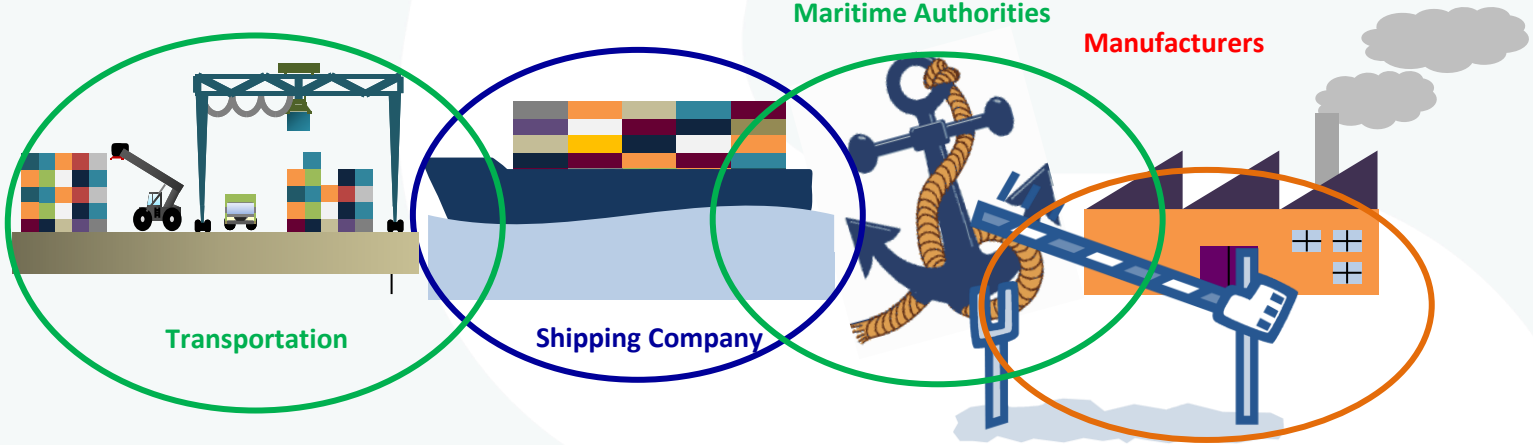
“This project has received fundingfrom the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833683“

CYBERSANE

A Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures

Dr. Spyridon Papastergiou, Maggioli Group
spyros.papastergiou@maggioli.it
Cyberwatching.eu Webinar
29.10.2020

Background & Motivation



Critical Information Infrastructures (CIIs)

Daily headlines on Cyber-Attacks

The Cyber-Security source

HOME | NEWS & FEATURES | BUYER'S GUIDE | OPI

SC UK | SC US

Source: https://www.scmagazineuk.com/half-norways-population-medical-data-leaked/article/1473442

Half of Norway's population have medical data leaked

Jan 19, 2018

NEWS by Grace Johansson

Healthcare data has been stolen from more than half of Norway's population by a hacker or hacker group. The attack happened on 8 January according to BleepingComputer and came to light this week.

Source: https://blog.cymulate.com/iranian-based-hacker-group-oilrig-keeps-cyber-drilling-posing-a-persistent-threat

Technology Intelligence

WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled

Follow

By Matthew Field

11 OCTOBER 2018 • 6:05PM

A devastating global cyber attack that crippled computers in hospitals across the UK has cost the NHS £92m, a report from the Department of Health has found.

The so-called WannaCry hack, which shut down hundreds of

messages from

ird of hospital trusts

care was disrupted

nts to be cancelled,

May and £72m in the

ems.

lock out users with

yptocurrency Bitcoin.

ackers after a year-

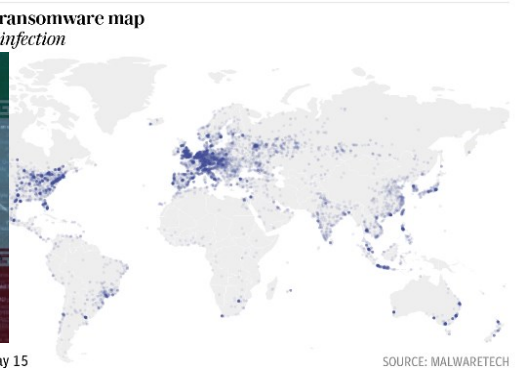
ed for using outdated

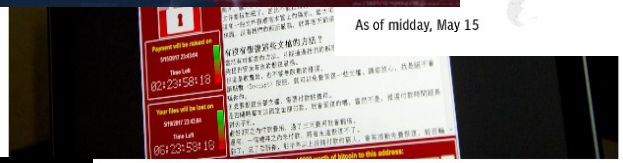
d operating system

Government said it

had continued to invest in its cyber security and infrastructure to prevent similar attacks.

Source:https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/





A computer hit by the WannaCry attack CREDIT: AP

WannaCry About NotPetya?

Source | http://www.diariotrv.com/articulo/internacional/nyetya-el-virus-responsable-del-ciberataque-que-mantiene-en-vilo-al-mundo/20170628100525001964.html

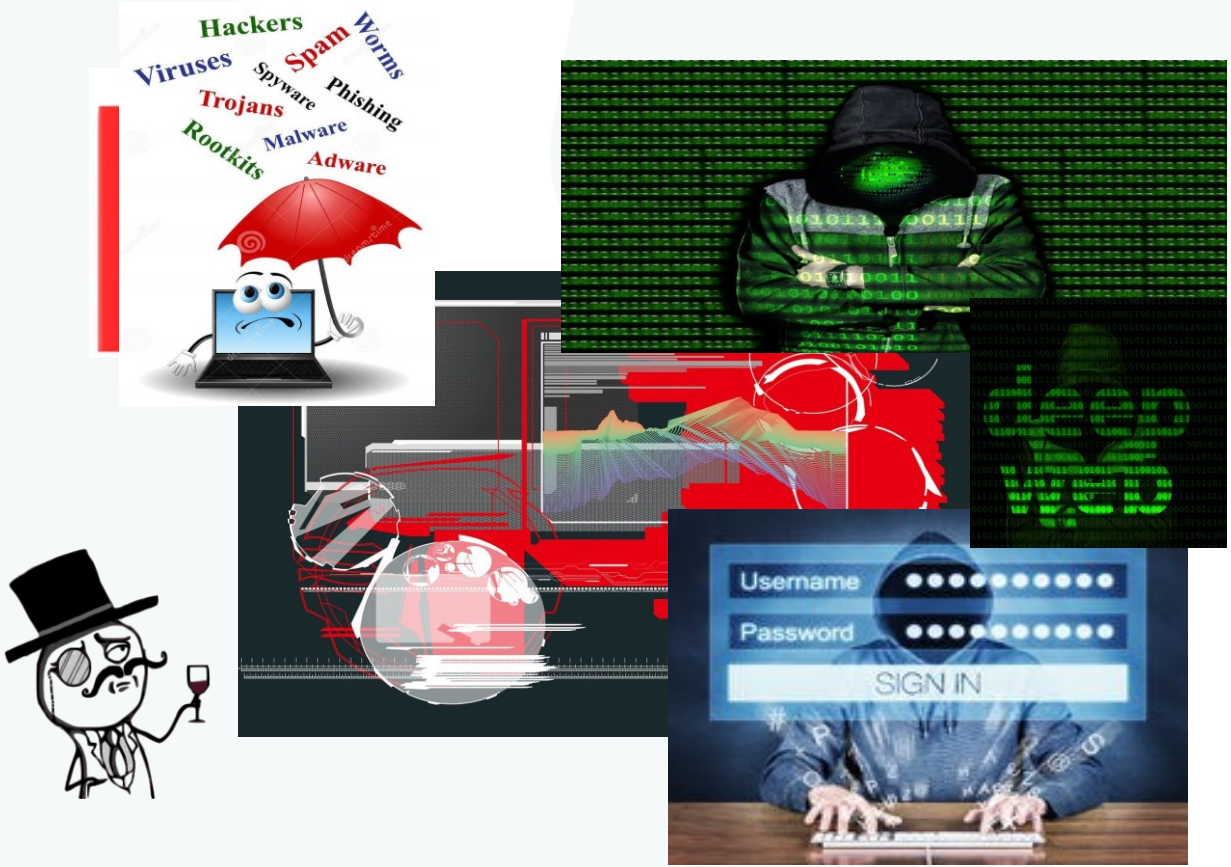
Podcast Episode 14

Ransomware stats

Source Rafael Fariñas |https://theusbport.com/ransomware-not-really-discover-notpetyas-true-objective/28191

- A business is hit with ransomware every **40 seconds** (Kaspersky)
- Average ransom demand = **$1077** (Symantec)
- **1 in 5** businesses that paid the ransom never got their files back (Kaspersky)
- **72%** percent of victims lost access to data for two days or more (Intermedia)

Cyber-criminal Activities



Under Pressure

How can we enhance the security and resilience of the critical infrastructures???

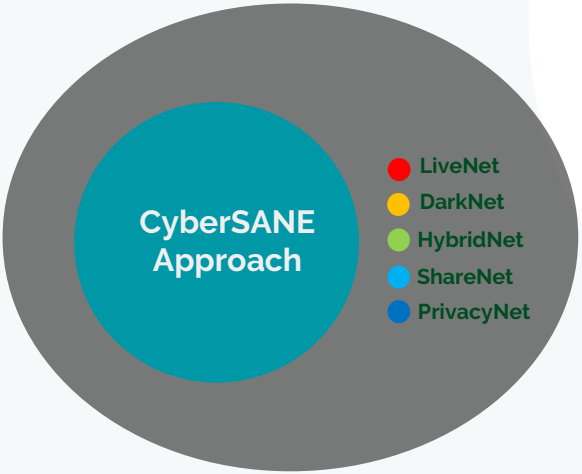
How to respond to a security event???

How these threats affect the infrastructures???

There is a pressing need for devising novel systems for efficient CIIs incident handling and support thorough and common understanding of cyber-attack situations in a timely manner.

CyberSANE Concept

E.U. Directive NIS, 2016 enforcing all CIIs (CSIRTs)



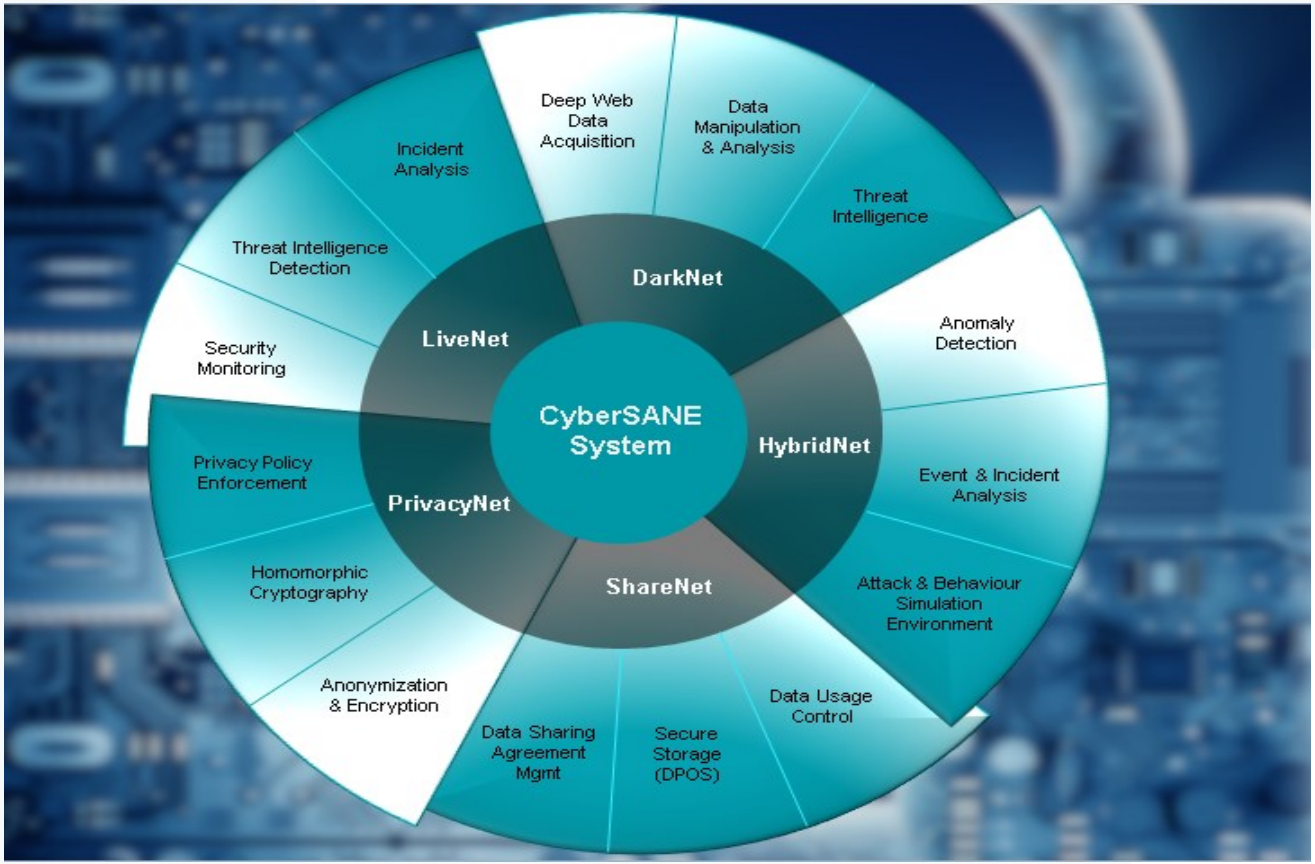
ISO/IEC 27035: 2016 Incident Management

CyberSANE aims to contribute towards the emerging need to improve the level of prevention, preparedness, reaction and resilience to cyber incidents and threats of the CIIs.

An advanced, configurable and adaptable, Security and Privacy Incident Handling system (CyberSANE system)

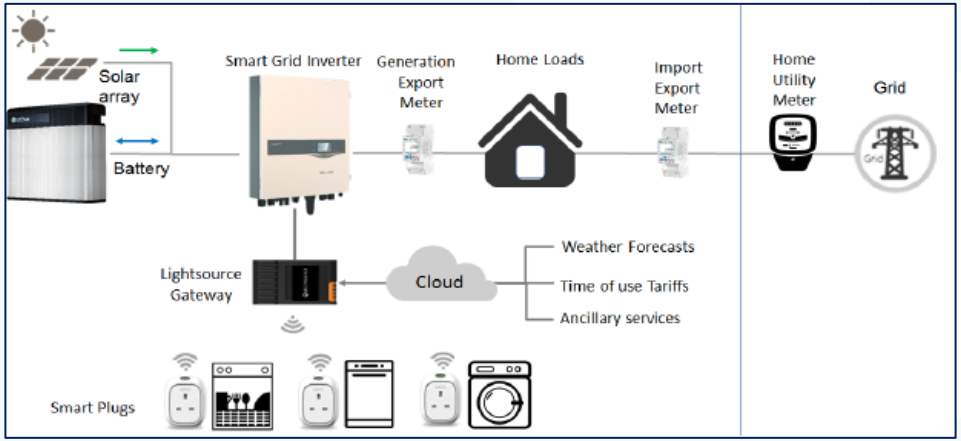
- ✓ thoroughly assess the vulnerabilities
- ✓ evaluate the probability of cyber-attacks;
- ✓ identify the relationships between indicators of compromise, threats, and adversaries
- ✓ estimate the cascading effects of the attacks;
- ✓ provide technical assistance and guidance on investigating and handling complex, interrelated cyber security incidents and data breaches
- ✓ combine and analyse all security incident-related information in an effective and accurate manner
- ✓ share information and warnings with all stakeholders

CyberSANE System

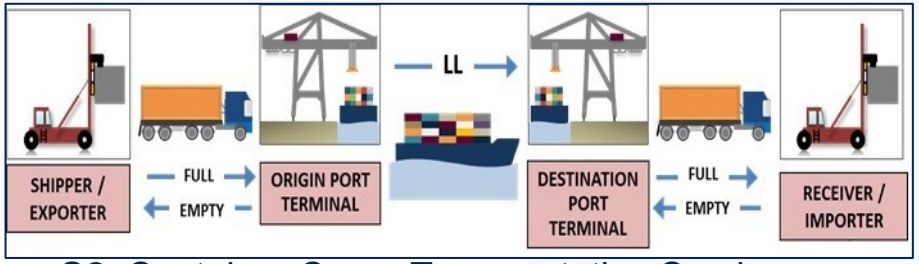


CyberSANE Component

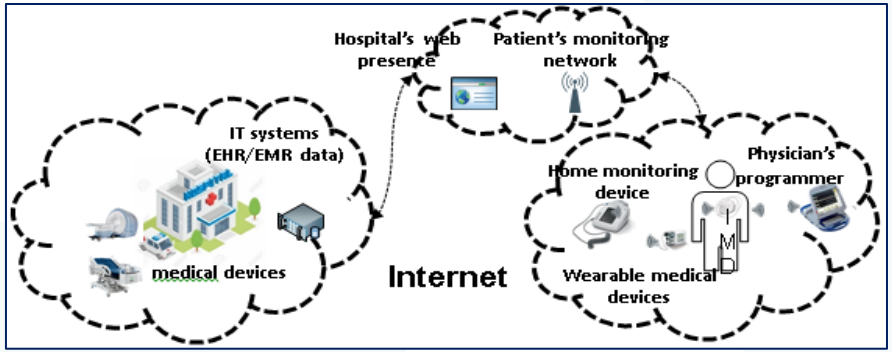
CyberSANE Showcase Scenarios



S1: Solar Energy Production, Storage & Distribution Service



S2: Container Cargo Transportation Service



S3: Real-time patient monitoring and treatment service

CyberSANE Added Value

- the **identification of attacks and incidents** using innovative approaches and algorithms of unobserved components techniques and linear state-space models **producing meaningful information from cyber systems**
- the **combination of active** incident handling approaches with **reactive approaches producing real-time insights, alerts and warnings** about cyber events
- innovative **normalization process** that unifies all relevant incident-related information gathered from heterogeneous CIIs
- novel **attacks' scenarios and evidence representation with simulation techniques** and visualization tools that increase the efficiency of investigation results

CyberSANE Consortium

Participant No *	Participant organization name	Part. short name	Country
1 (coordinator)	Projecto Desenvolvimento Manutenção Formação e Consultadoria	PDMFC	Portugal
2	Atos Spain S.A.	ATOS	Spain
3	Consiglio Nazionale delle Ricerche	CNR	Italy
4	S2 Grupo de Innovación en Procesos Organizativos, S.L.	S2	Spain
5	Institut National de Recherche En informatique Et Automatique	INRIA	France
6	Maggioli Group	MAG	Italy
7	UBITECH LIMITED	UBI	Cyprus
8	Jožef Stefan Institute	JSI	Slovenia
9	Foundation for Research and Technology – Hellas	FORTH	Greece
10	SPHYNX TECHNOLOGY SOLUTIONS AG	STS	Switzerland
11	Katholieke Universiteit Leuven	KUL	Belgium
12	SIDROCO Holdings Ltd	SID	Cyprus
13	University of Brighton	UoB	UK
14	Valenciaport Foundation	VPF	Spain
15	Lightsource Labs Limited	LSE	Ireland
16	Klinikum Nuremberg	KN	Germany

IA - Innovation action

Project Duration: 1st September 2019 – 31 st August 2022

Thank you!

Dr. Spyridon Papastergiou,
spyros.papastergiou@maggioli.it