

IOE-BASED ARCHITECTURE FOR ENHANCED CYBER SITUATIONAL AWARENESS

Dr. Ida Wahidah

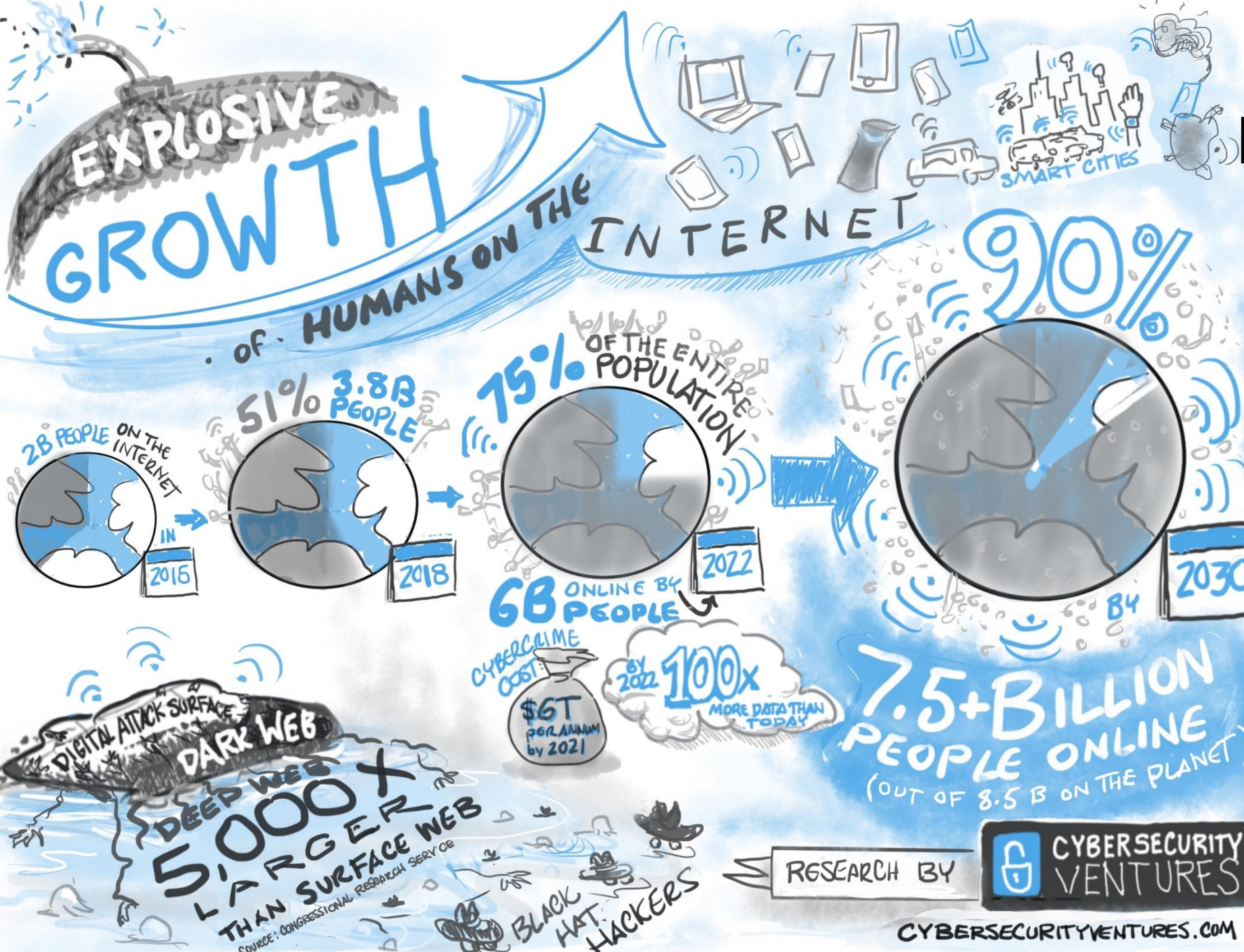
School of Electrical Engineering – Telkom University

wahidah@telkomuniversity.ac.id

AGENDA

- Latar Belakang
- Cyber Situational Awareness
- Internet of Everything
- Use Case: Heterogeneous Vehicles
- Use Case: Gas and Oil Storage
- Penelitian dan Pengembangan

PERTUMBUHAN RUANG SIBER



Ran k	Country	Popu lato n (milli on)	% Con nec ted
1	China	1,433	58
2	India	1,366	45
3	United States	329	84
4	Indonesia	270	36
5	Pakistan	216	33
6	Brazil	211	68

KONEKSI MOBILE INDONESIA

JAN
2019

MOBILE CONNECTIONS BY TYPE

BASED ON THE NUMBER OF CELLULAR CONNECTIONS (NOTE: NOT UNIQUE INDIVIDUALS)

Clip slide

- as

TOTAL NUMBER
OF MOBILE
CONNECTIONS



355.5
MILLION

we
are
social

MOBILE CONNECTIONS
AS A PERCENTAGE OF
TOTAL POPULATION



133%

GSMA

PERCENTAGE OF
MOBILE CONNECTIONS
THAT ARE PRE-PAID



97%

GSMA

PERCENTAGE OF
MOBILE CONNECTIONS
THAT ARE POST-PAID



3%

GSMA

PERCENTAGE OF MOBILE
CONNECTIONS THAT ARE
BROADBAND (3G & 4G)



84%

EKONOMI DIGITAL INDONESIA

JAN
2019

E-COMMERCE ACTIVITIES

PERCENTAGE OF INTERNET USERS WHO REPORT PERFORMING EACH ACTIVITY IN THE PAST MONTH [SURVEY BASED]

Clip slide

• as

SEARCHED ONLINE
FOR A PRODUCT
OR SERVICE TO BUY



we
are
social

93%

VISITED AN ONLINE
RETAIL STORE ON THE
WEB (ANY DEVICE)



global
web
index

90%

PURCHASED A
PRODUCT OR SERVICE
ONLINE (ANY DEVICE)



as

86%

MADE AN ONLINE
PURCHASE VIA A LAPTOP
OR DESKTOP COMPUTER



global
web
index

37%

MADE AN ONLINE
PURCHASE VIA A
MOBILE DEVICE



76%

CYBER SITUATIONAL AWARENESS



SITUATIONAL AWARENESS

- The purpose of Situational Awareness is to actively **discover and analyze information related to immediate operational stability and security** and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture
- **Goal 1:** Threat monitoring is performed
 - Has responsibility for monitoring sources of threat information been assigned?
- **Goal 2:** The requirements for communicating threat information are established
 - Have internal stakeholders (such as the critical service owner and incident management staff) been identified to whom threat information must be communicated?
- **Goal 3:** Threat information is communicated
 - Is threat information communicated to stakeholders?

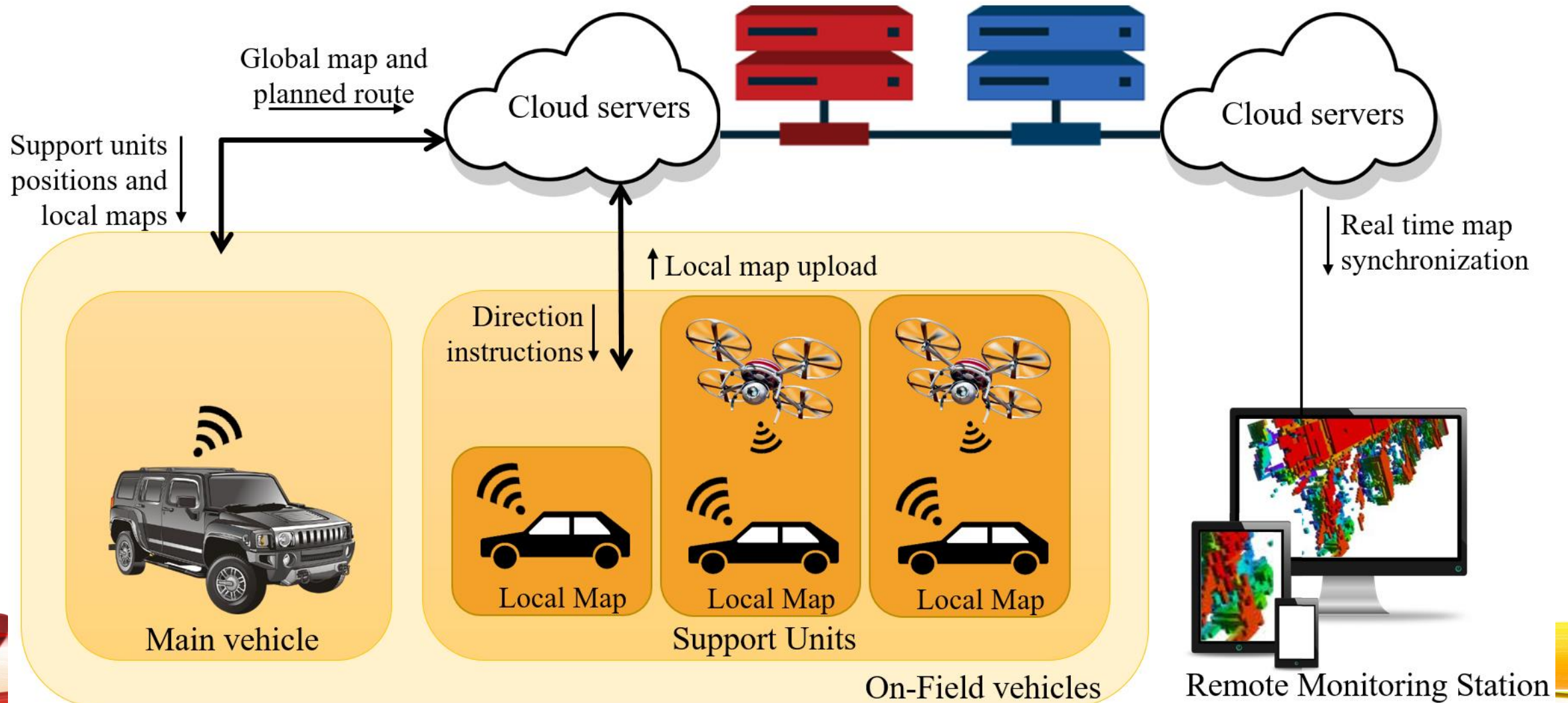
TANTANGAN

- Robust situational awareness
 - Low quantity or quality of data → serious consequences
- Enhancing situational awareness with **IoE-based architecture**
 - Critical case → natural disasters
- High levels of situational awareness in other use cases
 - **Autonomous vehicles**
 - **Gas and oil storage**
 - Banking and finance
 - Electrical energy
 - Government operations
 - Water supply systems
- Fundamental research: modelling the complexity of the infrastructure to achieve situational awareness

USE CASE 1: HETEROGENEOUS VEHICLES



ARSITEKTUR SISTEM

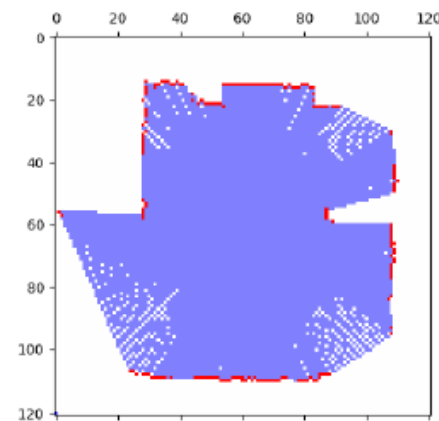


COLLABORATIVE SECURITY

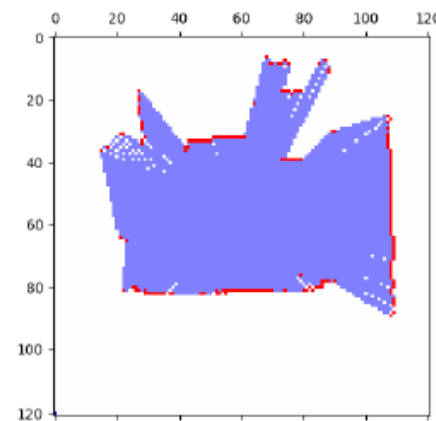
- **Collaborative system** → significantly improved situational awareness
 - Combination of IoE and swarm optimization
 - Map merging techniques
- Heterogeneous vehicle
 - **A large network of interconnected vehicles** will provide more accurate and efficient situational awareness
 - Main vehicle with objective destination, together with heterogeneous team of support vehicles
- IoE based system architecture
 - Heterogeneous support unit
 - Cloud servers

PATH & MAP PLANNING

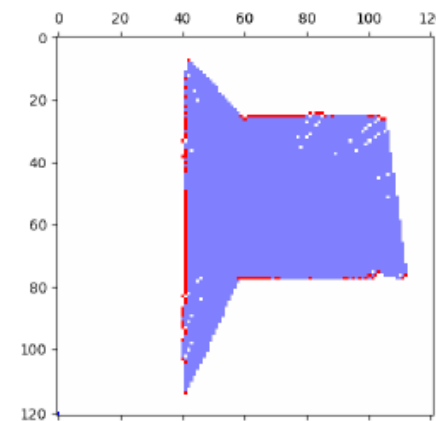
- Pemetaan dan penggabungan peta



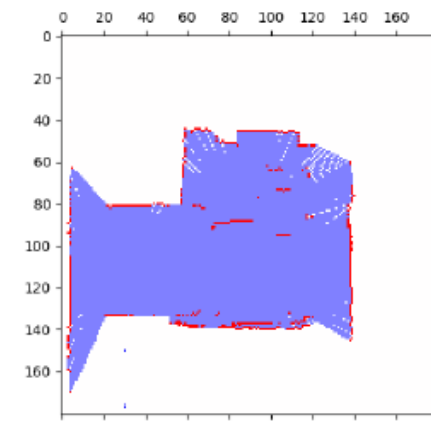
(a) Local map 1



(a) Local map 2



(a) Local map 3



(a) Merged map



USE CASE 2: OIL AND GAS SYSTEMS



TANTANGAN IOE MINYAK & GAS

- Aplikasi yang berdiri sendiri, 17 jaringan dengan standar berbeda, 30 ton pengkabelan
- Produksi data dalam **Terabyte per hari**
- Keterbatasan bandwidth
- **Security, security, security**
- Scala sangat besar (jutaan sensor)
- Standar proprietary (diperlukan interoperabilitas)



TANTANGAN SITUATIONAL AWARENESS

- Collaborative IoE untuk penguatan situational awareness

Cloud and Fog

Analytics

Security and
Identity Management

Open and
Programmability
(APIs)

Ease of Use
and Management



Applications



App Enablement

Event
Management

Workflow/
Rules Engine

Video
Sensing

Data Normalization
and Modeling

Protocol
Mediation

Enterprise App
Integration



Infrastructure

Software Defined Networking
Network Compute Storage



Things

RANGKUMAN

- Discover & analyse information
- Perform & communicate the threat monitoring

- IoE = IoT + advanced technologies
- Wireless mesh networks
 - Compressive sensing
 - Hybrid fog/cloud computing
 - Artificial intelligence

Collaborative security system

Cyber
Situational
Awareness

- Modelling the complexity of the system
- Predictive/forecasting model for intrusion detection

TERIMA KASIH

