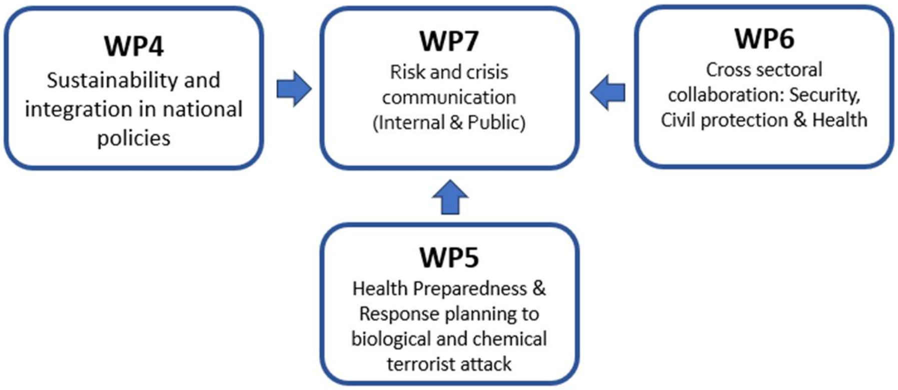

WP4
Sustainability and integration in national policies
WP7
Risk and crisis communication (Internal & Public)
WP6
Cross sectoral collaboration: Security, Civil protection & Health
WP5
Health Preparedness & Response planning to biological and chemical terrorist attack

Figure 2. **WP7 collaboration with other WP's of JA TERROR**

1.6. Methodology Followed to Produce D.7.2.

In accordance to Grant Agreement description the steps WP7 team should follow to complete successfully all the necessary requirements for producing Deliverable 7.2 are presented below.

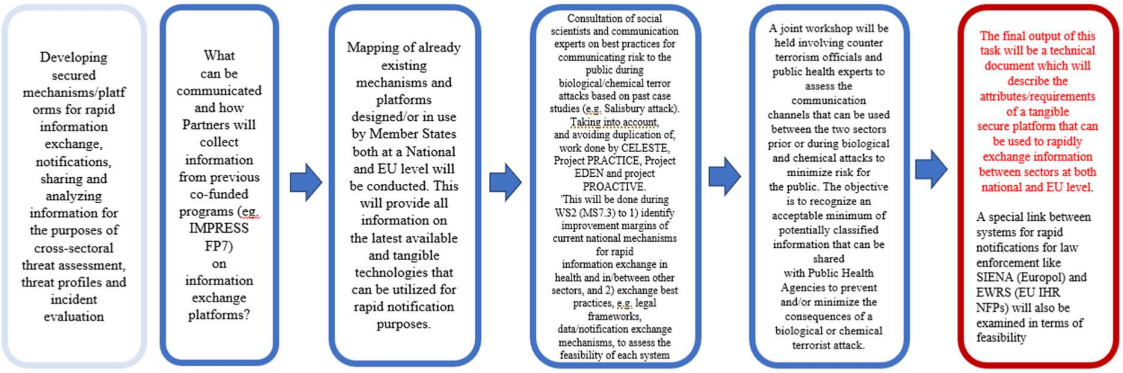

Developing secured mechanisms/platforms for rapid information exchange, notifications, sharing and analyzing information for the purposes of cross-sectoral threat assessment, threat profiles and incident evaluation
What can be communicated and how Partners will collect information from previous co-funded programs (eg. IMPRESS FP7) on information exchange platforms?
Mapping of already existing mechanisms and platforms designed/or in use by Member States both at a National and EU level will be conducted. This will provide all information on the latest available and tangible technologies that can be utilized for rapid notification purposes.
Consultation of social scientists and communication experts on best practices for communicating risk to the public during biological/chemical terror attacks based on past case studies (e.g. Salisbury attack). Taking into account, and avoiding duplication of, work done by CELESTE, Project PRACTICE, Project EDEN and project PROACTIVE. 'This will be done during WS2 (MS7.3) to 1) identify improvement margins of current national mechanisms for rapid information exchange in health and in/between other sectors, and 2) exchange best practices, e.g. legal frameworks, data/notification exchange mechanisms, to assess the feasibility of each system
A joint workshop will be held involving counter terrorism officials and public health experts to assess the communication channels that can be used between the two sectors prior or during biological and chemical attacks to minimize risk for the public. The objective is to recognize an acceptable minimum of potentially classified information that can be shared with Public Health Agencies to prevent and/or minimize the consequences of a biological or chemical terrorist attack.
The final output of this task will be a technical document which will describe the attributes/requirements of a tangible secure platform that can be used to rapidly exchange information between sectors at both national and EU level.
A special link between systems for rapid notifications for law enforcement like SIENA (Europol) and EWRS (EU IHR NFPs) will also be examined in terms of feasibility

Figure 3. **Requirements for Producing D.7.2. Based on GA**

After simplifying the described tasks, wp7 team concluded all the necessary steps need to be taken in order to satisfy all criteria and successfully produce D.7.2.:

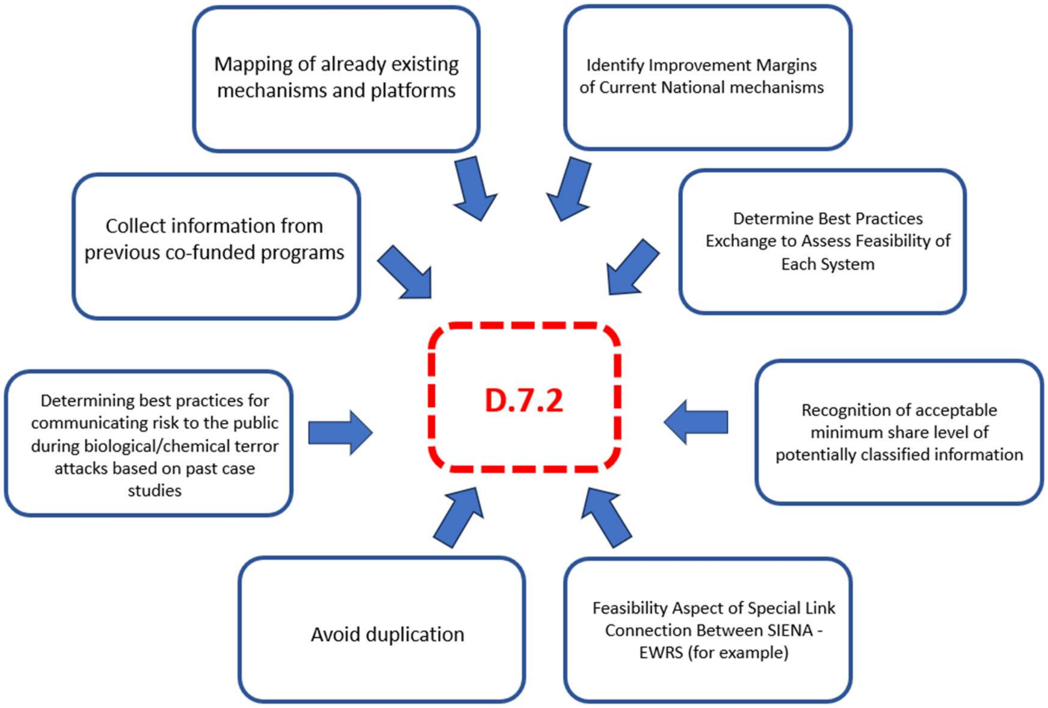

Mapping of already existing mechanisms and platforms
Identify Improvement Margins of Current National mechanisms
Collect information from previous co-funded programs
Determine Best Practices Exchange to Assess Feasibility of Each System
D.7.2
Determining best practices for communicating risk to the public during biological/chemical terror attacks based on past case studies
Recognition of acceptable minimum share level of potentially classified information
Avoid duplication
Feasibility Aspect of Special Link Connection Between SIENA - EWRS (for example)

Figure 4. **Decoding Tasks for Producing D.7.**

2. Collecting Information

2.1 Mapping of Existing Mechanisms and Platforms Designed/Or in Use by Members States both at a National and EU Level

As G.A. demands, a mapping of existing notification platforms was conducted by wp7 team used including both National level systems (per country) as well as EU level. Our findings also include systems that are in use in a variety of types such as Counter Terrorism, Civil Protection, Public Health Monitoring etc.

WP7 team put a lot of effort accessing information not only from the below table contents for rapid notification purposes systems but also from projects and programs like EU4Health, HADEA's Cybersecurity Work Program, Europe Work Program focusing on European Common data infrastructure and services, DigitalHealthAtlas and IHR. In all these projects and programs WP7 reviewed the most important aspects of each of them and kept all the necessary info needed to complete required task (where information was available). The main outcomes of all the above described gathering procedure are displayed on Table1 below.

Table 1. Map of mechanisms and platforms designed/or in use by Member States both at a National and EU level that can be utilized for rapid notification purposes.

Level	Country	System name	Branch	Type	Description	Source
EU		**Emergency Response Coordination Centre** **(ERCC)**	EU Civil Protection	CIVIL PROTECTION	Centre ensures the rapid deployment of emergency support and acts as a coordination hub between all EU Member States	https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/emergency-response-coordination-centre-ercc_en
EU		**Secure Information Exchange Network Application (SIENA)**	EUROPOL	LAW ENFORCEMENT	Large scale information exchange channel for exchange of operational and strategic crime-related information	https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena
EU		**Early Warning and Response System of the European Union (EWRS)**	ECDC	PUBLIC HEALTH	Web-based system for monitoring public health threats in the EU to control communicable diseases	https://www.ecdc.europa.eu/en/publications-data/early-warning-and-response-system-european-union-ewrs
EU		**CBRN Surveillance as a Service" Program - CBRN SaaS**	Permanent Structured Cooperati	COUNTER TERRORISM	CBRN Surveillance system utilizing manned-unmanned sensor network consisting of Unmanned Aerial System (UAS) and	https://www.pesco.europa.eu/project/chemical-biological-radiological-and-nuclear-cbrn-surveillance-as-a-service-cbrn-saas/

			on (PESCO)		Unmanned Ground Systems (UGS)	
EU		**European Radiological Data Exchange Platform (EURDEP)**	EU JOINT RESEARCH CENTRE	INFORMATION EXCHANGE	Real Time data mechanism for radiological data exchange	https://remon.jrc.ec.europa.eu/About/Rad-Data-Exchange
EU		**EU conflict Early Warning System (EWS)**	European Commission	CONFLICT PREVENTION	Evidence-based risk management tool for identification, prioritization and risk assessment of violent Conflict 11:1 in non-EU countries	https://knowledge4policy.ec.europa.eu/publication/eu-conflict-early-warning-system-objectives-process-guidance-implementation_en
EU		**ARGUS**		All crises	Internal communication network for concerned DG services during crisis situations	
EU		**CECIS (Common Emergency Communication and Information System)**		Radiological emergencies and nuclear accidents	Web-based, 24/7, communication and information sharing between the Monitoring and Information Centre of DG ECHO (Civil Protection) and designated contact points in the EU member states	
EU		**ADNS (Animal Disease Notification System)**		Notification system on contagious animal disease outbreaks		
EU		**RASFF (Rapid Alert System for Food and Feed)**		Food and feed emergencies	Rapid alert system for food and feed to exchange information in cases where risk to human health is identified in food or feed products	
EU		**RAS-BICHAT (Rapid Alert System on Biological and Chemical Agent Attack Taskforce)**		Biological and chemical threats	Web-based rapid alert system used for exchanging information on health threats due to deliberate release of chemical, biological and radio-nuclear agents	
EU		**RAS-CHEM (Rapid Alert System for Chemical Incidents)**		Chemical threats	Rapid alert system linking the various poison centers of the EU and the Ministries of Health for the exchange of information on incidents including chemical agents relevant to terrorism	

EU		**EUROPHYT (European Network of Plant Health Information Systems) Phytosanitary network**		Plant or plant product emergencies	Provides database for relevant information on interceptions of harmful organisms or prohibited plants and plant products	
EU		**RAPEX (Rapid Alert System for Non-Food Consumer Products)**		Non-food consumer emergencies	Provides rapid exchange of information on measures taken by national authorities and/or product distributers on non-food consumer products	
EU		**AFIS (Anti Fraud Information System)**		Economic security/Protection of EU budge	Rapid exchange of information on fraud between the European Commission and the competent authorities in the EU member states	
EU		**CIWIN (Critical Infrastructure Warning Information Network)**		Energy & Transport	Information exchange tool on critical infra-structure (energy and transport networks) through designated contact points in the EU	
EU		**TARIQA RELEX Crisis Management**		Socio-political conflicts/Humanitarian natural disasters	Rapid alert system for political and humanitarian crises, enabling the alerting of political and humanitarian crises which appear in the media	
FRANCE		**Reactive mortality surveillance system- syndromic surveillance system SurSaUD**			Combines both morbidity and mortality data (all-cause mortality surveillance system)	
GERMANY		**SARI (Severe Acute Respiratory Infections) surveillance system**			Acute respiratory infections, specifically influenza	
ITALY		**Emergency Department Syndrome Surveillance System**			5 syndromes including measles-like illness	
AUSTRIA		**Civil Protection Alarm**	Federal Ministry of the Interior	CIVIL PROTECTION	Rapid transmission system for notification of or the public in cases of disasters or crises	https://www.bmi.gv.at/204_english/skkm/warning.aspx

AUSTRIA		**Radiation Early Warning System**	Federal Ministry of the Agriculture	CIVIL PROTECTION	Radiation Early Warning System for large-scale radioactive contamination detection	https://www.bmi.gv.at/204_english/skkm/warning.aspx
GREECE		**Unified Operations and Crisis Management Coordination Center "POLYDEFKIS"**	HELLENIC POLICE	LAW ENFORCEMENT	Coordination and intercommunication system for information exchange between Greek police units	https://www.astynomia.gr/elliniki-astynomia/eidikes-ypiresies/eniaio-syntonistiko-kentro-epicheiriseon-kai-diacheirisis-kriseon-e-s-k-e-di-k/
SPAIN		**Early Warning System (SAT)**	Centro Criptológico Nacional	CYBERCECURITY	Cyber Security- oriented platform to detect an incident at an early stage in order to minimize its impact and reach.	https://www.ccn.cni.es/index.php/en/ccn-cert-en/early-warning-system-sat
PORTUGAL		**EARLY WARNING SYSTEM FOR COASTAL RISKS INDUCED BY STORMS**	LNEC - Laboratório Nacional de Engenharia Civil	WEATHER MONITORING	Coastal flooding and erosion early warning system (EWS) for both sandy and armoured coasts	https://www.lnec.pt/hidraulica-ambiente/en/estudos/detalhes.php?tipo=0&id=343
NORWAY		**Emergency Alert System**	Norwegian Civil Defence	CIVIL PROTECTION	Public notification system for emergency situations	https://www.emergencyalert.no/about-emergency-alert/
NORWAY		**Norwegian Surveillance System for Communicable Diseases (MSIS)**	Norwegian Public Health Institute	PUBLIC HEALTH	Surveillance system of infectious diseases in Norway	https://www.fhi.no/en/ou/msis/
NETHERLANDS		**ProMED-mail; the Program for Monitoring Emerging Diseases**			Emerging diseases involving humans, animals and plants around the world	
NORWAY		**National web-based outbreak rapid alert system (Vesuv)**			(1) outbreaks caused by infectious diseases that are notifiable to MSIS, (2) outbreaks suspected to be associated with food or water, (3) outbreaks of particularly severe illnesses (4) particularly extensive outbreaks, and (5) outbreaks in healthcare institutions *MSIS: Melding system for smittsomme cyclomer (MSIS) Norwegian Surveillance System for Communicable Diseases	
SPAIN		**System for Information on Detection and Analysis of Risks and Threats to**				

		Health (SIDARTHa)				
UK		**Emergency Department Sentinel Syndromic Surveillance System (EDSSS)**			Syndromic indicators (respiratory, gastrointestinal, cardiac, acute respiratory infection, gastroenteritis and myocardial ischemia)	
UK		**NHS Direct Surveillance System**			Syndromes which may represent the prodromal stages of disease caused by a bio-terrorist attack, or more likely a rise in common infections	

2.2. Collecting Info from Previous co-funded Programs on Information Exchange Platform

2.2.1 Impress FP7

One of the most important – and similar – to our program was Impress FP7,(Improving Preparedness and Response of Health Services in major Crises) Seventh Framework Program.

The program started at May 1st 2014 and ended at April 30th 2017 and aimed at communication between Health Services (and Emergency Responders) at all levels of response and the crisis cycle with the necessary health care systems support, supervision and management of participating organizations. Assisted health services in becoming more proactive, better prepared and interoperable with other emergency response organizations. Thus, medical emergency teams turned, using IMPRESS, into one coherent force. IMPRESS catalyzed a dramatic and durable impact in the way in which Health Services are provided in crisis situations, and helped improve the integration of health care actors and volunteers with other Crisis Management stakeholders, providing also an overall competitive advantage of CM-related SMEs and large businesses in Europe.

The IMPRESS project has resulted in the following main scientific and technological results:

1. a core taxonomy for the health services involved in emergency management, as well as a semantic reference model (ontology) for the specific domain, taking into consideration current standards and specifications for interoperability purposes.

2. a Health Emergency Management System (HEMS) approach which is most suited for European countries deployment, taking into consideration current adopted approaches and providing a comprehensive overview of the role, responsibilities and interactions of clinical and public health providers, given proper attention to the requirement of cross-border and multi-cultural

implementation. Abstraction has been made from the country-specific legal formalities and organizational traditions, and the typology and categorization of the health services has taken a more generic format of operational functions and responsibilities.

3. a new operating framework based upon a distributed, modular, scalable system, that is able of connecting systems from different organizations into a common advanced holistic response framework, catering for the necessary interconnection and interoperability layers

4. an integrated and interoperable multi-agency coordination and collaboration, COP, reporting and Decision support system to effectively and timely manage and respond, as well as optimize available resources during the management of large scale health emergencies. Those solutions help the different health agencies to share and combine information and resources, which in turn will help them to act in concert rather than as independent organizations. At the same time, the information sharing and combination help all Health Emergency Units to build a more complete picture of the crisis response from the fragments of data available to them. As a result, they are better able to coordinate and distribute resources across the event, increasing the efficiency and effectiveness of a Health Emergency response.

5. training component and associated training material as well as lessons learnt collection tool that both facilitate the easy deployment, use and know-how of end user operators and decision makers.

The program finally provided the following relevant to our project tools which were tested in three pilots, two real-life and one tabletop exercise.

- Call-Center Operations Management
- Operational Resource Management
- Incident Management & Computer Aided Dispatch
- Operational Resource Tracking
- Rostering
- Situational Reporting
- Radio over IP Communication
- Mobile Data
- Sensor Data
- Geographical Information System

All the above tools did not have available in detail technical description, plus the facts:

- ➔ described technologies did not include modern available approaches as AI,
- ➔ "target" entities the IMPRESS project focused were health services, hospitals, first health responders,

wp7 team resulted that the outcomes could not be used in a tailored to biological/chemical S.I.E.P and took advantage only some of the ideas the approach had (for example sensor data).

2.2.2 Research Methodology upon Similar Programs

At the same time wp7 team put a lot of effort to discover relevant EU co funded projects with the same or similar subject. WP7 team focused on Community Research and Development Information Service (CORDIS) portal to retrieve all possible available information. The provided CORDIS search engine was not sufficient for our work so, team decided to proceed with different (and slightly more complicated approach) in order to discover everything that was available at the time of writing this deliverable. The methodology team used was access at URL https://data.europa.eu and proceeded downloading a complete catalogue of all the projects and deliverables under horizon, horizon2020, and fp7 categories. Luckily the information was provided using .xlsx file format in more detail and included all the necessary information for extensive search and detection under category "title" and "object". Using keywords: "Information Exchange", "Terror" wp7 team tried to discover relevant programs/projects on project.xlsx files of horizon, horizon2020, and fp7.

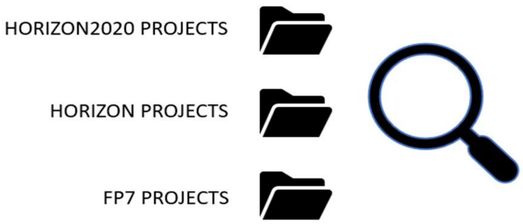


Figure 5. **data.europa.eu projects research**

If relative result was detected from previous step, extensive search was conducted on deliverables of the particular project

Figure 1.4. CORDIS Deliver

HORIZON2020 Deliverables
HORIZON Deliverables
FP7 Deliverables

Figure 6. **data.europa.eu deliverable research**

Based on methodology above the most relevant results are provided on following tables with the bold ones represent the most "closed ones" to our deliverable target:

Table 2. Horizon Projects Repository Relevant Results

Keywords	**Horizon Projects Repository** **Project Title**
Information Exchange	**•A EUROPEAN CYBER RESILIENCE FRAMEWORK WITH ARTIFICIAL INTELLIGENCE -ASSISTED ORCHESTRATION & AUTOMATION FOR BUSINESS CONTINUITY, INCIDENT RESPONSE & INFORMATION EXCHANGE** •MAXIMIZING THE TAX REVENUES FROM THE AUTOMATIC FINANCIAL ACCOUNT INFORMATION EXCHANGE SYSTEM •Fake News Risk Mitigator **•Powerful Lawful Interception, Investigation, and Intelligence**
Terror	**•European Network Against Crime and Terrorism (new)** •Travelling Intelligence Against Crime and Terrorism •Risk-based Approach For the Protection of public spaces in European CITIES **•European Global Counterterrorism (brand new) 24-27**

Table 3. Horizon2020 Projects Repository Relevant Results

Keywords	**Horizon2020 Projects Repository** **Project Title**
Information Exchange	•Architecture for European Logistics Information eXchange. •A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis.

	•HUMANE: a typology, method and roadmap for Human Machine Networks. •Competitive Methods to protect local Public Administration from Cyber security Threats. •Multi-layered Security technologies to ensure hyper connected smart cities with Blockchain, BigData, Cloud and IoT. •Coordination of Transmission and Distribution data eXchanges for renewables integration in the European marketplace through Advanced, Scalable and Secure ICT Systems and Tools. •Advanced Tools to Assess and mitigate the criticality of ICT Components and their dependencies over Critical Infrastructures. **•Next generation of information systems to support EU external policies.** **•Maritime Integrated Surveillance Awareness.** **•When a Profile is worth more than a Thousand of Hashtags: Automatic Inference of Personality Traits based on Images Shared in Social Networks**
Terror	•High quality real time broadcasting technology that provides reliable and resilient signal. •A fast non-intrusive vapour detection system that rapidly identifies explosives in public areas. •Innovative nanotech-based detection equipment in the area of homeland security. **•Crisis Communication and Deterrence: The Interaction of Facts and Fictions**. **•GeoViSense: Towards a transdisciplinary human sensor science of human visuo-spatial decision making with geographic information displays**. •Arctic and North Atlantic Security and Emergency Preparedness Network. •Autonomous emergency manoeuvring and movement monitoring for road transport security

Table 4. FP7 Projects Repository Relevant Results

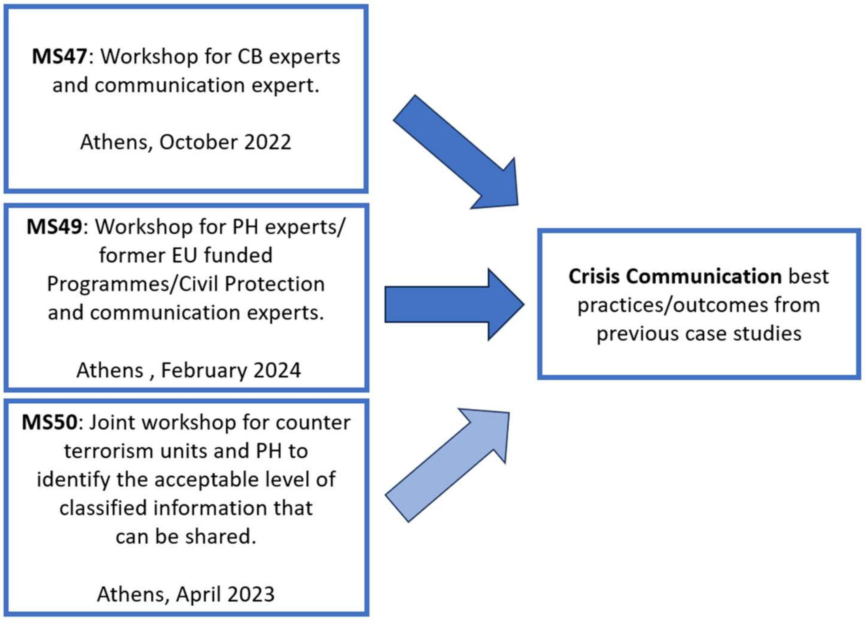
Keywords	**FP7 Projects Repository** **Project Title**
Information Exchange	•Indicator-based Interactive Decision Support and Information Exchange Platform for Smart Cities •GMES for Africa: Regional Network for Information Exchange and Training in Emergencies **•Information Exchange Policies for Human-Computer Negotiation** •Secure Imprint Generated for Paper Documents •Mobile Cloud Computing: Networks, Services and Architecture (MONICA) **•Making the Web an Exploratory for Geospatial Knowledge** •Indicator-based Interactive Decision Support and Information Exchange Platform for Smart Cities •Interoperability of data and procedures in large-scale multinational disaster response actions •Cooperative Networking for High Capacity Transport Architectures Integrative Computational Materials Engineering Expert Group •A Geospatial Knowledge World **•Physical Layer Wireless Security** •Integration of CryptoD to ERA

Terror	•Predictive Reasoning and multi-source fusion empowering Anticipation of attacks and Terrorist actions In Urban Environments •Can Natural Disasters Incite Terror? •Distributed Multi-way Analysis of Stream Data for Detection of Complex Attacks •Improved First Responder Ensembles Against CBRN Terrorism **•IP-Based Emergency Applications and Services for Next Generation Networks** **•Demonstration of Counterterrorism System-of-Systems against CBRNE phase 1** •Integrated Mobile Security Kit •Tools, methods and training for Communities and Society to better prepare for a Crisis **•Preparedness and Resilience against CBRN Terrorism using Integrated Concepts and Equipment PRACTICE** **•Counter-Terrorism Crisis Communications Strategies for Recovery and Continuity** **•Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces** •Detection Technologies, Terrorism, Ethics and Human Rights

3. Determining Best Practices for Communicating Risk to the Public During Biological/Chemical Terror Attacks Based on Past Case Studies

3.1. Methodology Used

Social scientists and communication experts play a crucial role in influencing public perception, disseminating accurate information, and minimizing panic. Long and detailed conversations took place during workshops mainly on *(MS47)* at Athens, October 2022, *(MS50)* at Athens, April 2023 and less on *(MS49)* at Athens, February 2024 regarding the approach and best practices communication experts should follow in case of biological/terror attack.



MS47: Workshop for CB experts and communication expert.

Athens, October 2022

MS49: Workshop for PH experts/ former EU funded Programmes/Civil Protection and communication experts.

Athens , February 2024

MS50: Joint workshop for counter terrorism units and PH to identify the acceptable level of classified information that can be shared.

Athens, April 2023

Crisis Communication best practices/outcomes from previous case studies

Figure 7. **Social Scientists & Communication Experts Workshops**

For this exactly reason extended analysis took place based on particular case studies such as 2004 Athens Olympic games - and "public communication mechanisms" were built at that time in case of a biological/chemical attack - , 1995 Tokyo sarin subway terror attack, and 2018 Salisbury attack. After a generic approach on all above case studies the experts chose to focus on Salisbury attack (as one of the most recent incidents) and accepted that the communication towards the public during the Salisbury poisonings was generally considered appropriate given the circumstances. Authorities, including public health officials and law enforcement agencies, provided regular updates to the public regarding the investigation, the nature of the nerve agent used (Novichok), and safety precautions. Efforts were also made to reassure the public, provide accurate information, and advise on any necessary precautions, such as avoiding areas where the poison was found and following hygiene guidelines. Additionally, there was transparency about the ongoing investigation and efforts to identify and hold accountable those responsible for the attack. While there was certainly concern and apprehension among the public, widespread panic was largely avoided.

3.2. Conclusions

Experts concluded during the previous mentioned workshops and examples they used that most of the times communication risk procedure was more or less successful **due in part to the clear and consistent communication from authorities, as well as the effective implementation of safety measures**. **However, misinformation did circulate during the incident, as is common in high-profile events. Also, rumors and conspiracy theories regarding the origins and motives behind the attack were spread through various channels, including social media and alternative news outlets**. Authorities worked to counter misinformation by providing accurate information and addressing false claims promptly. In hindsight, communication experts concluded there were areas where communication strategies could have been improved. Clearer and more consistent messaging from authorities could have helped alleviate confusion and anxiety among the public. Additionally, better coordination between different agencies and stakeholders involved in the response could have ensured a more cohesive communication approach. Finally, the experts underlined their vital role in promoting public safety, building resilience to hazards, and fostering trust and collaboration in communities facing uncertain or challenging circumstances as biological/chemical attacks. They also focused on how -and why - risk communication experts have a deep understanding of individuals' perception and interpretation of risks that no one could at modern times ignore. Their expertise and ability of "translating" scientific data, statistical analyses, and technical jargon into layperson-friendly language, ensuring that everyone can understand the risks they face and the actions they can take to mitigate them is also a crucial result of the above workshops. Finally, the outcomes of above workshops concluded that risk communication experts task **is not just about providing information; it's also about influencing behavior**. Risk communication experts referred a lot of times some basic behavioral science principles to design messages that motivate people to adopt risk-reducing behaviors, such as (for example) getting vaccinated, wearing protective gear, or evacuating during emergencies! This also was a very critical outcome on how and why we should take advantage of risk communication expertise and make the involvement of this science even more intense when we are facing/or planning a biological/chemical response attack plan. Best practices outcomes from previous mentioned workshops are summarized and presented below accordingly.

3.3. Outcomes: Determination of Best Practices

Table 5. Best Practices for communicating risk to the public during biological/chemical terror attacks

• Necessity Involving Social Scientists / Communication Experts in case of CB terror attack. The staff of the respective organisations should include communicators specialized in risk and crisis communication, in order to be able to address such issues, but also to establish a permanent understanding and appreciation of the increasingly significant role of communication in these situation.
• Clear Communication Channels Establishment. Establish clear and accessible communication channels for disseminating information to the public. This may include emergency hotlines, social media platforms, official websites, and traditional media outlets
• Provision of Timely and Accurate Information: Social Scientists / Communication Experts must prioritize the timely dissemination of accurate information regarding the nature of the biological/chemical threat, potential health risks, and recommended safety measures. Updates should be provided regularly to keep the public informed of any developments or changes in the situation.
• Tailor Messages to the Audience: Social Scientists / Communication Experts should tailor their messages to the specific needs and concerns of different audience groups, including the general public, healthcare professionals, first responders, and vulnerable populations. Messages should be clear, concise, and culturally sensitive to ensure maximum understanding and compliance.
• Address Public Concerns and Misconceptions: Social Scientists / Communication Experts should anticipate and address public concerns and misconceptions surrounding biological/chemical terror attacks. This may involve providing factual information to debunk rumors, addressing fears about exposure or contamination, and offering guidance on protective actions.
• Address Misinformation and Disinformation: Misinformation and disinformation are two significantly different issues, that both need to be address accordingly. Misinformation on one hand might be an outcome of a mistake, or not accurate information, and needs always to be addressed, but disinformation on the other hand is deliverable spread of false information for specific cause. The implementation of a disinformation strategy in case of a deliverable biochemical attack is highly probable, in order to multiply the effects of the attack, and as such, the development of respective mitigation strategy is of high importance.
• Provide Practical Guidance for Risk Mitigation: Social Scientists / Communication Experts should provide practical guidance on how individuals and communities can mitigate their risk of exposure to biological/chemical threats. This may include instructions on seeking shelter, avoiding contaminated areas, practicing good hygiene, and seeking medical attention if necessary
• Offer Psychological Support: Social Scientists / Communication Experts should recognize the psychological impact of biological/chemical terror attacks and offer support and resources to help individuals cope with fear, anxiety, and trauma. This may involve providing access to mental health services, crisis hotlines, and community support networks

• Coordination with Stakeholders: Social Scientists / Communication Experts should coordinate closely with relevant stakeholders, including government agencies, healthcare providers, emergency responders, and community organizations. Collaborative communication efforts ensure consistency, coherence, and effectiveness in reaching the public with important safety information.
• Monitor Feedback and Adjust Strategies: Social Scientists / Communication Experts should continuously monitor feedback from the public and stakeholders to evaluate the effectiveness of communication strategies. This feedback can inform adjustments and refinements to messaging, channels, and tactics to better meet the needs of the audience.
• Promote Resilience and Preparedness: Social Scientists / Communication Experts should use biological/chemical terror attacks as opportunities to promote resilience and preparedness within communities. This may involve encouraging individuals to develop emergency plans, assemble disaster supply kits, and participate in training exercises, where drills and simulations could be conducted.

4. Avoid Duplication, Identify Improvement Margins of Current National mechanisms and Determine Best Practices Exchange to Assess Feasibility of Each System

4.1. Duplication Control on CELESTE, PRACTICE, EDEN and PROACTIVE Projects

Grant Agreement required inspection to be contacted for the CELESTE, PRACTICE, EDEN and PROACTIVE previous EU funded programs. The details of each one of them are following below:

CELESTE project (part of EIT Urban Mobility 2020) (https://www.eiturbanmobility.eu/projects/celeste/) seeks to work both on technological solutions (including connected signals, extended data models and vehicle technology) and evaluation tools that can be transferred beyond the partner cities. The project purpose was also to materialise the solutions into functional prototypes thus delivering value globally to both project partners and EIT. The project aimed to address excessive vehicle speed limits and improve driver compliance within cities to increase citizen safety and reduce pollution, analyse the current synergies between dynamic speed limits and ISAs (Intelligent Speed Assistance systems), define traffic management solutions, and finally develop a speed limit enforcement system and recommended advisory solutions to ensure real-time regulatory compliance. All the above helps to conclude that there isn't any relevance between deliverable D.7.2 aim and the celeste program. The D.7.2 aims to produce an IT Platform for secure information exchange platform among involved stakeholders in case of biological/chemical incident and the CELESTE program aims to address excessive vehicle speed limits and improve driver compliance within cities to increase citizen safety and reduce pollution , analyse the current synergies between dynamic speed limits and ISAs (Intelligent Speed Assistance systems),define traffic management solutions, and finally develop a speed limit enforcement system and recommended advisory solutions to ensure real-time regulatory compliance. One of the relevant outcomes we could take in our mind is the UMF (Urban Mobility Flows) platform described as a cutting-edge big data analytics solution that uses anonymous telco data to determine aggregated journey flows across multiple transport modes. But, beyond the common technologies involved to create such an outcome of CELESTE program (for example: IT protocols, internet communication channels) there is nothing useful for our project to use and take advantage of. Also, FlexCurb "innovation project" is described as a set of application programme interfaces (APIs) that allow creation of a digital inventory of a city's curb regulations, so they can visualise and analyse the patterns of curb allocation and use, as well as to adapt and communicate curb regulations. This kind of technology is also already embedded on our deliverable. As a matter of fact the D.7.2 is much more complicated as an outcome with the latest technologies involved focused in Information exchange protocols and usage so nothing from this project could or should be possible be used.

Preventing Radicalism through Critical Thinking Competences - PRACTICE Program (PRACTICE – Project n° 2018-1-IT-02-KA201-048442)(https://practice-school.eu/the-project/) addresses current challenges & needs of preventing radicalisation in school & of supporting opportunities for teachers' continuing professional development in this area, by developing, testing & disseminating an innovative approach, using participatory methods collaborative process, that involve 7 partner organisations and 35 schools at local, national & EU level. The main objectives of this particular program were to develop an innovative and collaborative EU wide CPD programme on radicalism prevention within school education, empower teachers through capacity-building activities aimed to equip them with better tools to address diversity in the classroom and to understand and prevent radicalisation processes in educational settings, enhance the development of critical thinking skills and strengthen citizenship and the common values of freedom, tolerance and non–discrimination through education in secondary schools and foster the inclusion of students from all ethnic, faith and social backgrounds creating a safe space to become active and responsible citizens and open-minded members of society. The outcomes of this particular project were irrelevant with the needs of deliverable D.7.2 and no more action needed to be done.

European Distance and E-Learning Network – EDEN project consists of a smart network for the distance and e-learning professional community and a professional community for smart learning. The EDEN network consists of projects that up and running till now and projects that are completed and archived. As wp7 team we searched all the projects (active or not) to locate outcomes that could be relevant to this particular deliverable. The Playful Environment for Inclusive learning Design in Europe showed some "perspective' but nothing useful could be extracted from it because the focus was on teaching approaches using (for example) gamified platforms or hybrid I4Ts games. DIGI He from the other side had some generic and not relevant outcomes about the need of digitalization in higher education which is irrelevant with the description and requirements of a tangible secure information exchange IT platform tailored to biological/chemical attack needs. Also the repository research at URL address https://www.eden-online.org/eu-projects/archived-projects/ also revealed no useful results for our required outcome.

On the contrary, PROACTIVE project (Preparedness against CBRNE threats through Common Approaches between security Practitioners and the Vulnerable civil society) (https://proactive-h2020.eu) showed a lot of common elements with our deliverable (D.7.2) especially on the area of the secure information exchange platform and the approach was taken from the side of involved partners in this particular project. Scope of this particular program described as: "The main goal of the PROACTIVE project is to enhance preparedness against and response to a CBRNe incident through a better harmonization of procedures between various categories of practitioners, and a better understanding of the needs of vulnerable citizen groups.". Also the PROACTIVE project produced toolkits for CBRNe practitioners and for civil society organizations:

Toolkit for practitioners will include a web collaborative platform with database scenarios for communication and exchange of best practice among LEAs as well as an innovative response tool in the form of a mobile app.

Toolkit for civil society will include a mobile app adapted to various vulnerable citizen categories and pre-incident public information material.

After close deliverables inspection of PROACTIVE Project, [1], [2], [3], [4] - and knowing at the same time wp7 team's obligation to be also unique and distinct on our outcome trying to avoid as much as possible from the job completed on other projects - we processed all the available input from PROACTIVE Project and determined the "strategy" of approaching the writing of our deliverable. We also knew (and accepted) that is unavoidable to use a lot of common infrastructures and protocols in our outcome as the technology of the time written this deliverable is common for everyone (for example all the modern approaches use AES , TLS, HTTPS, and so on) and the difference could be only focused on how you use the "basic ingredients" describing/building such a platform.

So in order to avoid duplication in this particular case the basic writing deliverable strategy was followed as:

1) D.7.2 describes all the necessary attributes/requirements of a tangible secure platform for rapid information exchange between sectors. We didn't have the obligation to build such a platform but just to describe with the best possible and detailed understood way the elements we need to use to. For this reason, the deliverable describes the generic requirements of a secure exchange information platform vs the same platform tailored to biological/chemical terror attack communication needs focusing on detailed description of the basic protocols we used to produce this deliverable.
2) D.7.2 should be easy to be read from everyone without losing at the same time the technical character of the document and expertise should have.
3) D.7.2 proposes **VPN** technology to allow communication among remote endpoints instead mesh networks D.4.2 of PROACTIVE Project describes.
4) D.7.2 involves **A.I Technologies for sentiment analysis** and public interactions/responds.

The modular architecture D.7.2 describes allows integration of "part/s" of proposed tangible secure information exchange platform on existed operative systems.

4.2. Identification of Improvement Margins of Current National Mechanisms for Rapid Information Exchange in Health and/in Between Other Sectors

Critical role proceeding and identify possible improvements margins of current national mechanisms for rapid information exchange took place in Zagreb international workshop at 29th & 30th of November 2023. The interaction among partners gave valuable insights at national mechanisms and how these could be improved. Main results were provided especially during work session 2 topic 3 discovering existence of a lot of systems in parallel with no knowledge of each other, lack of good practices on information exchange among involved entities and overflow of information in some particular countries. The problem seemed to be not the lack of information systems provide but dissemination of it among services and involved entities. Once more the matter of confidentiality of available information and how (and if) should be disseminated (and to whom) was present again. Finally, the need of more homogenous systems at national level was underlined detecting also the necessity of information confidentiality propagation framework among involved entities.

4.3. Best Practices Exchange to Assess Feasibility of Each System

During concurrent workshops conduct - WS47 for CB and communication experts & WS48 involving analysis of existing guidance documents and implemented strategies- an extensive review took place focusing on best practices/techniques and approaches to assess feasibility of each existed system. The main conclusions of these two workshops are summarized below and describe the minimum and most important criteria regarding legal frameworks and data/notification exchange systems. The results below were used as a guide to determine the feasibility of each of the referred systems of Table 1 and co-funded programs.

Table 6. Best Practices Guide to Assess the Feasibility of Information Exchange Systems tailored to Legal Framework, Data/Notification Exchange Systems Criteria

1. Legal frameworks	**1.1 International Cooperation Agreements: Existence of legal agreements and frameworks at international level to facilitate information exchange between countries in the event of emergencies or crises. These agreements should outline protocols for sharing data, coordinating responses, and respecting each country's sovereignty and privacy laws**
	1.2 National Legislation: Comprehensive national legislation that governs information exchange during emergencies. This legislation should outline the roles and responsibilities of relevant agencies, mechanisms for data sharing, procedures for notification and reporting, and safeguards to protect sensitive information and individual rights
	1.3 Interagency Collaboration: Collaboration between government agencies responsible for emergency management, public health, law enforcement, and other relevant sectors. Ensure that legal frameworks enable seamless communication and coordination between these agencies to facilitate effective information exchange.
2. Data/ Notification Exchange Systems	2.1 Centralized Information Hub: Centralized information hub or platform where relevant agencies can securely exchange data and notifications during emergencies. This hub should have robust cybersecurity measures in place to protect sensitive information.
	2.2 Standardized Protocols: Standardized protocols and formats for data exchange to ensure interoperability between different systems and agencies. This includes common data standards, messaging formats, and encryption protocols to facilitate seamless communication.

	2.3 Real-Time Monitoring Systems: Real-time monitoring systems to track and analyze relevant data sources, such as surveillance data, laboratory reports, and social media feeds. These systems can help detect emerging threats, facilitate early warning notifications, and support decision-making processes.
	2.4 Automated Alerting Systems: Automated alerting systems that can quickly notify relevant stakeholders about emergencies or critical events. These systems should be customizable to deliver alerts via multiple channels, such as SMS, email, mobile apps, and social media, based on predefined criteria and escalation protocols
	2.5 Information Sharing Platforms: Secure information sharing platforms that allow authorized users to access and exchange data in real-time. Platforms should support role-based access controls, audit trails, and encryption to safeguard sensitive information and ensure compliance with privacy regulations.

After a thorough examination of the outlined criteria, participants reached at a collective understanding that the identity of each nation is inherently unique and shaped by a myriad of factors including economical status, cultural, and socio-political influences. It became obvious that nations have meticulously crafted information exchange systems tailored to address their specific needs and objectives. These systems, while effective within their respective national contexts, exhibit a remarkable degree of autonomy and differentiation among them.

Indeed, the intricate web of information exchange mechanisms within and among nations manifests as a mosaic of disparate systems, each operating within its own framework and governed by its own set of regulations and protocols. This fragmentation not only complicates the seamless flow of information at the supranational level, such as within the European Union, but also presents challenges at the domestic level, hindering efficient communication and collaboration among various entities within a nation.

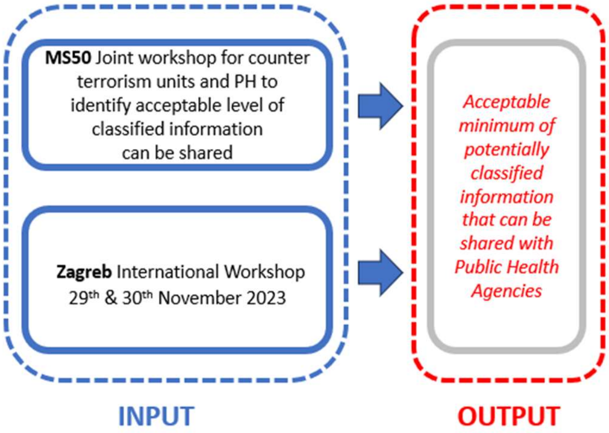
Moreover, the lack of standardized interfaces and interoperability further exacerbates the issue, impeding the facile transfer of information across borders and between jurisdictions. Consequently, what emerges is a landscape characterized by siloed information ecosystems, wherein the potential for synergistic collaboration and knowledge-sharing remains largely untapped.

Considering these observations, it became imperative for participants to recognize the need for greater cohesion and harmonization in information exchange systems, both at the national and international levels. Participants also concluded that efforts should aim at fostering interoperability and establishing common frameworks for data exchange which are crucial in overcoming the existing barriers and finally provide a more interconnected and resilient information infrastructure

5. Recognition of Acceptable Minimum of Potentially Classified Information that can be Shared with Public Health Agencies

Sharing potentially classified information with public health agencies requires careful consideration of national security concerns, privacy rights, and public health imperatives. MS50 joint workshop (Athens, April 2023) for counter terrorism units and PH tried to identify the acceptable level of classified information that can be shared and determine the "threshold" for sharing classified information. Discussion opened regarding general principles and considerations to guide the determination of an acceptable minimum of potentially classified information that can be shared with public health agencies. From the first second participants discovered the complication and almost impossible gathering procedure they should follow to collect legal and regulatory framework information, review relevant laws, regulations, policies related to national security, intelligence and so on and at the same time include the rationale, justification, and legal basis for sharing classified information among involved entities. For this exactly reason a risk-benefit oral analysis was conducted from all participants to assess the potential risks and benefits of sharing classified information with public health agencies, considering factors such as the severity of the public health threat, the likelihood of harm, the effectiveness of public health interventions, and the impact on national security interests. Factors such as the nature of the threat, the availability of alternative sources of information, and especially the potential consequences of sharing or withholding classified information were taken also in mind of the participants to determine the minimum level of sharing information among involved entities in case of biological/chemical terror attack.

Zagreb international workshop at 29th & 30th of November 2023, also provided valuable information regarding cross-sectoral information sharing and flow in preparedness and response



MS50 Joint workshop for counter terrorism units and PH to identify acceptable level of classified information can be shared
Zagreb International Workshop 29th & 30th November 2023
Acceptable minimum of potentially classified information that can be shared with Public Health Agencies
INPUT
OUTPUT

Figure 8. **Main Input Sources Determining Acceptable Minimum of Potentially Classified Information**

The implementation of appropriate security measures to safeguard classified information shared with public health agencies, using encryption, access controls, secure communication channels, and compliance with security clearance requirements revealed also immediately. Finally main summaries were produced among participants based on the extended discussion and experience of each one of them categorized as following:

Security measures every information exchange system should include: Implementation of appropriate security measures to safeguard classified information shared with public health agencies, including encryption, access controls, secure communication channels, and compliance with security clearance requirements ensuring public health agencies have the necessary safeguards and protocols in place to protect classified information in their possession.

Need-to-know principle: Limit the dissemination of classified information only to individuals and agencies with a legitimate need for access to fulfill their responsibilities. Ensure that public health agencies have a clear and documented need for the information to carry out their public health functions.

Establish mechanisms for accountability and oversight to ensure compliance with legal and regulatory requirements and to address any concerns or issues that may arise.

Documentation and Accountability: Maintain thorough documentation of decisions related to the sharing of classified information with public health agencies, including the rationale, justification, and legal basis for sharing classified information. Establish mechanisms for accountability and oversight to ensure compliance with legal and regulatory requirements and to address any concerns or issues that may arise.

By carefully considering above principles and considerations, partners tried hard to detect an acceptable minimum of potentially classified information that can be shared with public health agencies while balancing national security concerns, privacy rights, and public health imperatives. Also, collaboration between national security and public health agencies was characterized as essential to effectively respond to public health emergencies and protect the well-being of populations. Finally, participants concluded all available information should be available to individuals and agencies with a legitimate need for access to fulfill their responsibilities, with high level security measures and in accordance of national legal and regulatory frameworks.

6. Feasibility Aspect of Special Link Connection Between SIENA - EWRS or Similar Other Platforms

In today's interconnected world, the need for seamless communication and collaboration among various platforms is paramount. During the process of examining the feasibility aspect of a special link connection between SIENA (Secure Information Exchange Network Application) and EWRS (Early Warning and Response System) - or similar platforms - emerges as a promising solution. This endeavor holds immense potential for bolstering the efficiency, effectiveness, and overall resilience of emergency response mechanisms. First and foremost, the feasibility of such a link lies in its ability to streamline information exchange. By establishing a direct connection between SIENA and EWRS, or analogous systems, stakeholders involved in emergency response efforts can access real-time data and insights crucial for decision-making. This seamless flow of information can significantly reduce response times, enabling authorities to promptly address emerging threats and mitigate potential risks. Moreover, the proposed link offers a unique opportunity to enhance coordination and cooperation among different agencies and organizations involved in emergency management. By facilitating the exchange of critical information, such as threat assessments, resource availability, and response plans, the connection between SIENA and EWRS promotes a more integrated approach to crisis response. This collaborative framework not only optimizes resource allocation but also fosters synergy among stakeholders, leading to more effective and coordinated actions during emergencies.

Furthermore, the feasibility of this special link extends beyond its technical aspects to encompass its socio-economic implications. By enhancing the capabilities of existing emergency response systems, such as SIENA and EWRS, the proposed connection contributes to the overall safety and well-being of communities. Timely and coordinated responses to emergencies not only save lives and minimize damage but also enhance public trust in the resilience of the response infrastructure. Additionally, the establishment of a special link between SIENA and EWRS aligns with broader efforts to leverage technology for societal benefit. In an era characterized by rapid technological advancements, harnessing the power of connectivity and data exchange is imperative for addressing complex challenges, including those related to emergency management. By embracing innovative solutions and fostering interoperability between platforms, societies can better adapt to evolving threats and ensure the continuity of essential services.

Wp7 team finally concluded, the feasibility of establishing a special link connection between SIENA and EWRS, or similar platforms, represents a significant step towards enhancing emergency response capabilities. Through streamlined information exchange, improved coordination, and leveraging technological advancements, this initiative holds the promise of making our communities safer, more resilient, and better prepared to tackle emergencies of varying scales. Embracing such initiatives underscores in an increasingly interconnected world improves commitment to proactive risk management and collective security aiming undeniable towards the right direction.

7. Attributes / Requirements of Tangible Secure Information Exchange Platform

7.1 Tangible Secure Information Exchange Platform (S.I.E.P)

A tangible secure information exchange platform (S.I.E.P) involves a combination of physical and digital attributes to ensure the confidentiality, integrity and availability of exchanged information. It's a system that allows secure communication and sharing of information among users or entities while emphasizing physical security measures to safeguard the hardware, infrastructure, and access points. Such a platform is designed to protect sensitive data from unauthorized access, ensure data integrity, and provide a secure environment for information exchange. The key elements and requirements of such a system - in generic - are:

7.1.1 Physical Security

The physical security of a secure information exchange platform is a critical component in ensuring the overall integrity and confidentiality of the data it handles. Physical security measures are designed to prevent unauthorized access, protect against theft, and mitigate the impact of physical threats such as natural disasters. The most important key elements for the physical security of secure information exchange platform are:

Access Control: Restriction of access to unauthorized personnel to all core IT services and infrastructure such a data centre, networking equipment.

Surveillance Systems: CCTV cameras and monitoring systems to track and keep records of physical access.

Environmental Controls: Protection against environmental factors such as fire, suppression, temperature and humidity control.

By integrating these physical security measures, organizations can enhance the overall security posture of their information exchange platforms and protect sensitive data from physical threats and unauthorized access. Regular reviews and updates to security protocols are essential to address evolving risks and maintain a robust security infrastructure.

7.1.2 Data Encryption

End to End Encryption (E2EE) is a method of secure communication and it represents a key element during creation procedure of every S.I.E.P that prevents third parties from accessing data while it's transferred from one end system to another. The basic idea behind this powerful method is that data are encrypted at the source (sender's end) and **remain encrypted** until reach the destination (receiver's end). Then only the authorized recipient has the means to decrypt it. Typically, end-to-end encryption involves the use of asymmetric cryptography. Public keys are used for encryption, while private keys are used for decryption. The public key can be freely distributed, but the private key must be kept secret. Great examples of using E2EE at the core of their service are - already famous apps - like signal and WhatsApp taking advantage of this method to secure text messages, voice calls, and multimedia exchange among their users.

Data at rest Encryption is a security measure designed to protect data stored on various types of storage media, such as hard drives, solid-state drives, and other storage devices. The goal is to encrypt the data when it is not actively being used, making it more difficult for unauthorized individuals to access or misuse the information Implementing data at rest encryption is a critical part of a comprehensive data security strategy, especially in environments where sensitive or regulated data is stored. It adds an additional layer of protection to prevent unauthorized access to data even if physical access to the storage media is obtained.

7.1.3 Authentication and Authorization

Multi-Factor Authentication (MFA), also known as Two-Factor Authentication (2FA) or Two-Step Verification (2SV), is a security mechanism that requires users to provide two or more authentication factors to gain access to a system, application, or online account. This adds an extra layer of security beyond just a username and password. The basic principle of how this works can be described as:

● Users provide their standard username and password (something they know).

● After successfully entering the password, they are prompted to provide a second factor (something they have or something they are).

●The second factor must be delivered through a separate channel, enhancing security

Channels used for the second factor transmission are most of the time SMS service, authentication apps, biometric verification, email verification.

Role-Based Access Control (RMAC), is an access control model that restricts system access to authorized users based on their roles within an organization. It is a widely used method for managing permissions and ensuring that users have the right level of access to perform their duties. In short terms the RMAC assigns **Roles** (job function/user) , **Permissions** (Each role has specific permissions) and finally the model creates - based on the two previous assignments - a **Hierarchy** , a structure where higher level roles inherit permissions to lower level roles. This simple and powerful algorithm is a robust access control model that provides an organized and scalable approach to managing user permissions. It helps to enforce the principle of least privilege, ensuring that users have only the access they need to perform their job functions, which is crucial for maintaining the security and integrity of secure information exchange systems.

7.1.4 Audit Trails

Logging and Monitoring are crucial components of every IT system / platform information and vital element on a complete security and compliance strategy. They involve **the systematic recording** of **events** and **activities** within a system or network to facilitate analysis, detection of security incidents, and compliance with regulatory requirements. Basic purpose of such a system is to keep chronological records of system activities, including user actions, system events, and changes to configurations or data finally providing a **detailed history of activities** for forensic analysis, compliance, and incident response. Implementing effective logging, and monitoring practices is fundamental to maintaining the security and resilience of any IT system. These practices not only aid in proactive threat detection but also support post-incident analysis and compliance efforts.

Alerts and Notifications: Alerts and notifications play a crucial role in information exchange systems, serving as proactive mechanisms to inform users and administrators about important events, potential issues, or security incidents. These alerts help ensure the integrity, availability, and security of the exchanged information. Implementing a robust alert and notification system is essential for maintaining the security, reliability, and performance of S.I.E.P's. It helps respond promptly to potential threats, disruptions, or abnormal events, contributing to a proactive and resilient cybersecurity posture.

7.1.5 Secure Protocols and Standards

Use of HTTPS (Hypertext Transfer Protocol Secure) is essential for securing information exchange on online platforms. It is an extension of HTTP, the protocol used for transferring data over the web, but with an additional layer of security provided by SSL (Secure Sockets Layer) or its successor, TLS (Transport Layer Security). Its a fundamental security measure for information exchange platforms, **providing encryption, authentication, and data integrity**. Its adoption is critical for ensuring the privacy and security of user data, meeting regulatory requirements, and maintaining user trust in online interactions.

Compliance with Standards is crucial for information exchange platforms to ensure security, privacy, and interoperability. Various industry-specific and general standards exist, and adherence to these standards helps IT developers demonstrate a commitment to best practices and regulatory requirements. Some of the most famous and used standards are ISO 27001 (Information Security Management System) , GDPR (Global Data protection Regulation) , HIPAA (Health Insurance Portability and Accountability), OAuth (Open Authentication) and so much more. When implementing information exchange platforms, IT developers should assess the relevant standards based on their industry, regulatory environment, and the nature of the data being exchanged. Adhering to these standards not only helps in compliance but also enhances security, interoperability, and the overall trustworthiness of the information exchange ecosystem. Regular assessments and updates are crucial to adapting to evolving standards and regulatory requirements.

7.1.6 Vulnerability Management

Regular Security Audits are essential for information exchange platforms to identify vulnerabilities, assess the effectiveness of security controls, and ensure compliance with security policies and standards. They are an integral part of a proactive cybersecurity strategy and help to identify and address vulnerabilities before they can be exploited, contributing to a more resilient and secure information exchange platform.

Patch Management: Software regularly applying patches ensures that vulnerabilities are addressed, reducing the risk of security breaches and enhancing the overall reliability of the platform. Its an ongoing process that requires proactive planning, regular assessments, and collaboration between IT teams, security professionals, and other stakeholders. By prioritizing and addressing vulnerabilities promptly, information exchange platforms can maintain a strong security posture and reduce the risk of security incidents.

7.1.7 Data Integrity

Hashing Algorithms play a crucial role in information security, particularly in the context of information exchange platforms. Hash functions are cryptographic algorithms that transform input data into a fixed-size string of characters, which is typically a hash value or digest. When implemented properly, hashing provides several security benefits for information exchange platforms. These algorithms commonly used to verify the integrity of data during information exchange, storing passwords with safety, identify duplicate data and ensure consistency in the choice of hashing algorithms across different components of the platform. Implementing secure hashing practices is fundamental to maintain the integrity and authenticity of data in information exchange platforms. It is crucial for protecting sensitive information and ensuring the overall security of the platform and its users.

Checksums and Digital Signatures are cryptographic techniques used in information exchange platforms to ensure data integrity, authenticity, and security. Both methods involve generating fixed-size values based on the content of data, but they serve different purposes and provide different levels of security. **Checksums** are primarily used to verify the integrity of data and detect accidental errors or corruptions in transmitted or stored data. **Digital Signatures** also provide integrity verification of data and simultaneously authenticity of the sender. Level of non-repudiation (the sender cannot deny sending the message/data) is also provided by the same technique.

7.1.8 Incident Response and Data Availability

Incident Response Plan provides a structured approach to detect, respond to, and recover from security incidents. It’s usually dynamic, adaptive, and tailored to the specific needs and risks of the information exchange platform. Regular testing, training, and updates ensure that the plan remains robust and aligned with the evolving threat landscape.

Regular Backups serve as a “safety net” against data loss, corruption, or other unforeseen incidents. It’s a crucial component on every S.I.E.P and in the core of it. Implementing and maintaining a robust backup strategy is fundamental to safeguarding the continuity and integrity of any information exchange platform. Regular assessments, testing, and adherence to best practices contribute to the effectiveness of the backup system.

7.1.9 Secure Communication Channels

Virtual Private Network (VPN) is a critical component for securing communication and data exchange. Creates a secure, encrypted connection over a less secure network, such as the internet. It's a fundamental step toward securing communication and ensuring the confidentiality, integrity, and privacy of exchanged information. It's important IT developers to choose a VPN solution in alignment with specific security and operational requirements of the any platform that requires state of the art infrastructure based on safety of sensitive data exchange. Regular monitoring, updates, and security assessments contribute to the ongoing effectiveness of the VPN implementation

Secure Socket Layer (SSL) / Transport Layer Security (TLS) are cryptographic protocols providing secure communication over a computer network. They are commonly used in S.I.E.P's to ensure the confidentiality and integrity of data transmitted between clients and servers**.** These protocols prevents unauthorized parties from intercepting and reading sensitive information and are fundamental elements for secure communication **particularly in web-based applications.**

7.1.10 Human Factor – Education and Training

Security Awareness Programs are essential components of a comprehensive cybersecurity strategy within secure information exchange platforms. These programs aim to educate and empower users with the knowledge and skills needed to recognize and mitigate security threats. Customized user-friendly training material including multimedia resources such as videos, infographics and interactive modules that are relevant to the S.I.E.P is provided to users engaging interest increase, awareness and retention of security best practices. The content of these programs should be crystal clear about the role and the responsibilities each user has and must be easy to understand. It's an ongoing process that requires commitment from leadership and active participation from all users. By fostering a security-conscious culture and providing continuous education significantly enhances the overall security posture of any secure information exchange platform.

Phishing Awareness is also a crucial aspect of any S.I.E.P security strategy. Phishing attacks often target users through deceptive emails, messages, or websites to trick them into divulging sensitive information. It's part of the Security Awareness Programs but because the problem has gone wild the last years it represents a distinct category on his own. Special concern must take place on any training program of human resources as the "phishing procedure attacks" estimation was 36% of all data breaches by 2022. https://www.verizon.com/business/en-gb/resources/reports/dbir/

7.1.11 Legal and Compliance Considerations

Data Protection Laws Compliance is necessary to be followed during development and operation of S.I.E.P. Focuses on personal data, individual rights protection and consent and transparency. Addressing all above helps ensure the platform's integrity, security, and adherence to relevant laws.

It involves laws and regulations when we are dealing with personal data and ensures the platform follows principles related to data processing, user content and rights of data subjects. The compliance takes in mind also all the national data protection laws and schema's and issues like cross-border data transfers, electronic communications and e-signatures, compliance with industry standards, legal jurisdictions, consent mechanisms and insurance coverage.

Regulatory Compliance is a critical aspect of operating an information exchange platform, especially considering the sensitive nature of exchanged information. Focuses on broader scope (set of laws and regulations), industry-specific regulations, accessibility compliance aspect and cybersecurity regulations. Regulatory requirements vary across industries and regions, and compliance is essential for legal and ethical operation. Compliance with regulations is a multifaceted task that requires collaboration across legal, IT, and business teams. Regular assessments, updates, and ongoing vigilance are essential for maintaining a compliant information exchange platform. Regular engagement with legal counsel and compliance experts can provide valuable guidance in navigating the complex regulatory landscape.

7.1.12 Redundancy and High Availability

Implementing **Geographic Redundancy** helps prevent downtime, maintain continuous operations and enhance the reliability of the system. The mechanism behind this is very simple. Deploy multiple servers to distribute the S.I.E.P to different geographic locations, data centers, Cloud providers etc.. This procedure guarantees that if something happens to my core service in my main data center the critical service of S.I.E.P will automatically be provided by another one geographic location.

High Availability on the other hand implements load balancing mechanisms to distribute incoming traffic across multiple servers. This method ensures that no single server is overwhelmed, improving overall system performance. Failover mechanisms automatically redirect traffic to healthy servers if one becomes unavailable. Combining redundancy measures with high availability strategies, S.I.E.P can maintain uninterrupted service, even in the face of hardware failures, network issues, or other unforeseen events.

7.2 Secure Information Exchange Platform tailored for Biological/Chemical Terror Attack Incident Management

The big question was if WP7 team could implement **all the above** necessary characteristics to a specific oriented IT platform that will serve the need to exchange information on a biological/chemical terror attack incident. Creating a secure information exchange platform specifically tailored for biological/chemical terror attacks also required careful consideration of the unique challenges posed by such incidents. The platform should facilitate effective communication, collaboration, and information sharing among relevant authorities, emergency responders, and public health agencies with the highest degree of safety and availability. Such a complex and full of high-level safety requirements S.I.E.P wad definitely a challenge for everyone involved.

The first step of data gathering procedure was accomplished during 25th -26th April 2023 workshop (MS50). Using later the available results - as these were presented on evaluation report - it was clear that expertise partner/s on IT sector were not present , but this was not an obstacle for the deliverable creation procedure.

Instead, the conversation focused on general needs of communication exchange channels and the aim was everyone a) to understand what is the scope of D.7.2. and b) retrieve information in every possible way from all involved partners. The need of clarification about deliverable subject (wp7 - D.7.2) was absolutely necessary. The obligation Wp7 team had is to produce a deliverable describing not how we will really built a platform (so, during the conversation we would need technical details, IT expertise in the field, technology terminology, protocols, acronyms and so on) but instead to detect what are the key elements we would possible need to describe such a platform. For example a key element was described as "safe communication" and translated by Wp7 to IT terminology as End2End Encryption, SSL/TLS, HTTPS and so on. Our job as Wp7 team was to merge all the information we gathered and translate it to technical document as Deliverable 7.2 demands. It was the same issue that our team faced during presentation in Umea 25th -26th of May later the same year.

Our approach also involved and produced feedback in layman language like:

" What happens when the first responder arrives at the incident area? Does he have the tools to make a live streaming transmission from the area and provide to Operative Centre/Decision Makers "raw" information for evaluation?"

If answer was "yes" the second part of the question was "channels/apps/protocols used are safe?"

If answer was "no/I don't know" the second part of the question was "Does first responder uses other technology to communicate the incident? Plain GSM call (for example)?

It was easy to detect that information at this level was very difficult to collect. Noone would reveal possible gaps at their communication channels (at least in front of everyone). And lot of participants don't have the ability to collect such kind of information

7.2.1. UI Needs of Provision S.I.E.P Service to End Users

In every conversation and workshop conducted about the needs and abilities platform should include, always was mentioned the need of a safe exchange information "tool" targeting personnel involved to face the biological/chemical terror attack incident but with no access to computers. Also, these human forces need more mobile communication abilities including exchange voice/data/video information from the 'hot zone' incident occurred and around it. This is the reason developers of S.I.E.P must calculate this very important need and provide to end users also the mobile version of the service.

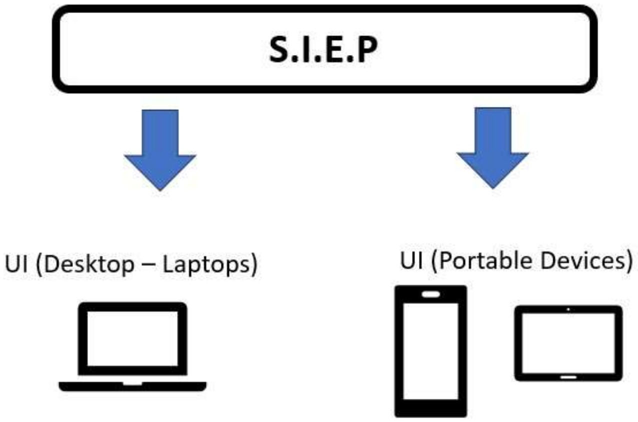


Figure 9. **User Interfaces**

7.2.2. Real-Time Incident Reporting Service

The S.I.E.P must provide to users having responsibility of reporting such an incident (first responders, law enforcement, civil protection etc.) the ability to quickly report biological/chemical incidents with detailed information, including location, nature of the threat, and potential casualties. Based on that, the services needed for such a critical service must include different and more sophisticated tools focused on security, instant times of reporting, easy to use service interface and multi data gathering abilities. The user interface of Real-Time Incident Reporting Service must be **User-Friendly** ensuring straightforward and easy navigation with quickly access to the incident reporting service. The personnel using such a critical service must have a **clear and concise instruction** "set" to follow as the seconds are passing from the time the incident happened is deadly important! The service must also provide all possible multimedia **capabilities** for attaching images, videos, sensor data related to the incident, plain voice channels and file exchange methods. Must also include a **Geolocation Integration** allowing capture and transmission of accurate location information for reported incidents utilizing mapping features to visually represent incident locations aiding responders in quick decision-making and resource allocation. Integration with **Sensor Networks** must also be taken into account minimizing delays in incident awareness. Finally the specific service must also provide **integration with Emergency Response Systems** - at least at National Level - providing in real time necessary alert "awareness" to all relevant agencies and Organizations needed to participate in crisis management in order to activate their action plans and prepare for involvement.

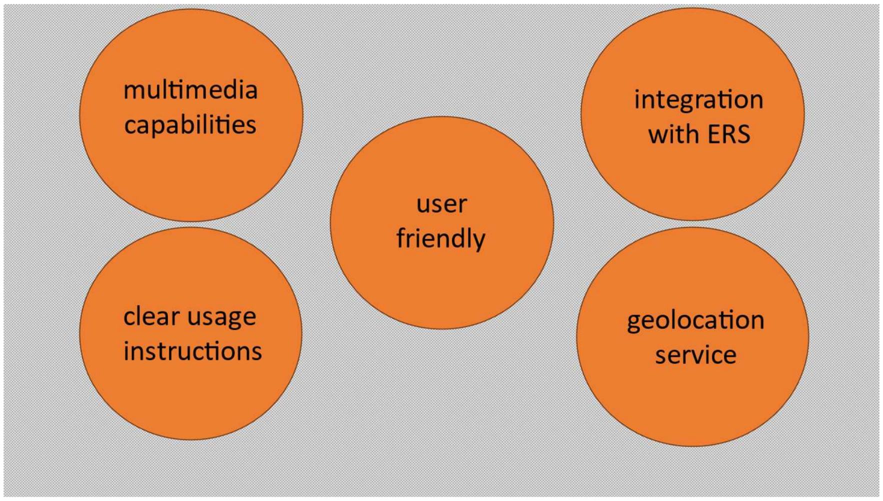
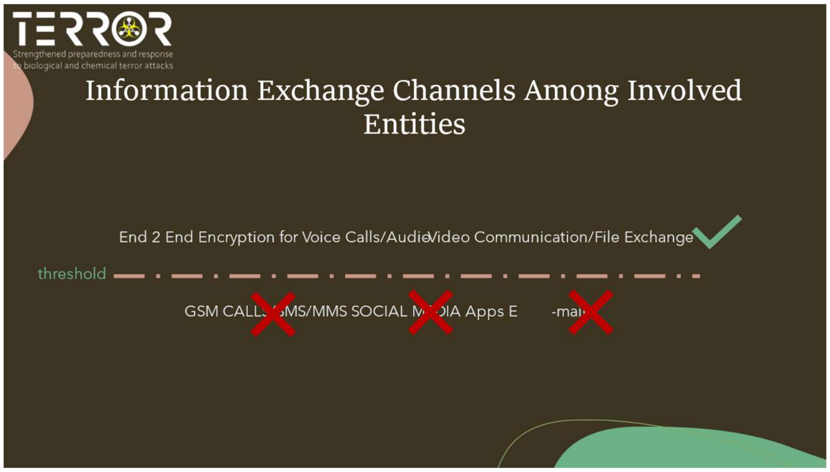


Figure 10. **Real time incident reporting service key elements**

A well-designed Real-Time Incident Reporting Service within a comprehensive risk and crisis communication exchange platform for biological/chemical incidents is a very critical component ensuring a coordinated, efficient, and transparent response to emergencies. Regular updates, user training, and ongoing refinement of the system contribute to its effectiveness over time.

7.2.3. Secure Communication Channels

Implementation of end-to-end encryption for all communication channels is absolutely necessary to protect sensitive information from unauthorized access and ensure confidentiality and integrity of communication. Previous workshops showed -at most of the times - the communication channels among involved entities during the crisis phase was not properly secured to communicate such a sensitive information. In example during the preparedness stage of workshop took place on October 25th -26th 2022 in Athens, representative of entity involved in Risk and Crisis Management biological/chemical incidents admitted that communication in such an event are committed with every possible way in order to disseminate information exchange, "sacrificing" security for immediate time transmission. This was exactly the reason that on Umea meeting on May 25th-26th 2023, WP7 team during presentation time of IT platform requirements showed the image below defining the threshold and above of all communication channels should involved entities use during the procedure of facing the attack. It was crystal clear as an absolute necessity the use of security protocols and encryption schemes and nothing less.



Information Exchange Channels Among Involved Entities

End 2 End Encryption for Voice Calls/Audio/Video Communication/File Exchange ✓

threshold

GSM CALLS ✗ SMS/MMS SOCIAL MEDIA ✗ Apps E-mail ✗

Figure 11. **Communication channels safety threshold**

End-to-end encryption **is a fundamental aspect** of ensuring the confidentiality and integrity of sensitive information exchanged during crises. By addressing key considerations, challenges, and integrating it with other security measures (for example multifactor authentication, access control), a risk and crisis communication exchange platform can provide a secure environment for effective and confidential communication. As an end-to-end encryption we can describe every security measure that ensures the confidentiality of data by encrypting it at the source (sender) and decrypting it only at the destination (intended recipient) while - at the same time - data remains encrypted and unreadable by intermediaries, including the platform provider, as it travels from the sender to the recipient. Key components of such a protocol includes encryption algorithms - for example AES, TLS - and key exchanges techniques (public and private) between source and receiver.

AES stands for Advanced Encryption Standard. Its a symmetric key algorithm, meaning the same key is used for both encryption and decryption. This key is typically referred to as the secret key or symmetric key with sizes of 128, 192, and 256 bits. The larger the key size, the stronger the encryption, but also more computationally intensive. AES operates on fixed-size blocks of data with block size 128 bits. The algorithm uses a fixed number of rounds for processing the data, with the number of rounds depending on the key size. For example, 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

TLS stands for Transport Layer Socket. Its a cryptographic protocol designed to provide secure communication over a computer network. TLS succeeds and builds upon the earlier SSL (Secure Sockets Layer) protocol. The primary goal of TLS is to ensure the privacy and integrity of data exchanged between two communicating applications, such as a web browser and a server (server/client model) . Encrypts the data transmitted between the client and the server, preventing unauthorized parties from eavesdropping on the communication. It uses various encryption algorithms (AES for example), and the choice of algorithm depends on the negotiated cipher suite between the client and the server

Its very common the combination of such encryption algorithms/protocols with - most of the times - AES as part of the encryption process within TLS. TLS ensures secure communication by providing a framework for key exchange, authentication, and encryption, and AES is the "responsible" encryption algorithm that can be used within TLS for securing the data being transmitted.

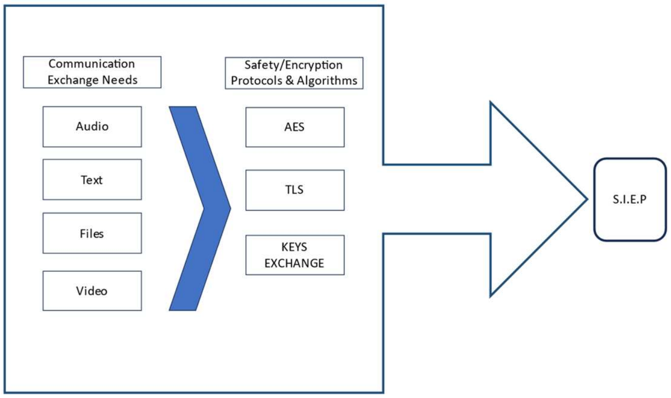

Communication Exchange Needs
Audio
Text
Files
Video
Safety/Encryption Protocols & Algorithms
AES
TLS
KEYS EXCHANGE
S.I.E.P

Figure 12. **Basic Elements of S.I.E.P**

So, nothing less than ultimate encryption and safety but how is it possible to achieve such a security on exchange layer among involved entities horizontally in every aspect of the communication channels when at the same time we want to transmit information from the first responders (audio/video), outcomes and instructions from decision makers, valuable info from law enforcement services and so on, in different geographic locations? First responders are on the incident area, operative centres are spread on different headquarter facilities, ministries and government services are on distinct also buildings .Is it possible all of them to communicate with maximum safety and use the same channel?

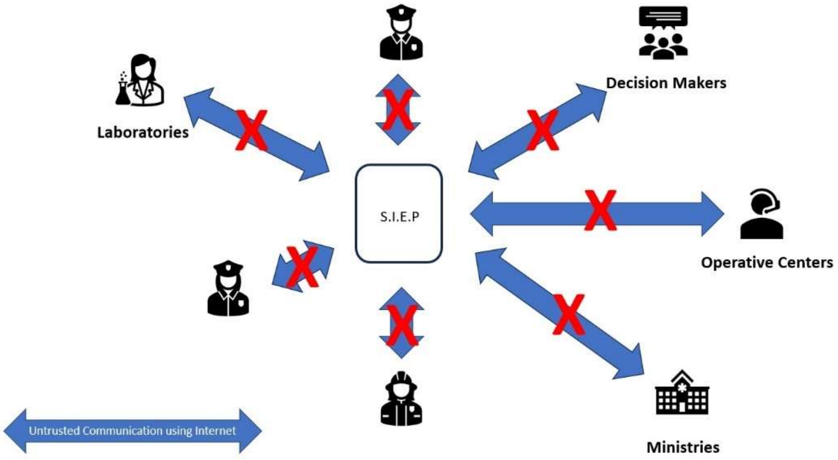


Figure 13. **Approaching S.I.E.P Remote End Users Access Problem**

Obviously using internet as-it-is service isn't a safe way of communication even if we are using such a strong encryption algorithms and protocols on our infrastructure. Satellite communications channels maybe? Military communications channels? Mesh networks as Proactive Project used? A lot of options to take in mind with each one of the referred approach having advantages and disadvantages! But the purpose of this deliverable is (also) to describe the best solution with the least expense/cost/complication/load and provide a cheap, possible and secure option of communication among every involved "entity" needs to have access on every way! The solution on this is the magic acronym VPN.

A Virtual Private Network (VPN) is a technology that provides a secure and encrypted connection over the internet, allowing users to access resources and services as if they were connected to a private network, even if they are physically located elsewhere. VPNs are commonly used for enhancing privacy and security, especially when accessing the internet from public networks or untrusted environments. A VPN encrypts the data transmitted between a device (computer, smartphone, etc.) and the VPN server. This encryption ensures that even if someone intercepts the data, they won't be able to understand or tamper with it without the appropriate decryption key. It uses a process of encapsulating the encrypted data within a secure "tunnel" known as tunneling. This provides a protective layer for data as it traverses the internet. This tunneling process shields the data from potential threats and ensures its confidentiality. OpenVPN is an open-source and highly configurable protocol known for its robust security. It supports various encryption algorithms and is adaptable to different network configurations such as:

L2TP/IPsec (Layer 2 Tunneling Protocol with IPsec): L2TP provides the tunnel, and IPsec adds a layer of security through encryption. It's commonly used for a balance of speed and security.

IKEv2/IPsec (Internet Key Exchange version 2 with IPsec): Known for its speed and ability to quickly re-establish connections if they are temporarily lost.

PPTP (Point-to-Point Tunneling Protocol): An older protocol with weaker encryption; not recommended for secure data transmission.

Also, VPN service is provided as:

Remote Access VPN: Allows individual users to connect to a private network from a remote location securely.

Site-to-Site VPN: Connects entire networks, such as branch offices or data centers, creating a secure communication link between them.

Client-to-Site VPN: Similar to remote access VPN, but with a focus on connecting individual devices to a network.

Finally, the basic VPN Components are:

Client Software: Installed on the user's device, it manages the secure connection to the VPN server.

VPN Server: Operated by the VPN provider, it handles user connections and data encryption/decryption.

Protocols and Encryption Algorithms: Define the rules and methods for secure communication.(see above AES/TLS)

Authentication Mechanisms: Ensure that only authorized users can access the VPN.

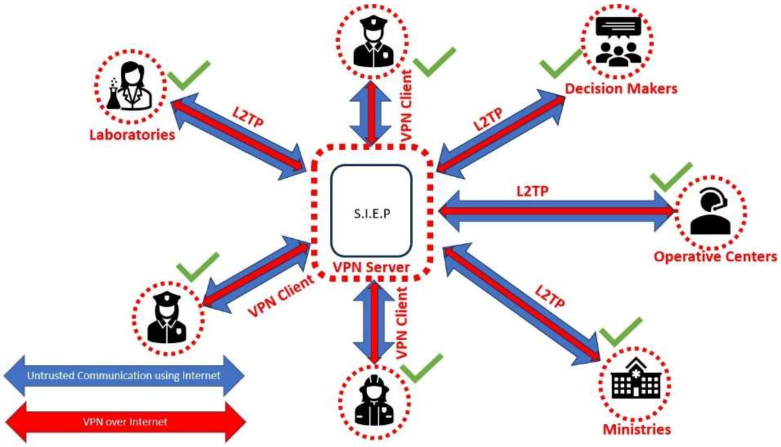


Figure 14. **S.I.E.P Remote Users Access Using VPN**

To put it simple we described so far:

1st: The need to cover all the needs of communication types and formats among involved stakeholders

2nd: The need any of the involved entities use the same strong encrypted channels and nothing less

3rd: The need to provide the communication channel to everyone using something "untrusted" like internet and transform it to a secure exchange channel.

7.2.4. Access Control and Authorization

Access control refers to the practice of restricting or allowing access to information resources based on the identity and attributes of the entities (users, systems, or processes) seeking access. Implementing robust access control is crucial for creating a secure information exchange platform, especially in environments where sensitive data is involved. The basic procedures every S.I.E.P (including tailored platforms to Biological/chemical Incidents management) are:

Identification: Verifying the identity of the entity, often through usernames, passwords, or other authentication methods.

Authentication: Confirming the claimed identity through the presentation of valid credentials.

Authorization: Determining what actions or resources the authenticated entity is allowed to access.

Logging and monitoring access events for audit purposes.

There are three basic access control models with different aspects and benefits each. The Discretionary Access Control (DAC) which allows users to set access permissions on their objects. The owner of an object can decide who has access and what type of access they have. The Mandatory Access Control (MAC): Access decisions are based on security labels assigned to each resource and the user's security clearance and finally the Role-Based Access Control (RBAC) with access granted based on the roles a user has within the system. Users are assigned roles, and roles are associated with specific permissions. The last one was the one presented on Umea by the WP7 team with detail and arguments why and how could be implemented.

7.2.5. Integration with Sensor Networks

Connect a S.I.E.P with sensor networks that can detect biological/chemical agents and provide real-time data on air quality and environmental conditions is an important aspect of such a system. The sensors could be deployed on critical infrastructures such governmental buildings, law enforcement agencies headquarters, warehouses and so on, providing real-time data on environmental conditions, detecting chemical agents, and monitoring potential biohazards. Collecting real-time data on environmental conditions, detecting chemical agents, and monitoring potential biohazards the sensor network could transmit proper signals when they are triggered by a biological/chemical agent and alert the users for taking necessary actions. Examples of such a sensor network could be gas sensors network with ability detect specific gases - such as toxic chemicals or hazardous substances in the air – and Biosensors Network utilizing biological components to detect and quantify chemical substances, often employed in medical or environmental monitoring. Also, the addition of environmental monitoring sensors with temperature or/and humidity variation monitoring abilities offers even more information to the system and makes the procedure of data gathering more efficient.

In real life we found that such sensor networks exists and there are based on "smart cities" model. Singapore for example has already deployed extensive sensor networks for environmental monitoring, traffic management, and public services and Copenhagen has implemented a smart city initiative that includes a sensor network for monitoring air and water quality, noise levels, and traffic. The added value of integrating sensors network abilities to any S.I.E.P is - without any doubt - crucial and necessary to make the system complete and much more useful and effective.

7.2.6. Geospatial Integration

Include geospatial mapping and visualization tools to display the location and spread of biological/chemical threats is one more crucial ingredient of any S.I.E.P. These tools leverage geographic information system (GIS) technology to provide a visual representation of the location such a dangerous incident took place. These tools leverage geographic information system (GIS) technology to provide a visual representation of the location and spread of biological/chemical incidents. Visualization tools allow users to overlay different layers on the map, such as biological/chemical agent concentrations, affected areas, and evacuation zones using different colours or symbols to represent various aspects, such as the severity of the threat, the affected population, or the progression of the incident. Geospatial mapping also enables the identification of spatial patterns in the spread of biological/chemical threats. Patterns may include concentration clusters, direction of dispersion, and areas at higher risk. Combined with prediction models geospatial tools support scenario planning by allowing users to model the potential spread of biological/chemical threats based on different parameters, such as wind direction, terrain, and population density and help decision-makers to anticipate the likely trajectory of the threat and optimize resource allocation. Finally, mobile mapping applications enable field personnel to collect and update data in real-time using smartphones or tablets with GPS technology ensuring accurate location tracking and enhances situational awareness for on-the-ground responders.

7.2.7. Laboratory Information Management System (LIMS)

LIMS plays a vital role in managing and exchanging laboratory-related information during biological/chemical terror attacks. Efficient integration with the S.I.E.P helps tracking and management of biological/chemical samples collected during investigations. The fast collection, travel and analysis of such a kind samples plays crucial role on determining the immediate measures decision and first responders should take in order to control the situation with the less possible casualties and side-effects. The combination of real-time data from environmental sensors and detectors helps to correlate sensor data with laboratory results for a comprehensive understanding of the incident. The propagation of results to all necessary involved entities such as hospitals, ministries, pharmaceutical warehouses and so on helps to contaminate the incident to a small area as possible.

7.2.7.1. Collaboration with Public Health Systems

In the event of a biological or chemical terror attack, collaboration with public health systems becomes paramount for effective response and mitigation efforts. The integration of public health systems into emergency response protocols enables authorities to leverage their expertise, resources, and infrastructure to address the unique challenges posed by such attacks.

Public health systems play a crucial role in detecting, monitoring, and containing outbreaks of infectious diseases, including those resulting from biological or chemical agents. Their expertise in epidemiology, disease surveillance, and risk assessment is invaluable in assessing the extent of the threat, identifying affected populations, and implementing appropriate public health interventions. Collaboration with public health systems also facilitates the rapid dissemination of critical information to healthcare providers, first responders, and the general public. Timely and accurate communication is essential for coordinating response efforts, providing guidance on preventive measures, and minimizing the spread of panic and misinformation.

However, in some cases, direct collaboration with public health systems may not be feasible due to logistical challenges, jurisdictional issues, or other constraints. In such scenarios, wp7 team concluded that the use of Application Programming Interfaces (APIs) can serve as a viable alternative to facilitate data exchange and interoperability between different systems.

7.2.8. Integration with emergency alert systems for widespread communication.

One more crucial element/service is the integration of emergency alert systems in the above described S.I.E.P. Some percentage of information should be disseminated not only inside the entities that share the same communication channels in S.I.E.P but also outside of them. For example a notification message - short information message - should trigger the "official public information service" (ministry of press, communication experts representatives of proper authorities, etc.) to start communicate the incident with the proper way to the public. At the same time S.I.E.P should also help involved entities have control of situation: "information flow" as much as possible.

Let's add more details: In a case of Biological/chemical terror attack two incidents happens at the same time.

The first is the incident itself, the biological/chemical agent, the safety of the people in the area incident took place, the side effects of biological/chemical agent ,first measures, area isolation and so on. At the same time another "incident" also happens in the binary world with the cell phones of people witness the incident propagate information on the social networks, web, press, providing photos, videos, plain phone calls in real time, interpretation of the incident, comments and so on! Two stories running on the same timeline with a lot of similarities and also a lot (and very important) differences.

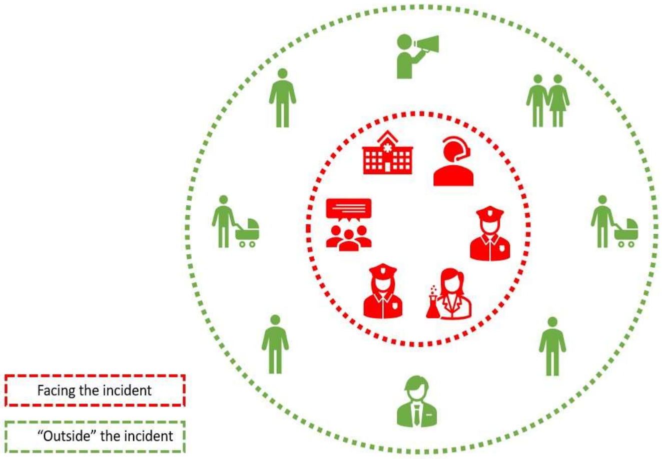
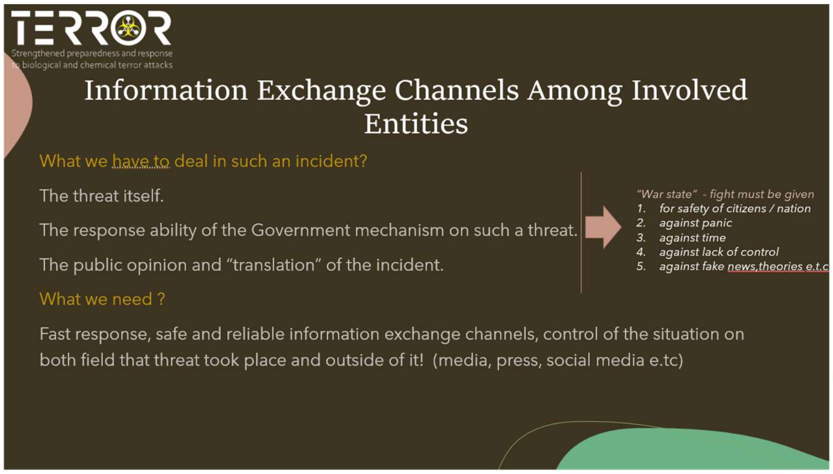


Figure 15. **Bubble of "entities" involved facing a Biological/Chemical terror Attack & Public**

In reality defense and response mechanism of every nation has to face this two-sided "war". In one hand the biological/chemical terror attack incident itself and the side effects it causes and in the other hand is what people see/feel/react on the incident field or not. How they "translate" the incident, the facts and so on. Each nation facing a biological/chemical terror attack clearly enters" war state" as we presented on Umea workshop!



TERROR
Strengthened preparedness and response to biological and chemical terror attacks

Information Exchange Channels Among Involved Entities

What we have to deal in such an incident?

The threat itself.

The response ability of the Government mechanism on such a threat.

The public opinion and "translation" of the incident.

"War state" - fight must be given

1. *for safety of citizens / nation*
2. *against panic*
3. *against time*
4. *against lack of control*
5. *against fake news,theories e.t.c*

What we need ?

Fast response, safe and reliable information exchange channels, control of the situation on both field that threat took place and outside of it! (media, press, social media e.tc)

Figure 16. **Entering "War State"**

The suggested S.I.E.P here is the invisible star of collection information procedure. It must have the abilities of gathering information of what happens ALSO outside the "bubble - facing the incident - entities" and put a.s.a.p. the fire down started by misinformed people with truth and undeniable facts.

7.2.8.1 – Collecting Information "Outside" S.I.E.P.

Creating a social media/web/press gathering information subsystem during a biological/chemical attack is crucial and involves specialized considerations due to the urgent nature of the situation. Such a subsystem could play a vital role in collecting, analyzing, and disseminating information relevant to the incident and the impact of the incident in public. It should Implement real-time monitoring of social media platforms for mentions, posts, and updates related to the biological/chemical incident integrating social media APIs to collect data rapidly. It should also incorporate tools for analyzing images and videos posted on social media to identify visual evidence and assess the severity of the situation. For example, image analysis tools like Google Cloud Vision API, Microsoft Azure Computer Vision, Clarifai, or Google Cloud Video Intelligence API for video analysis and Open Source based tools like Open-Source Computer Vision Library providing tools for image and video analysis, including object detection, image processing, and feature extraction are some of the "ingredients" every IT architect should take in mind. Ability of geospatial tracking to identify the location of posts and updates, helping responders understand the spread of information and incidents is also a must have option. Utilize sentiment analysis to gauge public sentiment and emotions expressed on social media platforms which could help authorities understand the public's perception of the situation. At the same time monitor emergency hashtags and keywords related to the biological/chemical incident to ensure comprehensive data collection. Artificial Intelligence (AI) in decision-making using public emotions and reactions involves leveraging advanced technologies to analyse and interpret sentiments, opinions, and behaviours expressed by the public. This application of AI is commonly referred to as Sentiment Analysis or Opinion Mining. Sentiment analysis involves using natural language processing (NLP) and machine learning algorithms to determine the sentiment (positive, negative, or neutral) expressed in text data, analyzing social media posts, news articles, and public comments to gauge the overall sentiment towards a particular topic, event, or product. Predictive analytics using AI models can forecast future trends based on historical sentiment data, predicting potential shifts in public opinion, allowing decision-makers to proactively respond

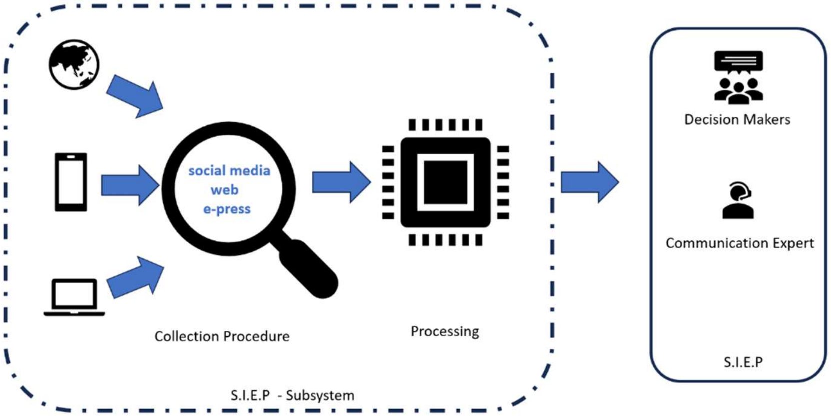


Figure 17. **Collecting Information from Social Media, Web, E - press**

At the same time enable two-way communication between responsible communication authorities and the public, allowing users to report incidents, ask questions, and receive official responses is also a must have service. The ability of a S.I.E.P tailored to Biological/chemical Terror Attack to provide such a ability of collecting information of "what is happening out there" during the incident and also provide critical information in minimum time to decision makers, communication experts and so on **is so important as the incident itself!**

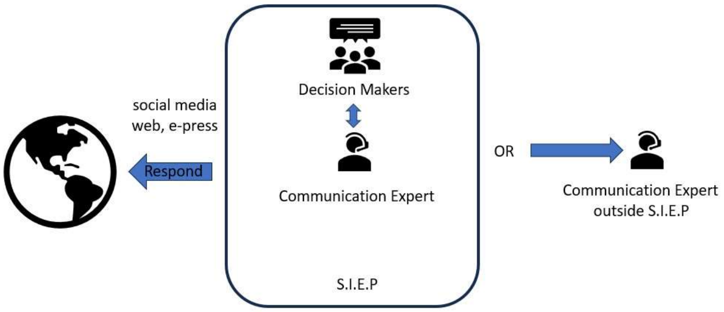


Figure 18. **Information Process and Respond**

A lot of opinions were exchanged among partners of JA Terror during workshops in Umea and Athens. We discovered that in lot of cases, Nations were not so "positive" to exchange information with other Nations if a biological/chemical incident happens. They wanted first to take control of the situation, recognize what they are dealing of, take first measures and only then (and may be) put the information on communication exchange channels with other countries. One of the questions needed to be answered also is if it is possible to use existent communication channels such as EWRS to disseminate information in case of biological/chemical incident . The answer is definite YES! Every modern web based platform has the ability (or it can be added/activated later) to integrate API technology for robust, safe and instant information exchange. But.. what is an API?

7.2.8.2 Application Programming Interfaces - API's

An Application Programming Interface, or API, is a set of rules and protocols that allows one software application to interact with or access the features, data, or functionalities of another software application, service, or platform. APIs act as intermediaries, enabling different software components to communicate with each other, share information, and perform specific tasks. An API defines the methods and data formats that applications can use to request and exchange information and enables the integration of different software systems, allowing them to work together seamlessly, share data, and perform actions. There are three basic types of API technology: Web APIs, allowing communication over the web and are commonly used for web and mobile app development, Library APIs, providing a set of functions and procedures that can be used by applications written in the same programming language and Operating System APIs, allowing applications to interact with the underlying operating system, accessing resources like file systems or hardware. The basic components of API's technology are:

Endpoints -> Specific URLs or URIs (Uniform Resource Identifiers) that define where API requests can be made,

Methods -> Actions or operations that can be performed, such as GET (retrieve data), POST (submit data), PUT (update data), or DELETE (remove data).

Request and Response -> The format in which data is sent (request) and received (response), often in JSON or XML.

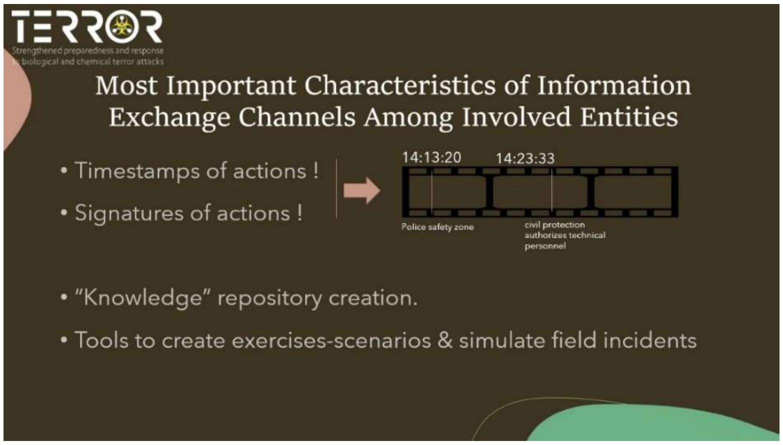
So, how API's working? An application makes a request to an API endpoint, specifying the desired action and any required parameters. The API processes the request and sends back a response with the requested data or the outcome of the action often using HTTP or HTTPS protocols for communication, leveraging standard methods like GET and POST. APIs may also require authentication, ensuring that only authorized users or applications can access the provided functionalities using API Keys and Tokens. Finally RESTful API is an architectural style for designing networked applications which use a set of principles and constraints to facilitate communication and interaction between systems. The above technology provides the ability of interaction, accessing features, data, or functionalities among different software applications and platforms.

7.2.9. Secure Data Storage and Evaluation Procedure.

Ensuring the secure storage of sensitive information related to biological/chemical incidents is paramount to protect both individuals' privacy and national security. All the information exchanged over the S.I.E.P must be kept confidential and at the same time available to authorized personnel for evaluation and traceroute procedures. Implement strong encryption algorithms to protect sensitive data, both in transit and at rest and use industry-standard encryption protocols (e.g., AES) to encrypt data stored in databases, file systems, and during transmission is a must have. But besides the strong encryption algorithms and safety of all the information stored in the platform there is also one more very important aspect. The evaluation procedure.

Using such a system gives the ability to proper users evaluate the steps and procedures each involved entity, physical person, authority took while everyone was dealing with the incident. The system could provide timelines of actions, logs, timeframes, signatures of actions etc. making the incident itself one of the most valuable training sessions any involved entity could ever take based in real facts!

This "feedback" procedure could improve the actions of each one involved entity and make the respond procedure on biological/chemical incidents more reliable, effective and fast. Also it would provide a repository of knowledge for similar events or even scenario based simulation exercises providing valuable information.



TERROR
Strengthened preparedness and response to biological and chemical terror attacks

Most Important Characteristics of Information Exchange Channels Among Involved Entities

- Timestamps of actions !
- Signatures of actions !

14:13:20
14:23:33
Police safety zone
civil protection authorizes technical personnel

- "Knowledge" repository creation.
- Tools to create exercises-scenarios & simulate field incidents

Figure 19. **Umea Workshop - Evaluation Procedure**

7.2.10. User Training, Awareness and Simulation Modules.

Every system is as much safe as the persons use it! A simple truth undeniable correlated with the IT platforms users are working on. It doesn't matter how safe a system is and what precautions IT architects took in mind when they built it if users are not able to use it properly with safety. They are the "living" variable on every IT Platform and they must be very well trained in using such sophisticated systems with maximum safety, minimum effort for them and maximum efficiency. This is the main reason that human factor plays so important role. Provide comprehensive training for platform users on security protocols, response procedures and raise awareness about the potential risks and challenges associated with biological/chemical incidents is a critical element. Develop training modules and simulation tools to prepare responders for biological/chemical incidents is also crucial. It's absolutely necessary platform users take advantage all the abilities system provides with minimal effort from their side providing a user interface (UI) easy to navigate, simple and role oriented in any aspect of it. Less is more once again!

7.2.11. Privacy Protections – Legal and Ethical Considerations

When a Biological/chemical incident occurs, national systems must be ready and well prepared to face such a threat. At the same time the respond mechanism must be aligned with the legal framework, data protection laws and regulations establishing measures to protect the privacy of individuals affected by biological/chemical incidents. Defining specific data categories that are essential for emergency response and strictly limit the collection of personal information or (if possible) replace identifiable information with pseudonyms and remove unnecessary details before storing or sharing data is a variable that must be taken in mind. Finally address legal and ethical considerations related to the handling of sensitive information and the response to biological/chemical terror attacks and comply with relevant laws and regulations governing emergency response.

7.2.12. Cybersecurity Measures

Implementing robust cybersecurity measures is crucial to protect an information exchange platform, especially in scenarios involving sensitive information related to biological/chemical incidents. The VPN technology guarantees in maximum degree the safety of information exchanged over the S.I.E.P but this is just one of the many measures every IT architect builder should take in mind.

Some of the most important security aspects such a system should include are:

Deployment of firewalls to monitor and control incoming and outgoing network traffic allowing only necessary traffic, block unauthorized access, and prevent malicious activities is absolute necessary.

Regular security audits and penetration tests to identify and address vulnerabilities.

Hire cybersecurity professionals perform thorough assessments of the platform's security posture.

Implement IDPS (Intrusion Detection and Prevention Systems) to detect and respond to suspicious activities and potential security breaches.

Secure endpoints (devices accessing the platform) against malware and unauthorized access.

Developers should use secure coding practices, conduct code reviews, and use automated tools to identify and fix security issues during the development lifecycle.

Establish a patch management process to regularly update and patch all systems. Prioritize critical security patches.

Regularly update security protocols to address emerging vulnerabilities.

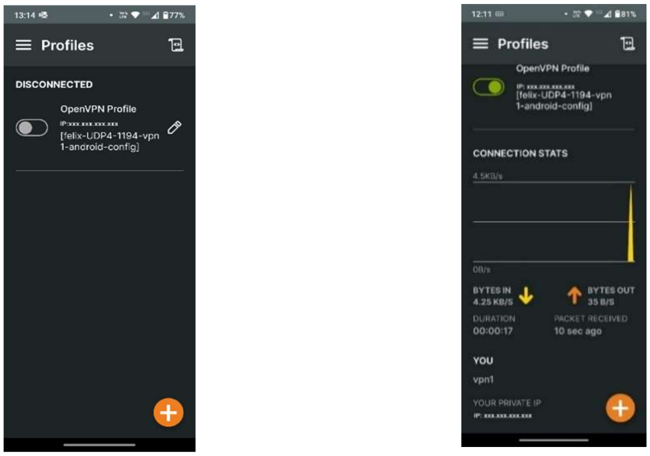
Maintain documentation for audit trails and compliance reporting.

Implementing such cybersecurity measures collectively forms a comprehensive strategy to protect the information exchange platform from a wide range of cyber threats. It's an unstoppable obligation for Administrators of such systems to regularly review and update these measures to adapt to emerging threats and ensure a proactive cybersecurity posture

7.2.13. Secure Mobile Applications

As described earlier (7.2.1.) the development of a S.I.E.P implements two major UI's. The first one concerns the "core" services of the platform with all the available services ready to use and be provided to final users. Core services are provided using VPN technology to all the necessary users with computer web browser access. The other is the mobile app. The mobile app should be provided also using the VPN technology to end users with no easy access to full browser capabilities and with intensive needs of voice, video and file communication by default. For example, first responders at the "hot zone" incident occurred and police / fire officers moving all the time to collect and transmit information to their operational centres.

The mobile device (Android or IOS based device) using a particular VPN client app will be able to access the needed services S.I.E.P offers. These are the same services S.I.E.P provides but in more "poor" and operative format focusing on simplicity in use. At the time the terminal device enters VPN channel every other communication ability of the mobile device stops, and all traffic is enforced to travel through VPN channel. This is succeeded using "force tunnel configuration" on VPN server which forces every client needs to access the S.I.E.P. (This tunnel configuration is also applied on desktop-laptops terminal devices with exactly the same impact on them.)



13:14 77%

Profiles

DISCONNECTED

OpenVPN Profile
IP:xxx.xxx.xxx.xxx
[felix-UDP4-1194-vpn
1-android-config]

12:11 81%

Profiles

OpenVPN Profile
IP: xxx.xxx.xxx.xxx
[felix-UDP4-1194-vpn
1-android-config]

CONNECTION STATS

BYTES IN
4.25 KB/S

BYTES OUT
35 B/S

DURATION
00:00:17

PACKET RECEIVED
10 sec ago

YOU
vpn1

YOUR PRIVATE IP
IP: xxx.xxx.xxx.xxx

Figure 20. **Screenshots of Open VPN Client with profile ready to be used.**

In the above figure we present an installed vpn client during the verification procedure of this deliverable. The client app and testing configuration was installed in Android 13 OS based device for testing reasons.

7.2.14. Continuous Improvement and Updates

Every system is "alive", and it is imperative that we perceive it as such. It should be in a constant state of evolution, never ceasing to adapt emerging technologies. Should any internal audits breach the security threshold, IT builders must promptly initiate the necessary updates. Concurrently, human resources, who serve as users of the provided services, must continuously undergo updates and improvements. The improvement process should be approached and addressed as a cohesive entity, closely paired with procedural enhancements to ensure seamless advancement.

7.2.15. Special Considerations, Sustainability and Modular Architecture Approach

It's crystal clear that a Secure Information Exchange Platform tailored to Biological/chemical Terror Attack includes all the elements of such a system should have (strong encryption, physical security of infrastructure and terminal devices, secure communication channels etc.) but must also include some very specialized - for this particular scope - elements (for example integration with sensor networks or geospatial abilities)

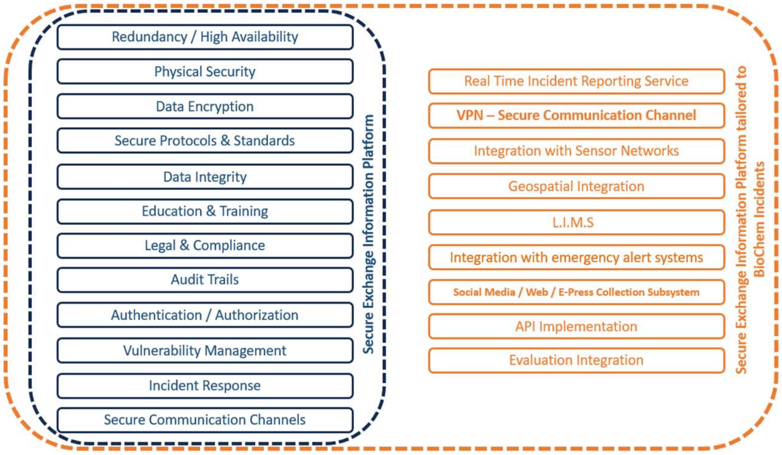

Redundancy / High Availability
Physical Security
Data Encryption
Secure Protocols & Standards
Data Integrity
Education & Training
Legal & Compliance
Audit Trails
Authentication / Authorization
Vulnerability Management
Incident Response
Secure Communication Channels
Secure Exchange Information Platform
Real Time Incident Reporting Service
VPN – Secure Communication Channel
Integration with Sensor Networks
Geospatial Integration
L.I.M.S
Integration with emergency alert systems
Social Media / Web / E-Press Collection Subsystem
API Implementation
Evaluation Integration
Secure Exchange Information Platform tailored to BioChem Incidents

Figure 21. **Common S.I.E.P vs Tailored to Biological/chemical Terror Attacks S.I.E.P.**

It's also a challenge to build such a system and even more challenging is to keep it up and running.! Biological/chemical terror attacks are not happening very often and we can not rely only to periodic use of such sophisticated system to have it active and ready for use. The best way to keep it alive is to use it!

Questions arise and a lot of doubt on this approach starts to be present!

"How can this happen? Is really possible?",

" Can this happen without affecting the operative ability of the defense mechanism of every nation/ entity?",

*"I don't want all of these! I need only this ….service!.", …….*and a million more appears!

Lets try to answer some of the most important justified worries with the following QA's section everyone is having in his mind.

Q: How can this happen ?

A: Well, the proposed solution is to use such a unique complete communication platform for all the entities involved on the defense mechanism of every nation (for example police, civil protection and so on). The benefits of a unified approach are truly endless with the most important of them described as:

Improved Coordination: Having all relevant entities on a single platform allows for seamless communication and coordination between different branches of defence, such as police, civil protection, military, and emergency services. This facilitates faster response times and more effective collaboration during crises or emergencies.

Enhanced Situational Awareness: A unified communication platform provides real-time updates and information sharing among all stakeholders. This allows decision-makers to have a comprehensive understanding of the situation, enabling better-informed decisions and more effective resource allocation.

Streamlined Processes: Standardizing communication protocols and procedures across different defence entities reduces confusion and improves efficiency. This streamlines processes such as reporting incidents, requesting assistance, and coordinating operations, leading to quicker response times and better outcomes.

Resource Optimization: By sharing resources and information across different defence entities, duplication of efforts can be minimized, and resources can be allocated more effectively based on priority and need. This can result in cost savings and a more efficient use of available resources.

Improved Interagency Collaboration: Bringing together different defence entities onto a single platform fosters closer collaboration and integration between agencies that may have traditionally operated independently. This enables a more holistic approach to defence and security, with agencies working together towards common goals.

Better Communication with the Public: A unified communication platform can also facilitate better communication with the public during emergencies or crisis situations. It allows for timely dissemination of information, updates on safety measures, and instructions on how to respond to specific threats, enhancing public safety and trust in the defence mechanism.

Implementing a single complete communication platform for all defence entities can greatly enhance the effectiveness, efficiency, and responsiveness of a nation's defence mechanism.!

The example we described on this "ideal communication world" among all EU Nations on Zagreb Workshop was this:

1) We create an app/webservice (Lets name it "EUExch").

EUExch is provided for use using private channels (not in app stores).

EUExch shares military grade safety characteristics, modular architecture, encryption algorithms and so on..

Every EU Nation deploys distinctively EUExch and allows access only to National "entities"

2) All the EU Nations use the EUExch platform. During the use of the platform authorized users could communicate with any other user on National level. If information needs to be propagated outside the National stakeholders, law enforcement and so on "propagation information procedure is activated on demand" .

Q: What is the main achievement on such an approach?

***A:** A new commonly accepted "language". Now we can all communicate because we all speak English! (if we borrow the example of natural speaking language). Its possible to exchange information with no need for API's , system "translations/conversions", incompatibilities among different systems protocols and platforms, safety "gaps" and so on. Take a minute to think about this: If we were sitting on a table and each one of us spoke his national language would be possible to exchange information? Of course no! And this takes us to the next question:*

Q: But is this really possible to be adapted? Systems already exists on every aspect of involved entities in case of biological/chemical incident!

A: Implementing a single complete communication platform for all involved entities may indeed present challenges, especially considering the existing systems in place and the complexities involved in coordinating different agencies. However, there are several strategies that can help facilitate the adaptation of such a system:

Gradual Integration: Rather than implementing a complete overhaul of existing communication systems, a gradual integration approach can be adopted. This involves integrating different defence entities onto the new platform in phases, allowing for smooth transition and minimizing disruptions to existing operations. Also, developing interoperability standards and protocols that allow different systems to communicate and share information seamlessly is essential, ensuring existing systems can still function while being able to exchange data with the new platform.

Stakeholder Engagement: Engaging with key stakeholders, including leaders from different defence agencies, policymakers, and technology experts, is important throughout the planning and implementation process. Their input and support can help address concerns, garner buy-in, and ensure the success of the project.

Pilot Programs and Testing: Conducting pilot programs and testing the new communication platform in real-world scenarios allows for identification of any potential issues or challenges and provides an opportunity for refinement before full-scale implementation.

While adapting a single complete communication platform for all defence entities may pose challenges, careful planning, collaboration, and strategic implementation can help overcome these obstacles and realize the benefits of a more integrated and efficient defence mechanism.

Q: I don't need such a "complete" system. I want to adapt only one particular service! (For example) social media / e-press information collection subsystem!

A: This is the reason that our proposed S.I.E.P tailored to biological/chemical incidents provides all the necessary services in modular architecture. With this approach every Nation / entity can adapt any missing service based on his needs. The modular architecture used on this deliverable provides:

Scalability: Modular architectures allow systems to scale more easily. By breaking down a system into smaller, independent modules or services, it becomes simpler to add or remove components as needed, enabling the system to adapt to changing requirements and handle increased workload without compromising performance.

Flexibility and Adaptability: With a modular architecture, each service can be developed, deployed, and maintained independently. This flexibility allows for easier updates, enhancements, and bug fixes without affecting other parts of the system. It also enables organizations to adopt new technologies or replace outdated components more seamlessly.

Simplified Development and Maintenance: Modular architectures promote a more organized and structured approach to development. By dividing a system into smaller, more manageable modules, development teams can focus on building and maintaining specific functionalities or services, leading to faster development cycles, improved code quality, and easier debugging.

Reuse of Components: Well-defined services in a modular architecture can be reused across different parts of a system or even in entirely different projects. This promotes code reuse, reduces duplication of effort, and accelerates development timelines. Additionally, it ensures consistency and standardization across the system.

Improved Collaboration: Modular architectures facilitate collaboration among development teams by providing clear boundaries and interfaces between different services. Teams can work on individual modules concurrently without interfering with each other's work, leading to better productivity and coordination.

Fault Isolation and Resilience: In modular architectures, failures or issues in one service are less likely to impact other parts of the system. This fault isolation improves system resilience and reliability, as failures are contained within individual modules and do not propagate throughout the entire system.

Easier Testing and Debugging: Each module or service in a modular architecture can be tested independently, allowing for more thorough testing and easier identification of issues. This simplifies debugging processes and ensures that changes or updates to one service do not inadvertently introduce regressions in other parts of the system.

Overall, a modular architecture with distinct and well-described services offers numerous advantages in terms of scalability, flexibility, development efficiency, collaboration, fault tolerance, and maintainability, making it a preferred approach for building complex and robust software systems.

Using this approach its very easy to adapt the missing element every nation /involved entity needs and embed it on national working service repository.

8. Risk Assessment

Conducting a risk assessment of a "tangible secure platform for rapid information exchange between sectors" involves evaluating the various potential risks associated with the physical infrastructure, data security, privacy, and operational efficiency. Here is a structured risk assessment for such a platform:

Table 7. Risk Assessment

Risk	Impact	**Probability**	Mitigation	Others
1. Security Risks				
a. Physical Security Breaches**:** **Unauthorized physical access to the platform's hardware.**	Theft, tampering, or destruction of hardware leading to data loss and service disruption.	High	Implement physical security measures like surveillance, secure access points, and security personnel.	
b. Cyber Attacks: **External cyber threats such as hacking, malware, or DDoS attacks.**	Compromise of data integrity, leakage of sensitive information, and operational downtime.	High	Use of firewalls, intrusion detection systems, regular security updates, and strong encryption protocols.	
c. Insider Threats: **Malicious or negligent actions by employees or authorized users.**	Data breaches, unauthorized access, and potential sabotage.	Medium	Implement strict access controls, employee training, and monitoring of user activities.	
2. Privacy Risks				
a. Confidential Information Exposure: **Unintentional or intentional exposure of**	Regulatory non-compliance, loss of trust, and potential legal actions.	High	End-to-end encryption, secure data storage solutions, and compliance with privacy regulations.	

sensitive information during transmission or storage.				
b. Data Handling and Processing: **Improper handling, processing, or sharing of data.**	Data breaches, privacy violations, and legal consequences.	High	Establish clear data handling policies, regular audits, and ensure data minimization principles.	
3. Operational Risks				
a. Infrastructure Failures: **Hardware or software failures leading to downtime or data loss.**	Interruption of information exchange and operational inefficiencies.	Medium	Regular maintenance, redundant systems, and robust disaster recovery plans.	
b. Scalability Challenges Risk: **Inability to handle increased demand or expanded operations.**	Performance degradation and delayed information exchange.	Low	Scalable infrastructure design, performance monitoring, and capacity planning.	
4. Compliance Risks				
a. Regulatory Non – Compliance: **Failure to adhere to specific regulations and standards.**	Legal actions, and operational restrictions.	Medium	Regular compliance audits, adherence to standards, and legal consultations.	
b. Cross-Sector Regulations: **Complexities arising from different regulatory requirements across sectors.**	Legal challenges and operational inefficiencies.	Medium	Comprehensive regulatory mapping, cross-sector agreements, and adaptable compliance strategies.	
5. Reputation Risks				

a. Public Trust: **Loss of public trust due to perceived or actual security incidents.**	Decreased platform adoption and potential user attrition.	Low	Transparent communication, proactive incident response, and ongoing improvements in security measures.	
b. Stakeholder Confidence: **Erosion of confidence among stakeholders due to operational failures or security breaches.**	Loss of partnerships, investment, and collaboration opportunities.	High	Regular stakeholder engagement, robust risk management practices, and performance transparency.	
6. Technological Risks				
a. Technological Obsolescence: **Platform becoming outdated due to rapid technological advancements.**	Reduced competitiveness and increased operational costs.	High	Continuous technological upgrades, research and development investment, and staying updated with industry trends.	
b. Integration and Interoperability Issues: **Challenges in integrating with other systems or platforms used by different sectors.**	Reduced functionality and user frustration.	High	Adoption of standard protocols, APIs, and ensuring compatibility with other systems.	

A comprehensive risk assessment of a tangible secure platform for rapid information exchange between sectors must address physical security, cyber security, privacy, operational efficiency, compliance, reputation, and technological advancements. Implementing robust mitigation strategies for these risks is crucial to maintaining the platform's integrity, security, and efficiency. Regular reviews and updates to the risk management plan are essential to adapt to evolving threats and ensure continuous improvement.

9. Conclusions

Each EU nation faces the critical task of evaluating its exchange information systems in preparation for potential biological/chemical terror attacks, necessitating careful consideration of several key factors. Firstly, the safety and security of existing systems must be thoroughly assessed to ensure they can effectively withstand and mitigate threats. Additionally, evaluating the age of these systems and their capacity for updates is paramount, as outdated infrastructure can pose significant vulnerabilities. Understanding the breadth of services included within these systems, as well as identifying any critical services that may be missing, is crucial for ensuring comprehensive preparedness. Furthermore, assessing the ease of use and flexibility of these systems is essential, as they must be intuitive and adaptable to swiftly respond to evolving threats and emergency scenarios

In the modern landscape of security threats, the spectre of biological and chemical terror attacks looms large, necessitating robust and innovative solutions to safeguard communities. A tangible, secure exchange platform tailored specifically for addressing these perils emerges as a vital component in fortifying defence mechanisms and enhancing capacity to respond effectively to such crises. This conclusion encapsulates the imperative of such a platform, drawing upon a series of compelling arguments that underscore its significance in ensuring the safety and security of nations across the European Union (EU).

Firstly, the uniform adoption of the same technology and platform among all EU nations lays the groundwork for seamless collaboration and communication. By standardizing technology across borders, the need for compatibility fixes among distinct systems and protocols is rendered obsolete. This streamlined approach not only eliminates barriers to interoperability but also facilitates rapid information exchange during critical moments. The cohesive adoption of a shared platform enables nations to harness collective intelligence and resources, thereby enhancing the efficacy of response efforts against biological and chemical terror threats.

Secondly, the linguistic cohesion among EU nations further facilitates the exchange of information with safety and speed. With a common “shared technological language”, communication barriers are minimized, enabling swift and accurate dissemination of critical intelligence. This linguistic homogeneity fosters a climate of trust and cooperation, allowing for seamless collaboration in the face of emergent threats. The ability to communicate effectively in a common language empowers nations to coordinate response efforts seamlessly, ensuring a unified and timely response to biological and chemical terror attacks.

Moreover, the principle of national sovereignty remains paramount, with each nation retaining complete control over the dissemination of information. This ensures that sensitive data remains secure and that nations can tailor their response strategies according to their unique circumstances and priorities. The platform serves as a conduit for collaboration while respecting the autonomy and sovereignty of individual nations. This decentralized approach fosters trust and cooperation among EU member states, ensuring that response efforts are effective and sustainable. At the same time the cost-effectiveness of creating such a platform using open-source technologies offers a compelling incentive for its implementation. By leveraging open-source solutions, the financial burden associated with developing and maintaining the platform is significantly reduced. This democratizes access to critical security infrastructure, ensuring that even nations with limited resources can benefit from its capabilities. The cost-efficient nature of open-source technologies makes the platform accessible to all EU nations, regardless of their financial constraints, thereby promoting inclusivity and equity in security preparedness.

One of the most important conclusions WP7 team reached is the integration of Virtual Private Networks (VPNs) and the crucial role this technology plays connecting remote endpoints and ensuring the secure transmission of data across the platform. VPNs enhance the resilience and reliability of communication channels, safeguarding against cyber threats and unauthorized access and by incorporating VPN technology into platform's architecture, the integrity and confidentiality of sensitive information are upheld, bolstering trust and confidence in its efficacy. Additionally, the implementation of Artificial Intelligence (AI) provides invaluable insights through sentiment analysis and decision-making algorithms. AI-driven sentiment analysis enables authorities to gauge public perceptions and sentiments, facilitating targeted communication strategies and fostering public trust and cooperation. Moreover, AI algorithms can analyse vast amounts of data in real-time, identifying patterns, anomalies, and emerging threats. This analytical insight empowers decision-makers with actionable intelligence, enabling them to respond proactively to potential biological and chemical terror attacks.

Finally the modular architecture of the platform further enhances its versatility and adaptability. By providing missing services, such as VPN or AI sentiment analysis, to already running systems, nations can integrate new functionalities without overhauling their existing infrastructure. This modular approach enables nations to tailor the platform to meet their specific needs and requirements, ensuring flexibility and scalability in response efforts against biological and chemical terror attacks.

In conclusion, the imperative of a tailored, secure exchange platform for addressing biological and chemical terror attacks cannot be overstated. By leveraging standardized technology, linguistic cohesion, national sovereignty, cost-effective open-source solutions, VPN technology, AI implementation, and modular architecture, it's the key to enhance security and resilience across EU member states. Its very important to embrace this initiative underscores with collective commitment to safeguarding communities, preserving national sovereignty, and fostering collaboration in the face of evolving threats. By investing in this essential security infrastructure, we can fortify our defences and protect against the scourge of biological and chemical terrorism.

Relevant Literature

1. Performance comparison of IPsec and TLS based VPN technologies (2011) IEEE Conference Publication | IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/6112567.

2. A new method for constructing dynamic VPN cooperating with OpenFlow control technology and healthcare PKI (2015) IEEE Conference Publication | IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/7275381.

3. Study of the Data Exchanging Safely and Quickly for Sudden Leakage of Dangerous Chemicals Emergency Decision System Based on VPN (2010) IEEE Conference Publication | IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/5634929.

4. A Survey of Mobile VPN Technologies (2016) IEEE Journals & Magazine | IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/7314859.

5. Performance Test and Analysis of Ground-Air Communication Network based on IPSec VPN (2021) IEEE Conference Publication | IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/9586831.

6. Performance analysis of virtualized VPN endpoints (2017) IEEE Conference Publication | IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/7973470.

7. *Sentiment analysis in a cross-media analysis framework* (2016) *IEEE Conference Publication | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/7509790.

8. *A conflict opinion recognition method based on graph neural network in Aspect-based Sentiment Analysis* (2022) *IEEE Conference Publication | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/9943870.

9. *Sentiment Embeddings with Applications to Sentiment Analysis* (2016) *IEEE Journals & Magazine | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/7296633.

10. *Aspect Level Sentiment Analysis Aided Supportive System for Interactive Platforms* (2022) *IEEE Conference Publication | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/10099722.

11. *Rule based sentiment analysis system for analyzing tweets* (2017) *IEEE Conference Publication | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/8286061.

12. *Sentiment Analysis on User Feedback of a Social Media Platform* (2023) *IEEE Conference Publication | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/10105082.

13. *Sentiment analysis on Facebook group using lexicon based approach* (2016) *IEEE Conference Publication | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/7873080.

14. *Product Prediction using Sentiment Analysis and Linear Regression* (2023) *IEEE Conference Publication | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/10134054.

15. Wang, M., Pan, J. and Zheng, Z. (2012) *The Application of VPN in the Remote Virtual Classroom*, *IERI Procedia*. doi:10.1016/j.ieri.2012.06.178.

16. Rikli, N.-E. and Almogari, S. (2013) *Efficient priority schemes for the provision of end-to-end quality of service for multimedia traffic over MPLS VPN networks*, *Journal of King Saud University - Computer and Information Sciences*. doi:10.1016/j.jksuci.2012.08.001.

17. Jim, J.R., Talukder, M.I., Malakar, P., Kabir, Md.M., Nur, K. and Mridha, M.F. (2024) *Recent advancements and challenges of NLP-based sentiment analysis: A state-of-the-art review*, *Natural language processing journal*. doi:10.1016/j.nlp.2024.100059.

18. Halawani, H.T., Mashraqi, A.M., Badr, S.K. and Alkhalaf, S. (2023) *Automated sentiment analysis in social media using Harris Hawks optimisation and deep learning techniques*, *Alexandria Engineering Journal*. doi:10.1016/j.aej.2023.08.062.

19. Tyburec, M., Doškář, M., Zeman, J. and Kružík, M. (2022) *Modular-topology optimization of structures and mechanisms with free material design and clustering*, *Computer Methods in Applied Mechanics and Engineering*. doi:10.1016/j.cma.2022.114977.

20. Krämer, M. and Senner, I. (2015) *A modular software architecture for processing of big geospatial data in the cloud*, *Computers & Graphics*. doi:10.1016/j.cag.2015.02.005.

21. Bareto, R. and Gada (2023) *Survey on Securing Traffic with IP Security VPN*, *ResearchGate*. Available at: https://www.researchgate.net/publication/370462569_Survey_on_Securing_Traffic_with_IP_Security_VPN.

22. Masuduzzaman, M., Mahmud, A., Islam, A. and Islam, M.M. (2019) *Two Phase Authentication and VPN Based Secured Communication for IoT Home Networks*, *arXiv.org*. Available at: https://search.arxiv.org/paper.jsp?r=1910.13625&qid=1712056082150ler_nCnN_-1950689526&qs=vpn.

23. Jaballi, S., Mahjoubi, A., Hazar, M.J., Zrigui, S., Nicolas, H. and Zrigui, M. (2024) *Decoding Multilingual Topic Dynamics and Trend Identification through ARIMA Time Series Analysis on Social Networks: A Novel Data Translation Framework Enhanced by LDA/HDP Models*, *arXiv.org*. Available at: https://arxiv.org/abs/2403.15445.

24. *Share and Multiply: Modeling Communication and Generated Traffic in Private WhatsApp Groups* (2023) *IEEE Journals & Magazine | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/10064263.

25. *Improving TLS Protocol Using Identity-Based Double-certificate Mechanism* (2012) *IEEE Conference Publication | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/6322310.

26. *Deep Learning approach for text, image, and GIF multimodal sentiment analysis* (2020) *IEEE Conference Publication | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/9303676.

27. *Choice, Uncertainty, and Decision Superiority: Is Less AI-Enabled Decision Support More?* (2023) *IEEE Journals & Magazine | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/document/10177274.

References

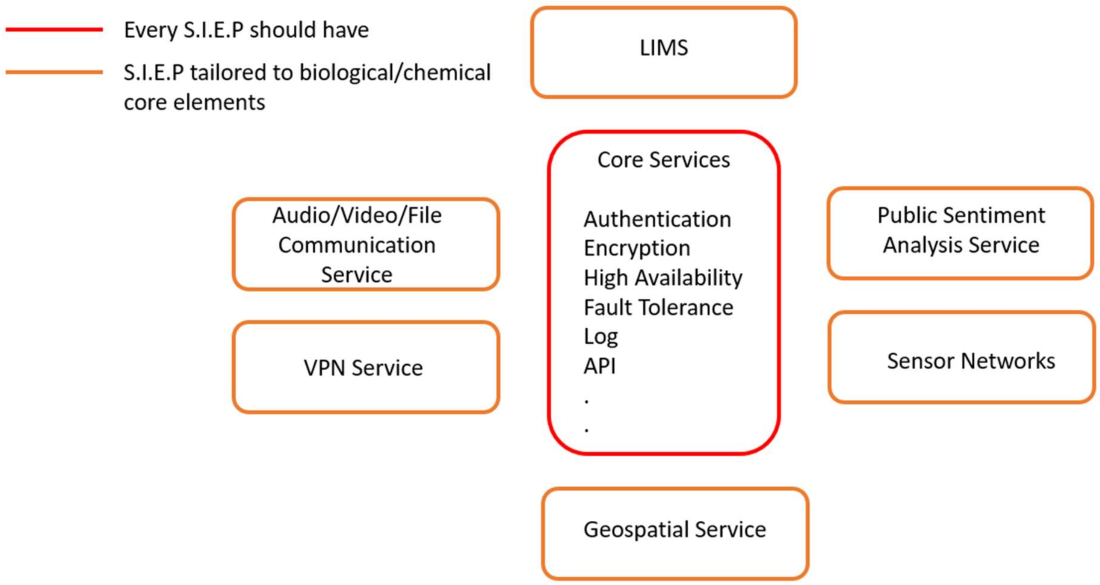
1. Charlotte Hall , Natalie Williams , Louis Gauntlett , Holly Carter , Richard Amlôt , Laura Petersen , Danielle Carbon , Natasha Newton , Garik Markarian , Dale Weston (2021) PROACTIVE D1.1 – Findings from Systematic Review of Public Perceptions and Responses | Available at: https://proactive-h2020.eu/wp-content/uploads/2021/04/PROACTIVE_20210312_D1.1_V5_PHE_Systematic-Review-of-Public-Perceptions-and-Responses_revised.pdf

2. George Kolev , Garik Markarian , Nataly Polushkina PROACTIVE D4.1 – Report on the High-level Architecture design including an interface control document | Available at: https://proactive-h2020.eu/wp-content/uploads/2021/04/PROACTIVE_20210312_D4.1_V6_RINI_Report-on-the-high-level-architecture-design_revised.pdf

3. George Kolev , Garik Markarian , Nataly Polushkina, Laura Petersen , Grigore Havârneanu PROACTIVE D4.2 – Developed Web Collaborative platform | Available at: https://proactive-h2020.eu/wp-content/uploads/2023/09/PROACTIVE_20230831_D4.2_V7_RINI_Developed-Web-Collaborative-platform.pdf

4. George Kolev , Garik Markarian , Nataly Polushkina Laura Petersen , Grigore Havârneanu (2023) PROACTIVE D4.3 – Modular App for Practitioners | Available at: https://proactive-h2020.eu/wp-content/uploads/2023/09/PROACTIVE_20230831_D4.3_V6_RINI_Developed-Modular-App-for-Practitioners.pdf

Annex 1A. – Modular Architecture Design


Every S.I.E.P should have
S.I.E.P tailored to biological/chemical core elements
LIMS
Core Services
Authentication
Encryption
High Availability
Fault Tolerance
Log
API
.
.
Audio/Video/File Communication Service
VPN Service
Public Sentiment Analysis Service
Sensor Networks
Geospatial Service

Annex 1B. – Specific Needs of S.I.E.P tailored to Biological/Chemical Terror Attack

Need	Purpose Serves During Biological/Chemical Terror Attack
Geolocation Service	pinpointing threats and coordinating responses
Real Time Incident Reporting Service	audio/video/file exchange posibility
VPN Remote Endpoint Connection Service	secure data transmission for remote users safeguarding sensitive information from potential breaches.
AI - Sentiment Analysis Service	gauge public response aiding in tailored communication and crisis management
Sensor Network Implementation	detect hazardous substances and monitoring environmental conditions enhancing situational awareness and response capabilities
L.I.M.S Integration	manage laboratory data ensuring accurate analysis and rapid response coordination