Defending smart cities and beyond

Konrad Wrona (and Michael Street)

NATO Communications and Information Agency

The Hague, The Netherlands

Motivation

Identify

various scenarios for integration of IoT with current command and control systems

technical enablers

possible building blocks and architecture patterns

Validate

implementing a proof-of-concept

Prepare

Security, performance, scalability and standardization

Command and control systems

- NCOP
- TAK
- SitaWare Suite

Situational Awareness

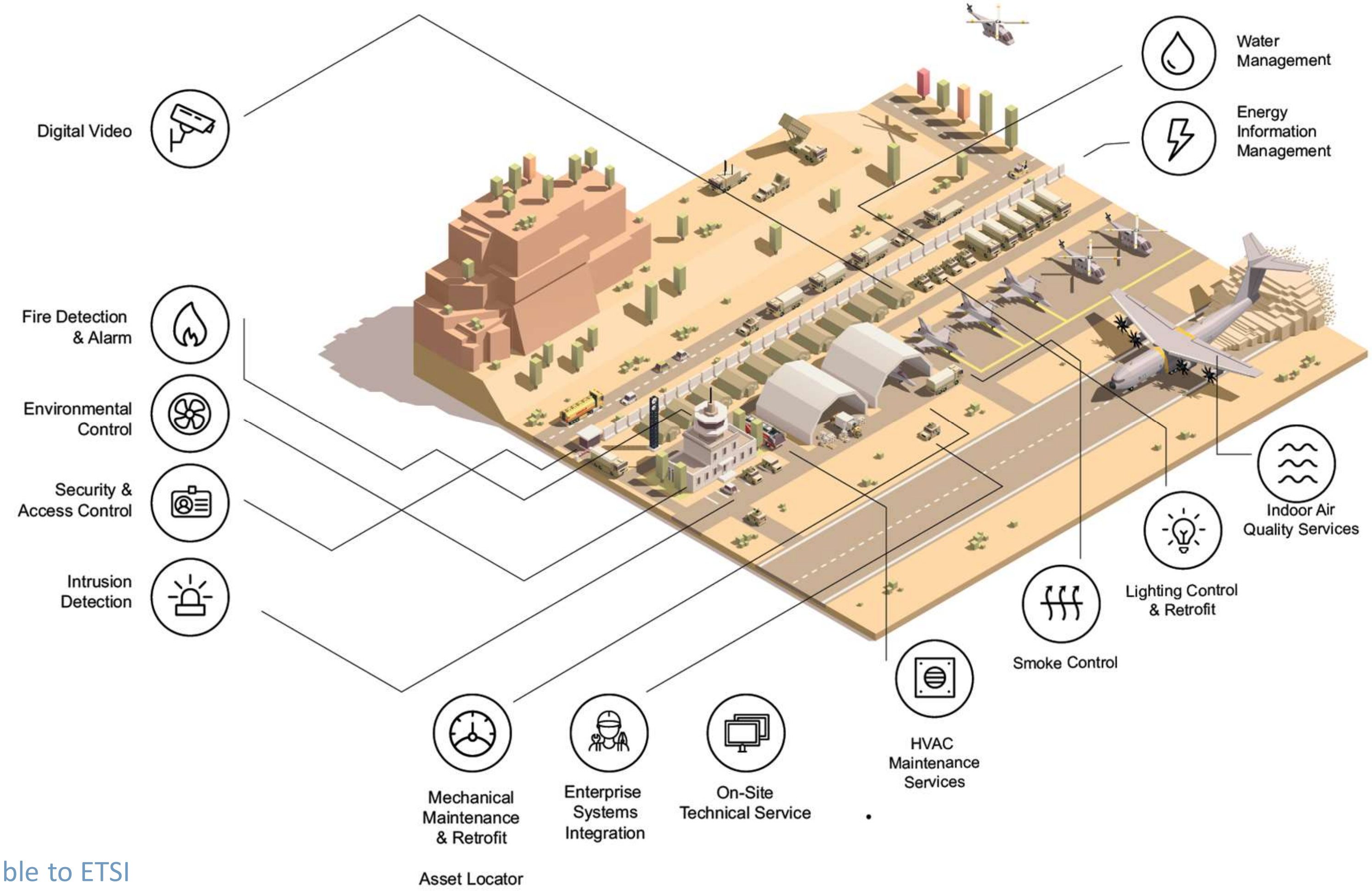
- JChat

Communications

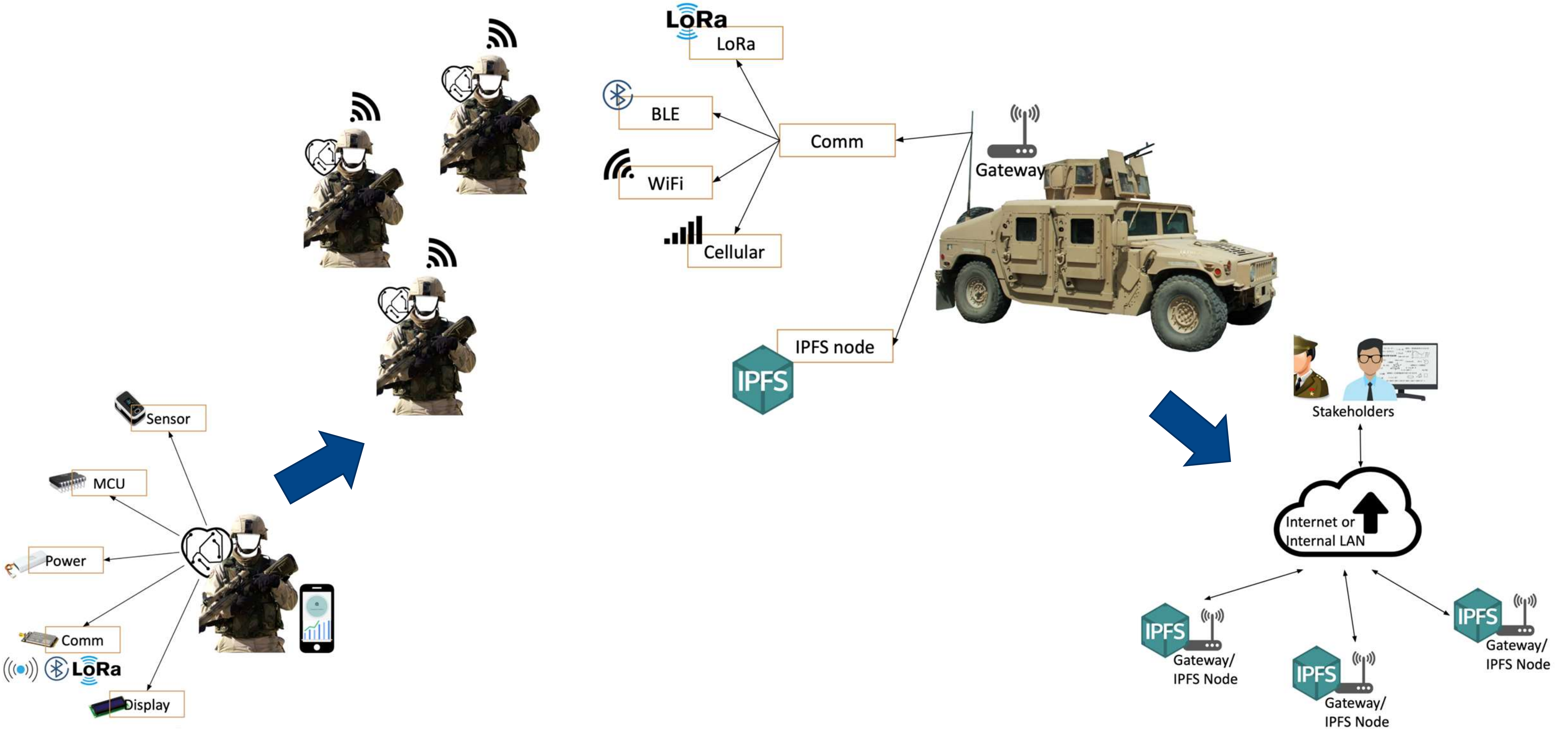
- MEDSuite

Medical support

Smart base


Digital Video
Fire Detection & Alarm
Environmental Control
Security & Access Control
Intrusion Detection
Water Management
Energy Information Management
Indoor Air Quality Services
Lighting Control & Retrofit
Smoke Control
HVAC Maintenance Services
Mechanical Maintenance & Retrofit
Enterprise Systems Integration
On-Site Technical Service
Asset Locator

Connected unit comprising of connected soldiers



Sensor

MCU

Power

Comm

LoRa

Display

LoRa

BLE

WiFi

Cellular

Comm

Gateway

IPFS node

Stakeholders

Internet or Internal LAN

Gateway/ IPFS Node

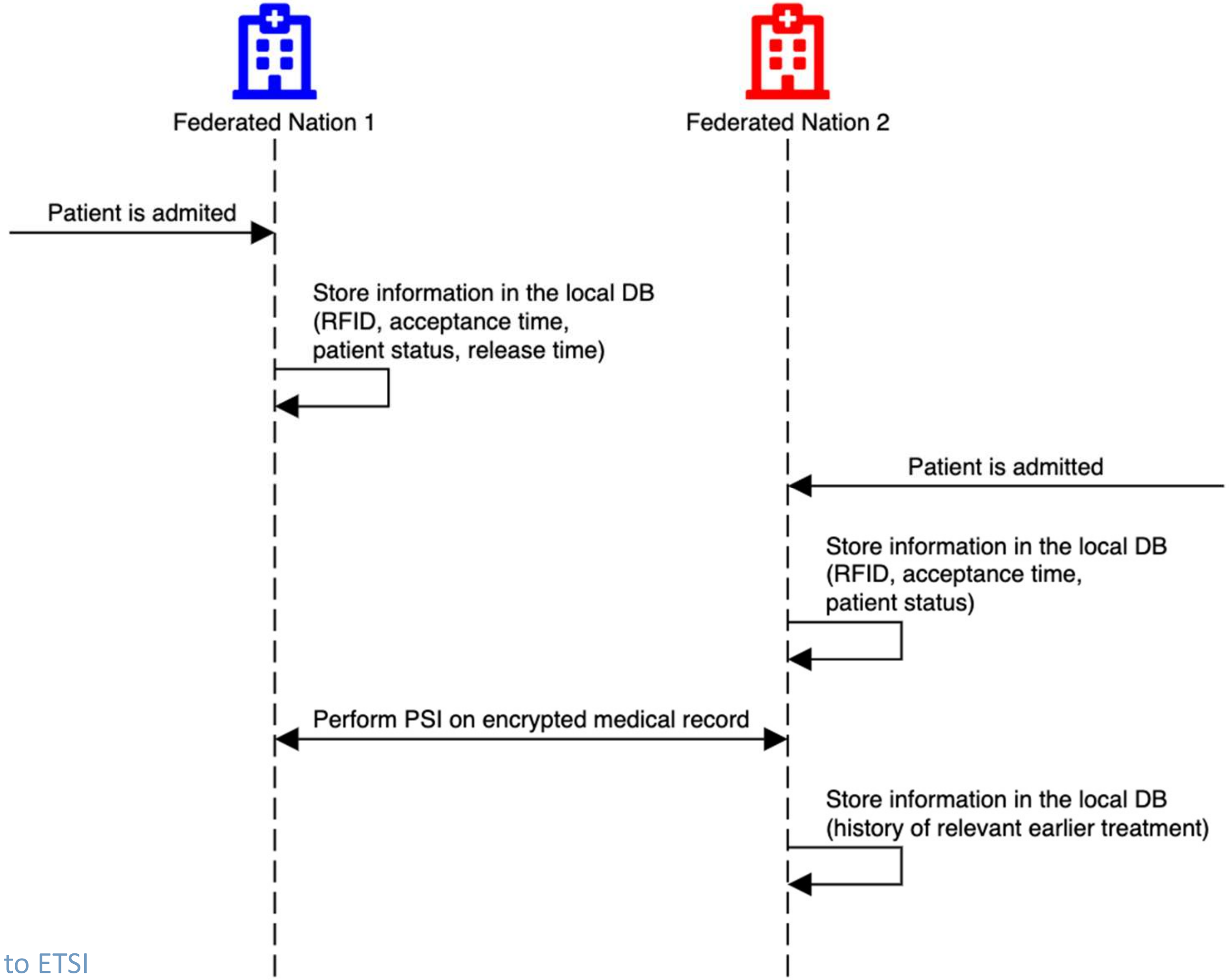
Gateway/ IPFS Node

Gateway/ IPFS Node

Connected soldier

Distributed network of connected units

Patient tracking



Federated Nation 1

Federated Nation 2

Patient is admited

Store information in the local DB
(RFID, acceptance time,
patient status, release time)

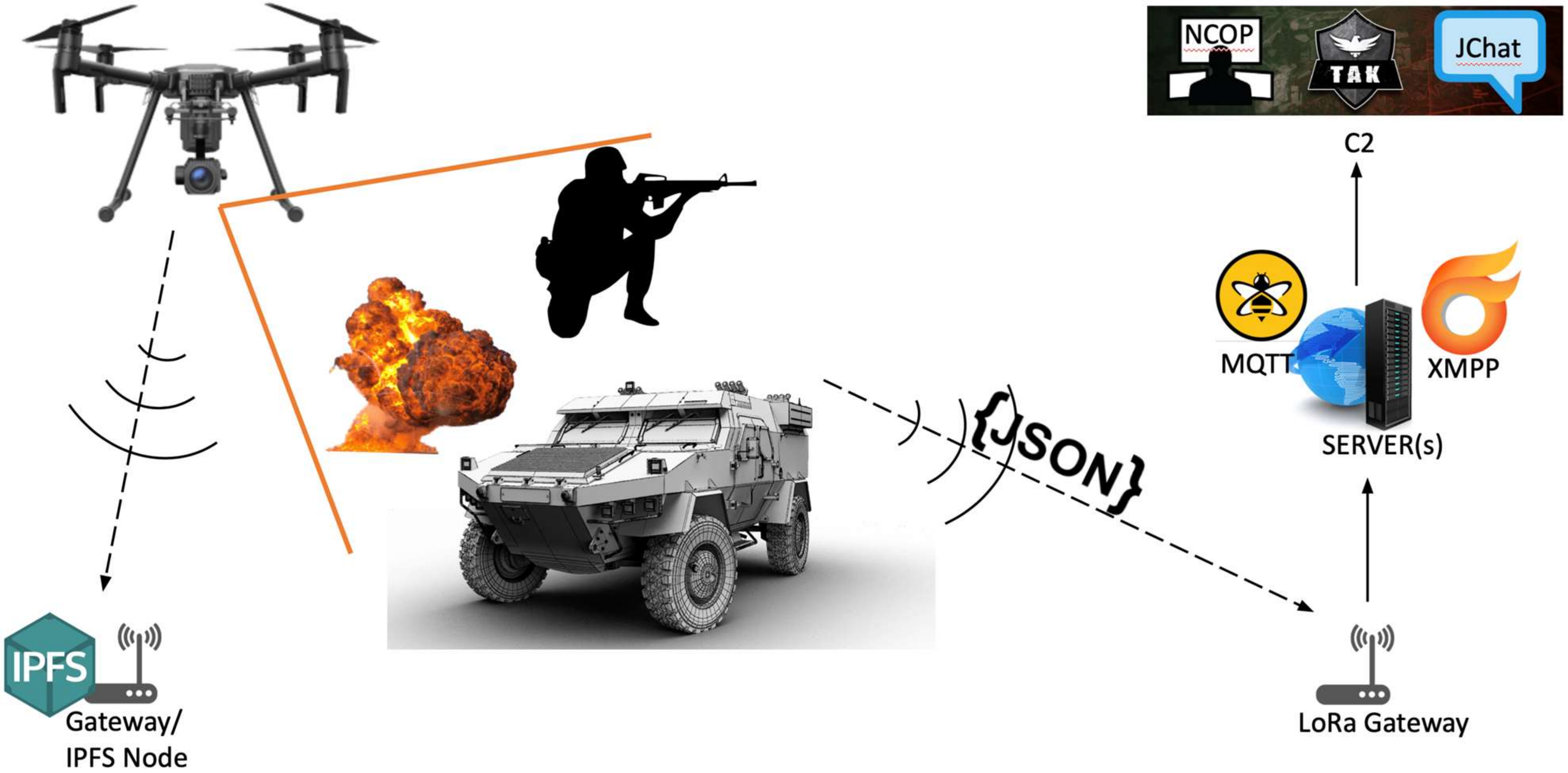
Patient is admitted

Store information in the local DB
(RFID, acceptance time,
patient status)

Perform PSI on encrypted medical record

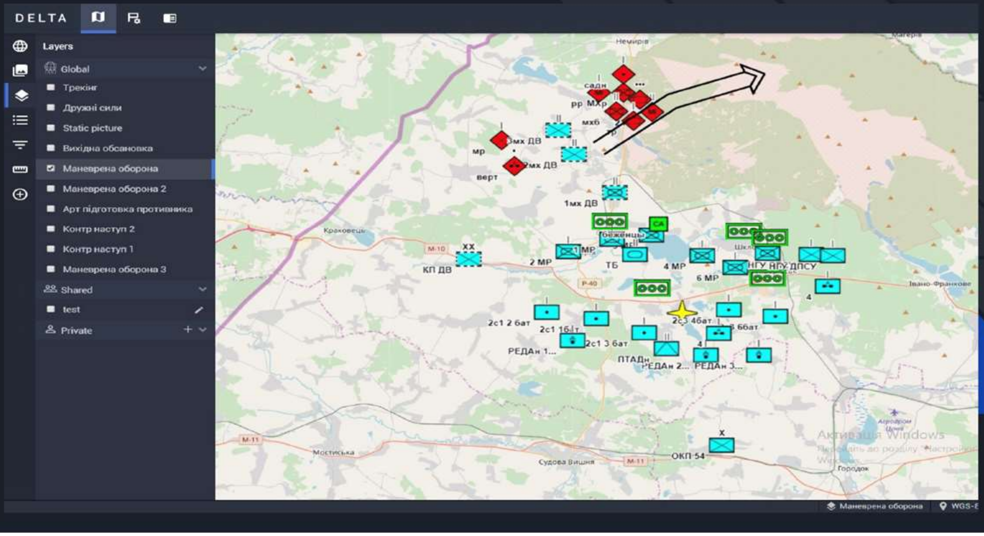
Store information in the local DB
(history of relevant earlier treatment)

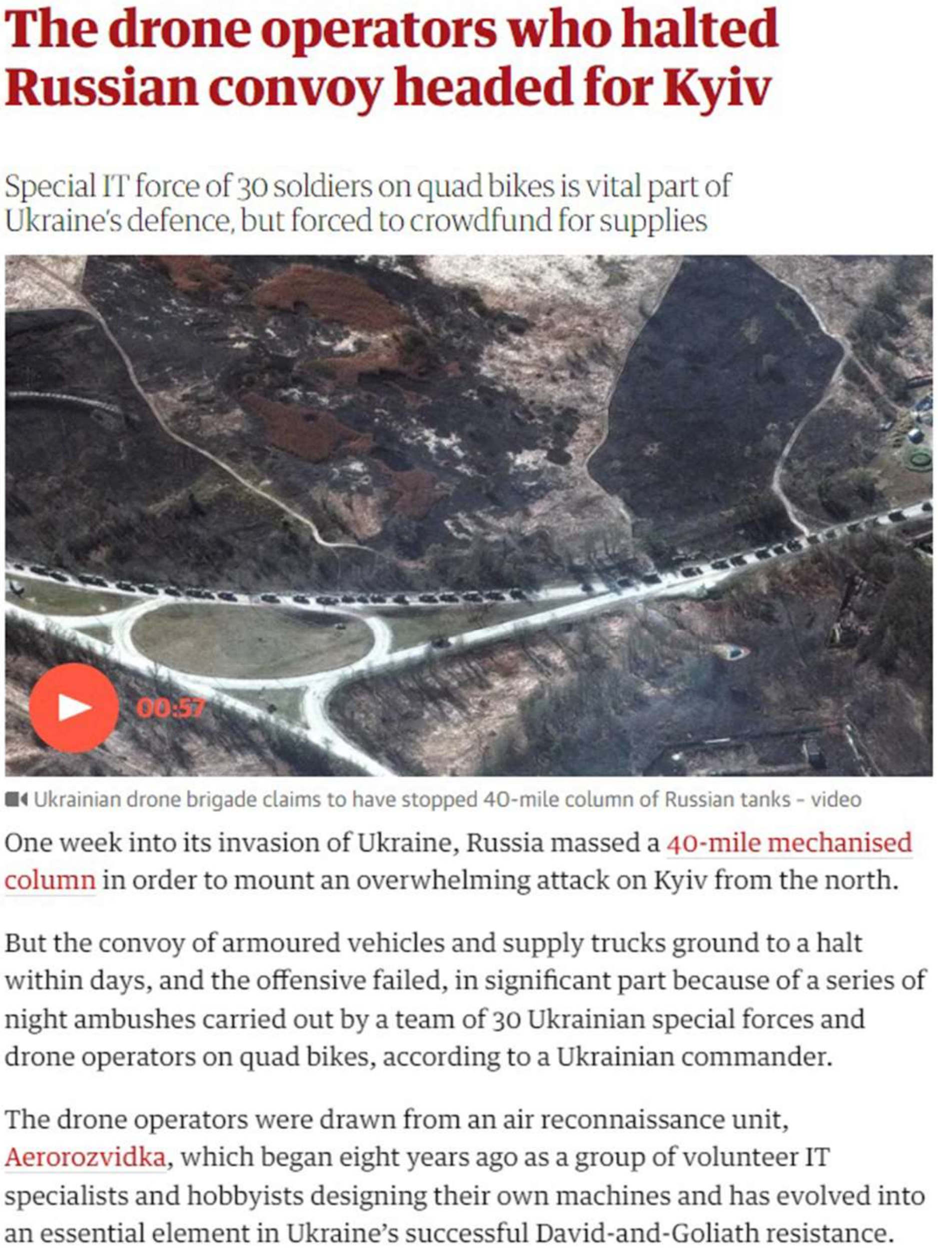
Threat recognition



Aerorozvidka (C4ISR Centre of Ukraine)

Aerorozvidka was established in June 2014 as a response from an active part of Ukrainian society to the challenges posed by the occupation of Crimea and Donbas.





The drone operators who halted Russian convoy headed for Kyiv

Special IT force of 30 soldiers on quad bikes is vital part of Ukraine's defence, but forced to crowdfund for supplies

Ukrainian drone brigade claims to have stopped 40-mile column of Russian tanks - video

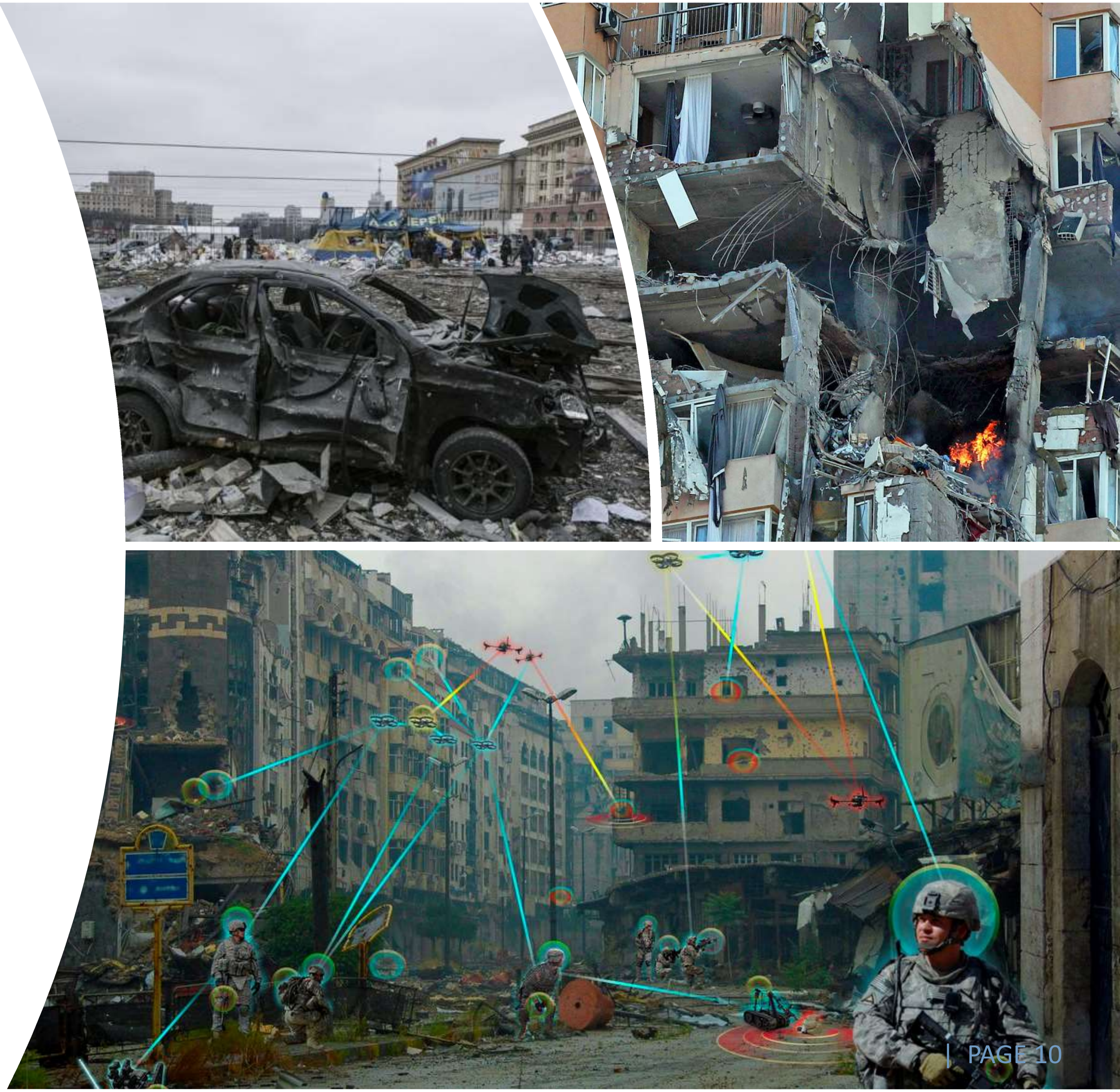
One week into its invasion of Ukraine, Russia massed a 40-mile mechanised column in order to mount an overwhelming attack on Kyiv from the north.

But the convoy of armoured vehicles and supply trucks ground to a halt within days, and the offensive failed, in significant part because of a series of night ambushes carried out by a team of 30 Ukrainian special forces and drone operators on quad bikes, according to a Ukrainian commander.

The drone operators were drawn from an air reconnaissance unit, Aerorozvidka, which began eight years ago as a group of volunteer IT specialists and hobbyists designing their own machines and has evolved into an essential element in Ukraine's successful David-and-Goliath resistance.

Humanitarian Assistance and Disaster Relief

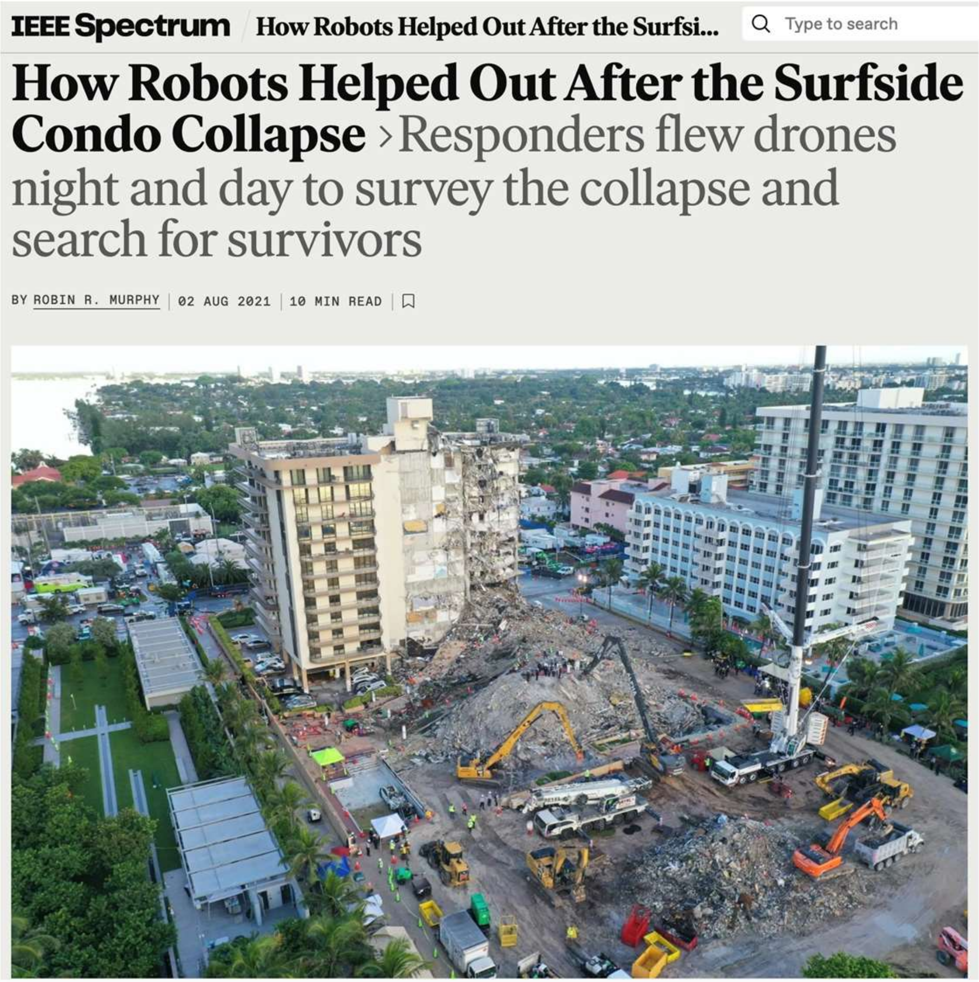
- Gas sensors, motion sensors, air quality sensors;
- Image processing (object detection and recognition);
- Drones and robots



Enhancing IoT: Robots and UxVs

- Internet of Robotic Things:

  Gobot; Artoo; Cylon



How Robots Helped Out After the Surfside Condo Collapse › Responders flew drones night and day to survey the collapse and search for survivors

BY ROBIN R. MURPHY | 02 AUG 2021 | 10 MIN READ

Technical enablers

- Development boards

  Arduino; Nvidia Jetson; Raspberry Pi; Adafruit Feather; Waspmote; Pycom

- Sensors

- Communications:

  LoRa; LTE-M; BLE; Zigbee; NB-IoT; Sigfox; WiFi

- Data exchange

  MQTT; AMQP

- Data visualization

  The Things Stack, TIG (Telegraf Influx Grafana), Things Board, Thinger.io

- Application-level cryptography:

  Identity-based and Attribute-based Encryption; Private Set Intersection; Homomorphic Encryption

- Vulnerability assesement:

  securiCAD Vanguard; Shodan; Nessus

Enhancing IoT: Distributed ledgers and storage

- Hyperledger Fabric

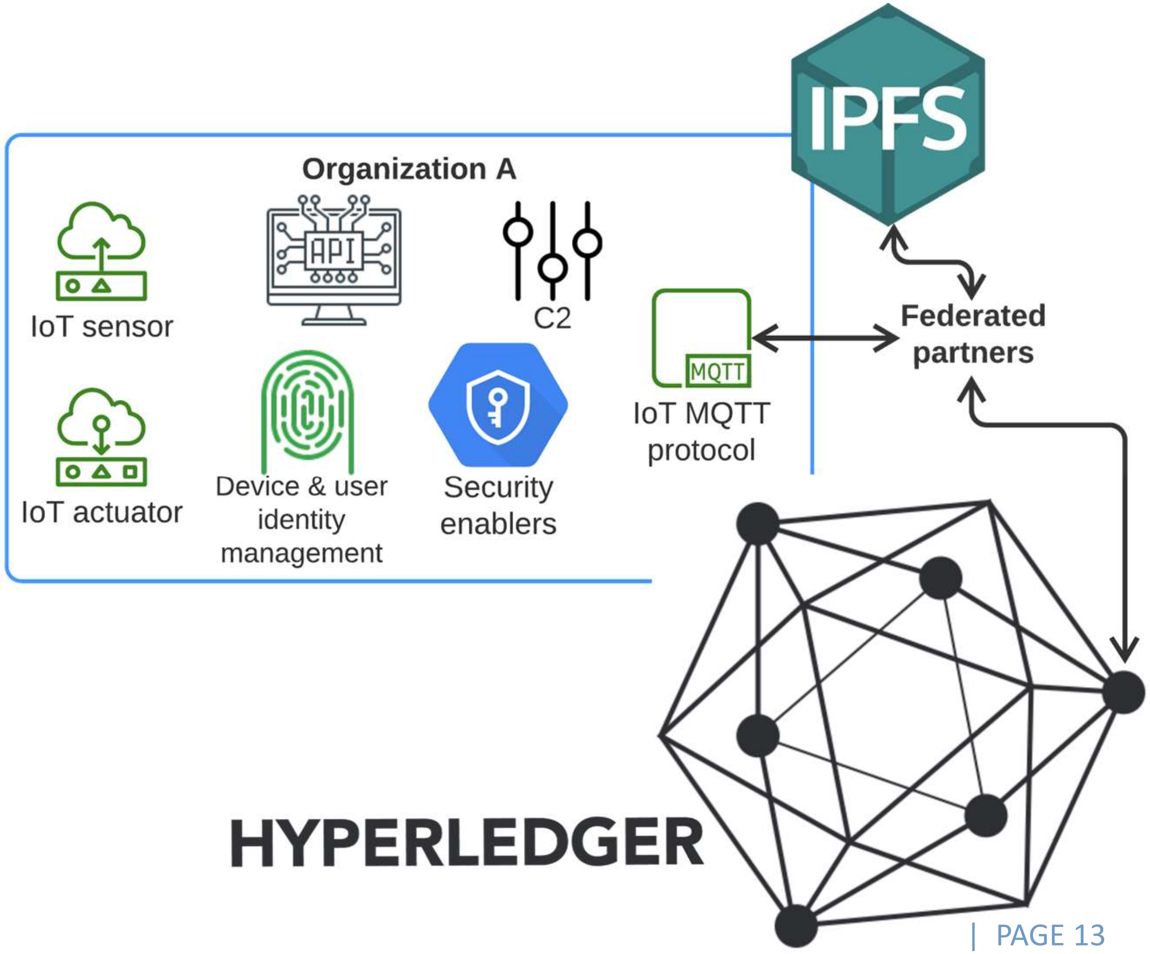
    No single point of failure;

    Integrity and accountability;

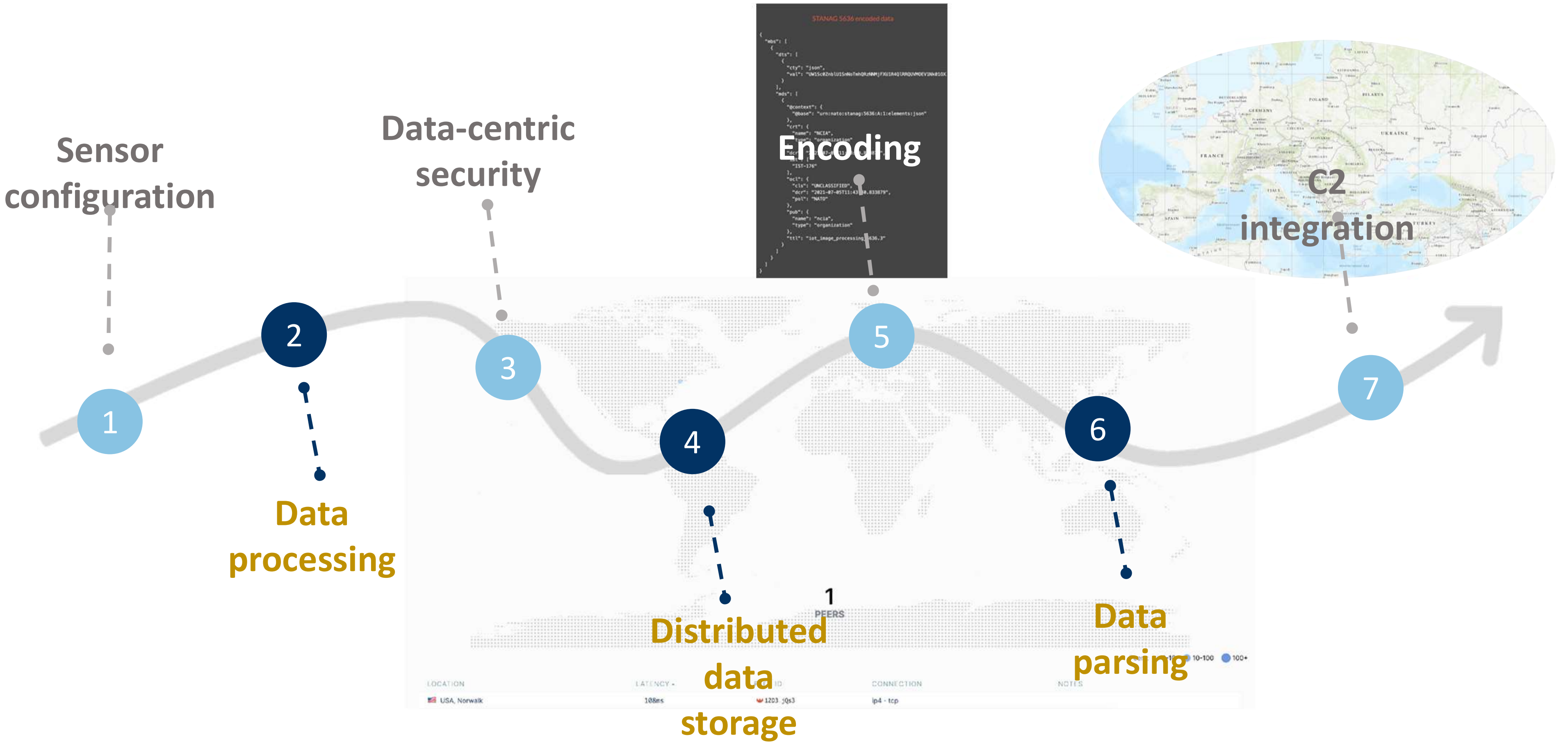
    Transparency and access control

- IPFS

    Secure distributed storage



Secure pipeline: from a sensor to C2



1 Sensor configuration

2 Data processing

3 Data-centric security

4 Distributed data storage

5 Encoding

6 Data parsing

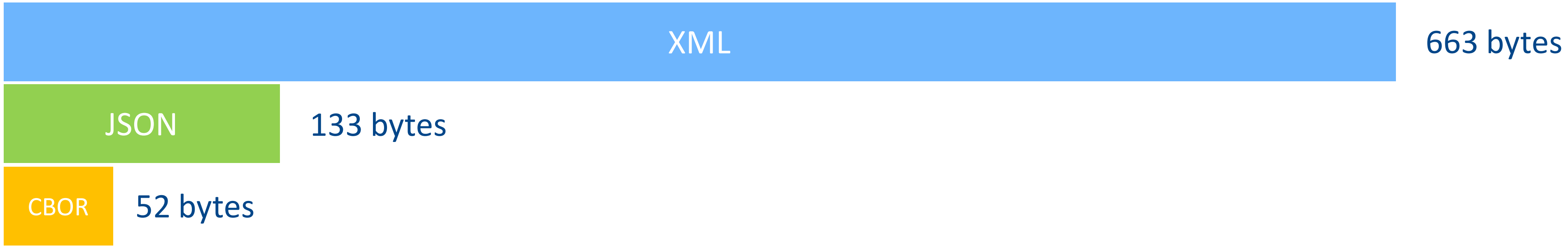
7 C2 integration

STANAG 5636 encoded data

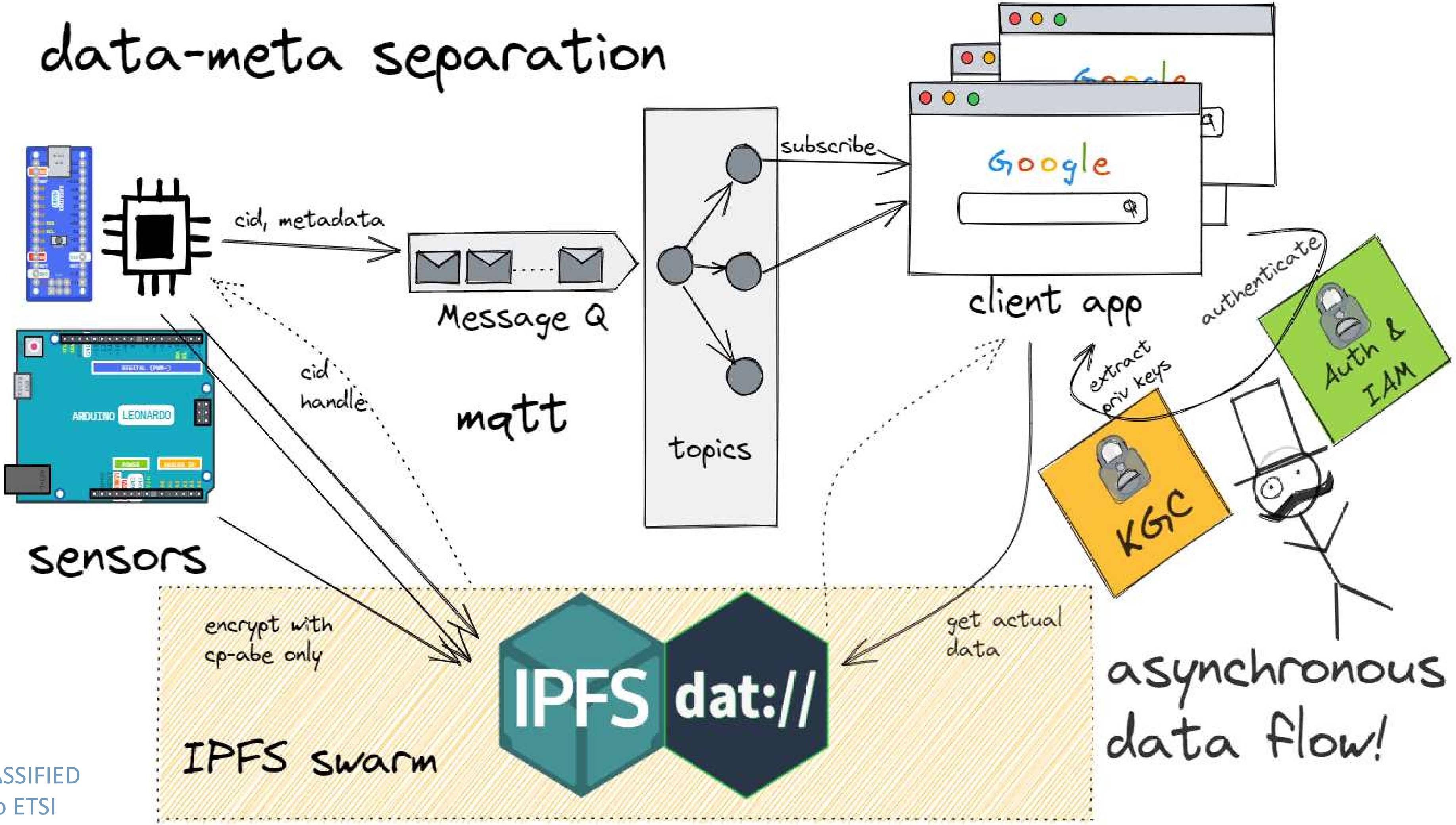
```
{
  "mbs": [
    {
      "dts": [
        {
          "cty": "json",
          "val": "UW1Sc0ZnblU1SnNoTmhQRzNNMjFXU1R4QlRRQUVMOEV1NkR1GX
        }
      ],
      "mds": [
        {
          "@context": {
            "@base": "urn:nato:stanag:5636:A:1:elements:json"
          },
          "crt": {
            "name": "NCIA",
            "type": "organization"
          },
          "dcr": "2021-07-0[illegible]",
          "sbt": [
            "IST-176"
          ],
          "ocl": {
            "cls": "UNCLASSIFIED",
            "dcr": "2021-07-05T11:43:[illegible]0.833879",
            "pol": "NATO"
          },
          "pub": {
            "name": "ncia",
            "type": "organization"
          },
          "ttl": "iot_image_processing_[illegible]636.3"
        }
      ]
    }
  ]
}
```

Optimized labelling formats

- New services require new formats
- XML – good for documents
- JSON – the choice for services and applications data
- CBOR – Internet of Things and constrained environments



Architectural patterns



Main takeways and future work

- IoT has a high potential to icrease effectiveness of C2 systems
- Security and interoperability are critical aspect
  - Access control and information sharing
- Federation requires a flexible approach to trust
  - Integrity, authorization and accountability
- Modern cryptography opens new opportunities
  - IBE, ABE, PSI, FHE
- Secure IoT pipeline – from sensor to C2 application
- Stay tune for more scientific results from the NATO STO IST-176

Takeways for standardization

- Increased dual use requires inclusion of defence requirements by design
  - IoT and smart environments
- Trustworthy data labelling
  - STANAG 4774 and 4778
- Provenance tracing
  - Where the data comes from, who owns the devices, by whom it was processed
- Federated trust and accountability
  - Permissioned distributed ledgers and smart contracts
- Cryptography and cryptographic access control
  - Post-quantum and lightweight crypto - largely covered by NIST
  - Attribute-based Encryption – and signatures?
  - Homomorphic encryption, multi-party computation, etc.

Some relevant standardization activities at ETSI

- SAREF
- oneM2M
- Data spaces
- Distributed ledgers
- ABE
- QKD
- ...

NATO OTAN

NATO Communications and Information Agency

NCI AGENCY

Questions?

konrad.wrona@ncia.nato.int