CYBER-SECURITY THREATS AND PROTECTION OF C4ISR SYSTEMS

Panagiotis Katsaros, Associate Professor
Aristotle University of Thessaloniki (GR)

PANAGIOTIS KATSAROS, MSc, PhD

School of Informatics, Aristotle Un. Of Thessaloniki

e-mail: katsaros@csd.auth.gr

url: http://delab.csd.auth.gr/~katsaros

https://depend.csd.auth.gr (Dependability research group)

- Research interests:

  31 peer reviewed journal articles, 70 conference papers, 4 PhD theses supervised on

  System dependability, **Software security**, **Formal (mathematical) verification of systems safety/security**

- Visiting Professor:
  - Department of Computer Science of the Stony Brook University in New York, 2010
  - Sino-Europe Institute of Dependable and Smart Software, Institute of Intelligent Software, Nansha, China, 2019
- Research funds (currently working 4 PhD students, 3 postdoctoral researchers):
  - **European Space Agency – Technology Research Program** (2014-2016): two projects on the engineering of spacecraft onboard software
  - **Horizon 2020 European Union program on Information and Communication Technologies** “Foundations for Continuous Engineering of Trustworthy Autonomy” (2020-2023)
  - **Hellenic Republic Research - Development - Innovation program** “Managing Forest Fires via IoT Technologies” (2020-2023)

Critical success factors in military operations

- Situational awareness

  The knowledge of where you are, where other friendly elements are located, and the status, state, and location of the enemy.

- Information superiority

  The relative advantage of one opponent over another in commanding and controlling his force.

  - make rapid and appropriate decisions using superior technical information means

  - act in order to degrade and deny these same capabilities to the opponent while protecting our own capability

C4ISR systems

- **C**ommand and **C**ontrol

  The exercise of authority & direction by a commander over assigned forces in the accomplishment of the mission.

- **C**ommunications and **C**omputers

  Process and transport information.

- **I**ntelligence

  Information and knowledge about foreign countries or an adversary obtained through observation, investigation, analysis, or understanding.

- **S**urveillance

  Systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.

- **R**econnaissance

  Obtain, by visual observation or other detection methods, information about the activities and resources of an enemy, or secure data concerning the characteristics of an area.

C4ISR potential

- C4ISR systems provide
  - timely intelligence
  - greater situational awareness
  - a single integrated operational picture of the battlefield

and support new modes of military operation including

  - greater freedom of action for small, decentralised forces
  - the massing of firepower rather than massing of forces

Examples of C4ISR systems

- Global command & control:

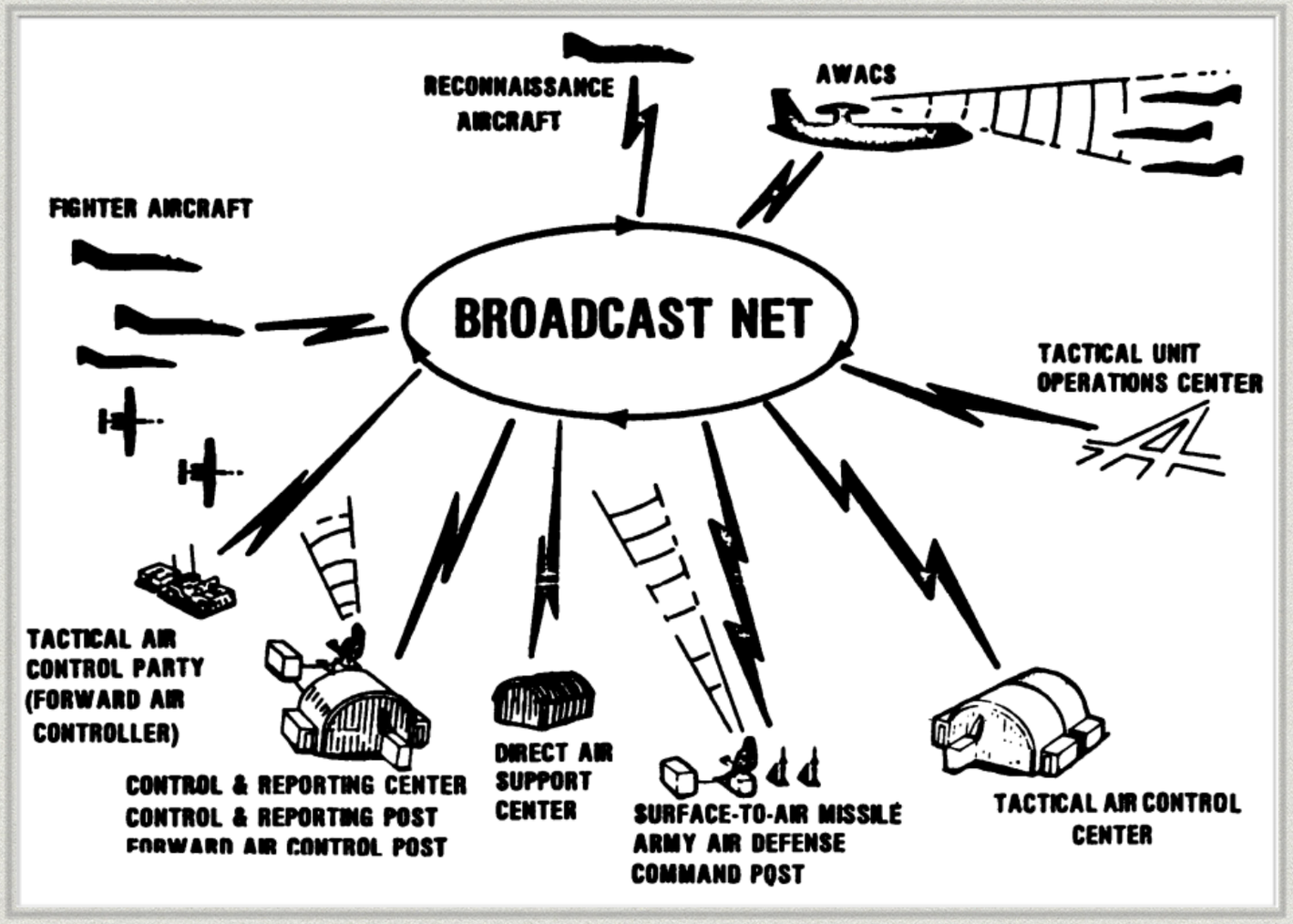
  integrated picture of the battlefield, planning and assessment

- Field Artillery Tactical Data System:

  automated fire support command and control functions

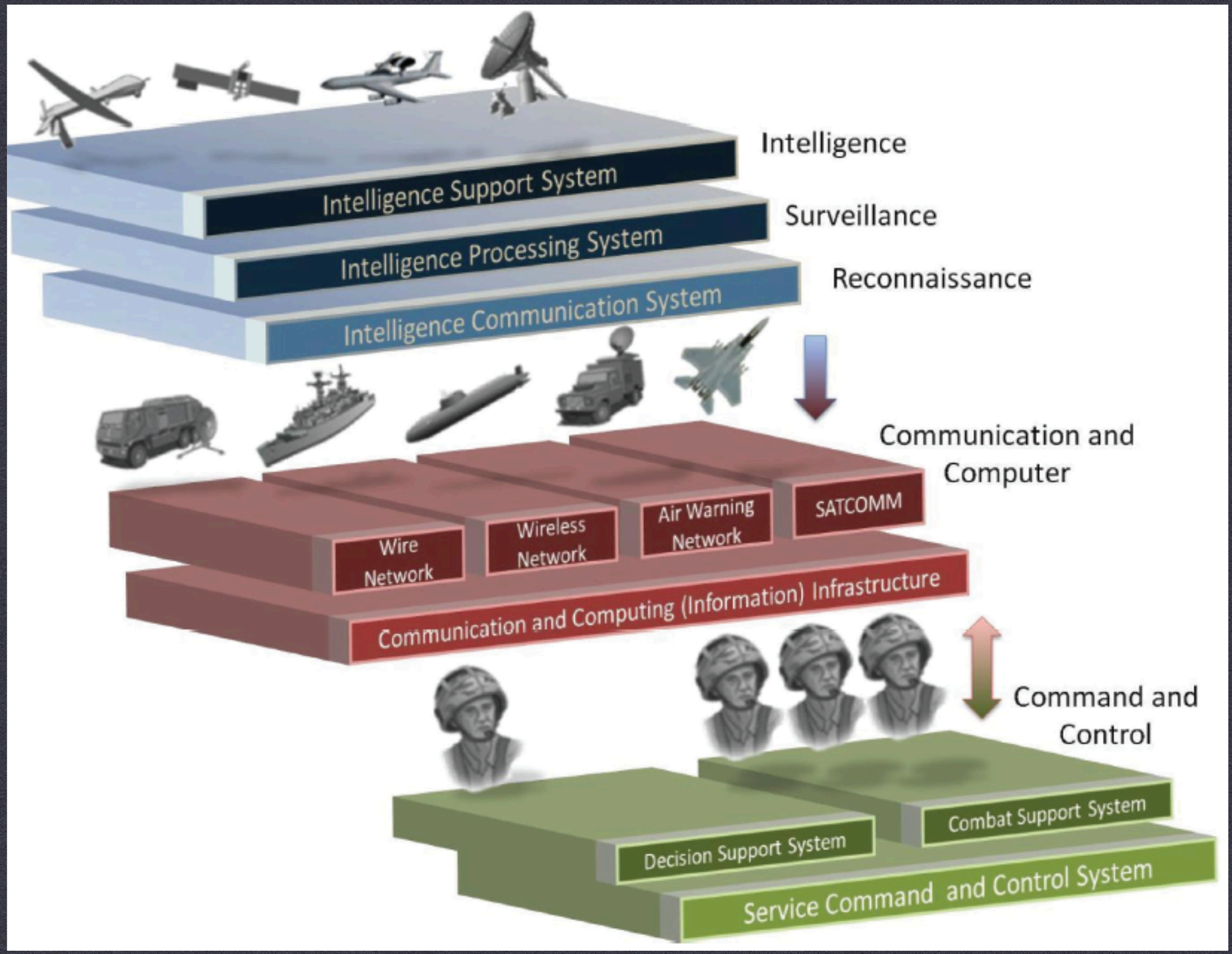
- Joint Tactical Information Distribution System:

  secure, anti-jam-protected digital data and voice communications for theater, air, ground, and naval forces



C4ISR challenges

- C4ISR systems are based on rapidly advancing computing and communications technology, driven
  - primarily by commercial solutions
  - continuous technology exploitation, if superiority is to be maintained (potential adversaries may have access to the same underlying information technologies)
- Ultimate goal: improved military effectiveness
  - evaluate the impact of information technology to drive budget trade-offs between C4ISR and other systems



INTEGRATED & INTEROPERABLE SYSTEMS

Figure: The concept of C4ISR (Application of Cyber Security in Emerging C4ISR Systems, Malik et. al., 2012)

C4ISR challenges

Success depends on meeting the challenges (1) and (3) with respect to acquisition and effective use of C4ISR technologies.

1. **Interoperability**

   - operational interoperability: ability of systems, units, or forces to provide services to or access services from other systems, units, or forces, and use the services to operate effectively together.

   - technical interoperability: condition achieved among communications-electronics systems when information or services can be exchanged directly and satisfactorily between them and/or their users

2. **Information systems security**

   - poses a high level of current risk

3. **Processes and culture involving C4ISR**

C4ISR interoperability

- C4ISR systems must be able to share data in a timely, reliable manner that is operationally useful, and must operate across service or agency boundaries to support joint missions.
  - Federated Mission Networking (FMN) is a NATO initiative to help ensure interoperability and operational effectiveness of C4ISR and decision-making by enabling rapid instantiation of mission networks.
- There are trade-offs between security and interoperability.
  - Interoperability can promote an attacker's access to diverse systems, thus facilitating the rapid spread of attacks.
  - Ad hoc work-arounds to overcome a lack of inherent interoperability can introduce many hard-to-manage security problems.
  - Potential for interoperability problems when introducing new security features into part of a larger system of systems.

C4ISR technical interoperability

- For two C4ISR systems interoperate, they must be able not only to exchange relevant bitstreams but also to interpret the bits they exchange according to consistent definitions.
- Interoperability requires that the format and semantics of exchanged data are coordinated.
  - e.g. if using non-co-located sensors for fire control, the implicit assumption of identical Earth models for target and launcher geographical coordinates may not be valid
- Technical interoperability poses requirements at multiple levels, from physical interconnection to correct interpretation by applications of data that is provided by other applications.

Technical approaches to interoperability

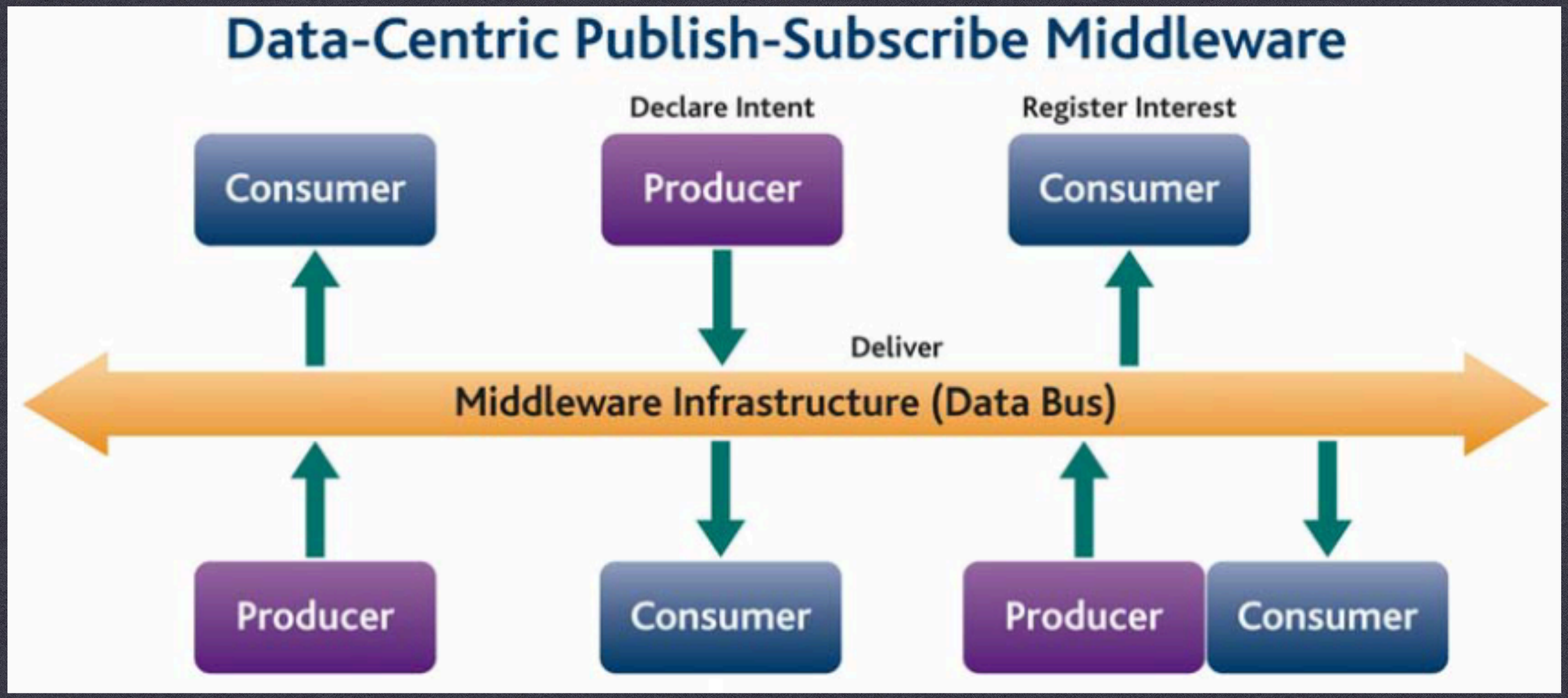
- Invest on an information systems environment based on:
  - clean architecture (an hierarchical description of the design of a system and how it will be developed, evolved, and operated)
  - common data structures
  - common interface requirements (whenever one component or subsystem needs to interact with another) and well-specified information flows
  - middleware to reduce dependence on particular operating systems and provide higher-level functions to be used in common among applications
- To design a system of systems, identify layer abstractions that correspond to widely adopted standards:
  - they are accepted by multiple vendors
  - make it easier to exploit changing technologies
  - provide an understanding of data or a platform common to all component developers

Data interoperability

- Designers of individual systems tend to make locally optimal decisions about data definitions and formats.
- Data formats resulting from such local decisions may not be compatible when a network of systems are called upon to interoperate.
- Architectural design has to minimise the applications-layer incompatibilities that inevitably arise when systems with different purposes must communicate with each other.
- According to the data “bus” approach, each system can use its own data definitions internally, but
  - data exchanges are conducted through a “bus”, i.e., a common data standard into which data must be translated before being transmitted to another system
  - any system wishing to use this data then downloads it from the “bus” and retranslates the data into locally meaningful terms before that data is used.

The Data Distribution Service (DDS)

- DDS is widely deployed in mission-critical (military) systems
  - e.g. the US Army Software Engineering Directorate has chosen DDS to be the communications architecture backbone for its Network Operation Center
- It is a standard-based middleware
  - for distributed systems with real-time constraints
  - for handling data distribution in a predictable, deterministic, and efficient way
- It decouples space, time, and flow via
  - anonymous publish/subscribe protocols
  - scalability
  - platform flexibility



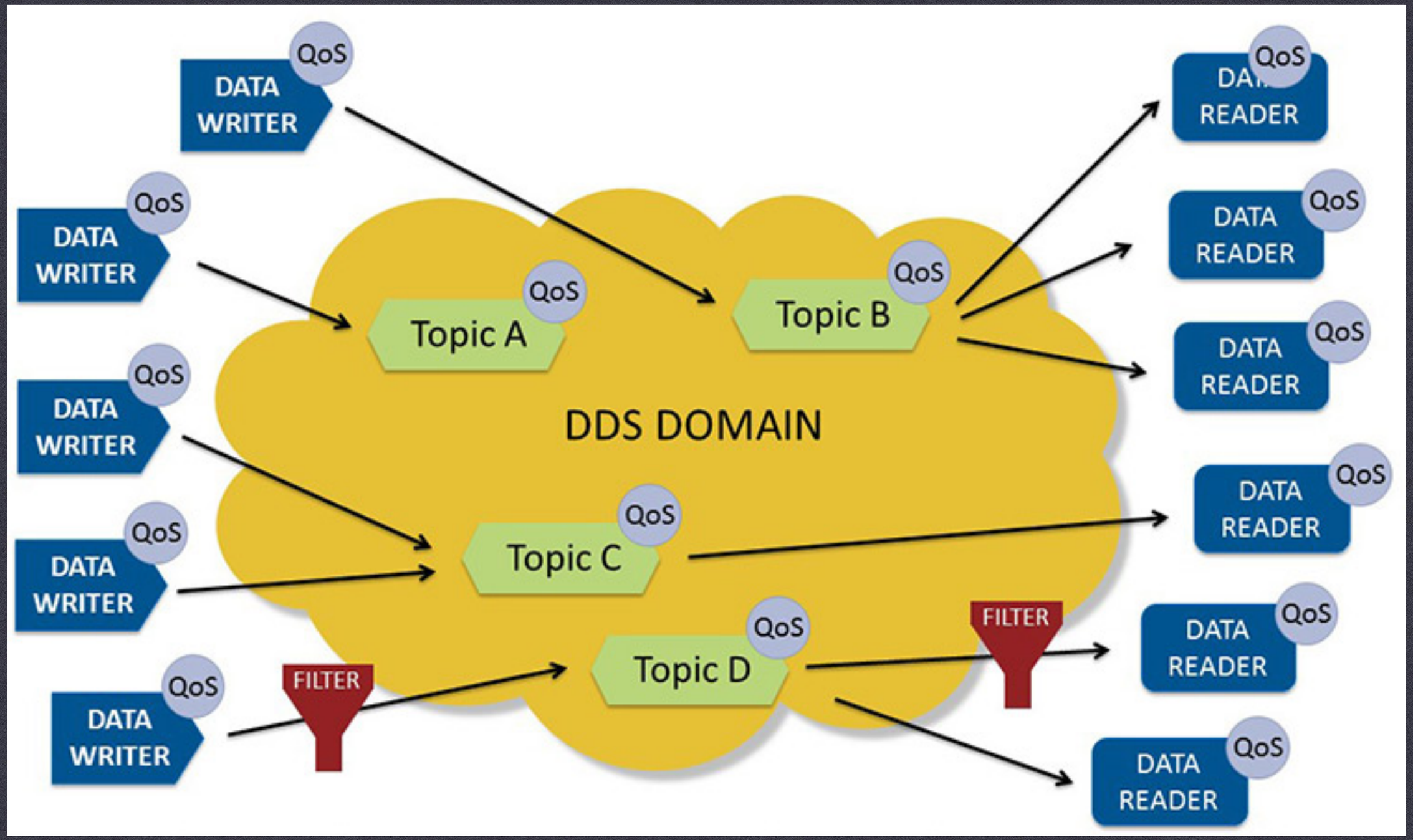
A DDS application is composed of data providers & consumers, each potentially on different computers.

A data provider publishes “topics” whereas consumers subscribe. An application may both publish and subscribe.

Figure: The Data Distribution Service - Reducing Cost through Agile Integration, UAS Control Segment, 2011

The Data Distribution Service (DDS)

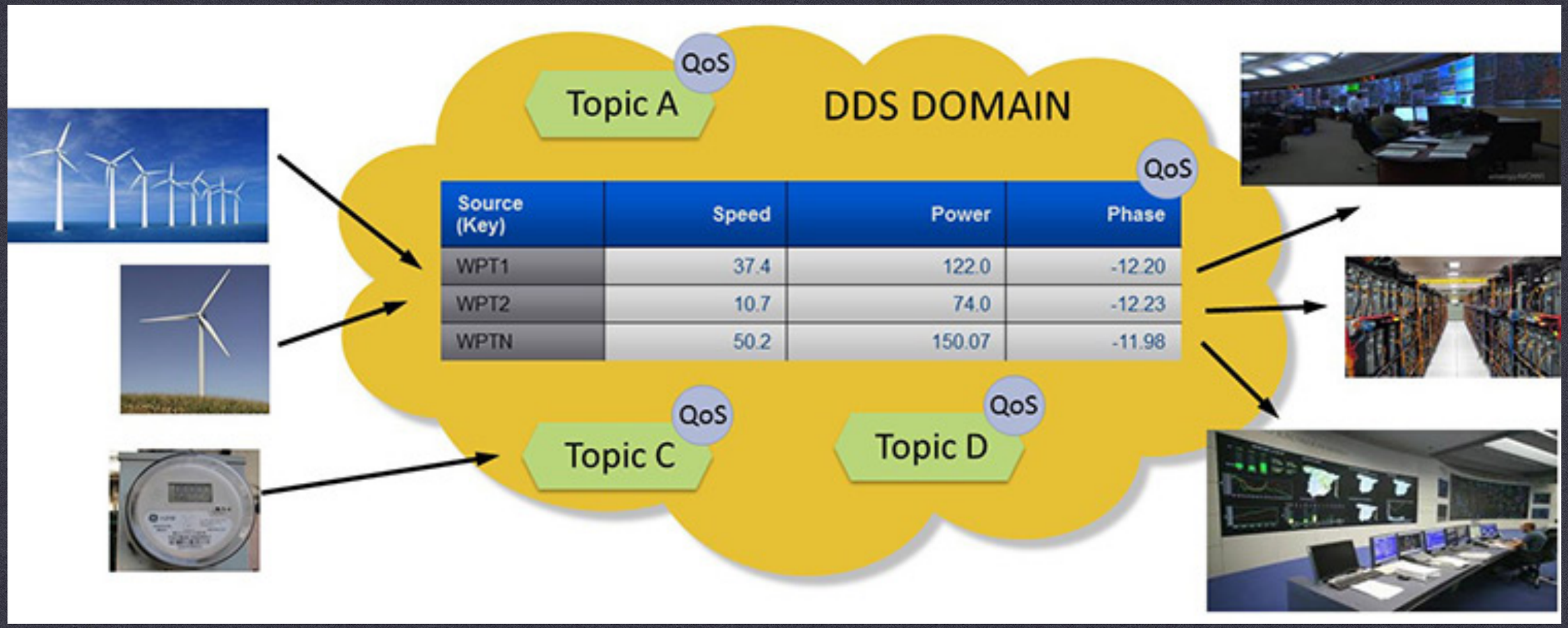
- DDS creates a global shared data-space that simplifies integration.
  - it transmits data directly from a publisher to all its subscribers with no intermediate servers.
- Publishers and subscribers can join or leave easily, be anywhere, publish at any time, and subscribe to any data (with permission).
- Timing and flow are precisely controlled.
- Computer platform and language differences are automatically translated.



DDS provides QoS-controlled data-sharing. Subscriptions can specify time and content filters and get only a subset of the data being published on the Topic.

Different DDS Domains are completely independent from each other. There is no data-sharing across DDS domains.

Figure: https://www.dds-foundation.org



The unit of information sharing is data-objects within Topics. Each application locally stores only what it needs and for as long as it needs it. DDS maintains a global data space (virtual concept), i.e. a collection of local stores.

The global data space shares data between embedded, mobile, and cloud applications across any transport, regardless of language or system, and with extremely low-latency.

Figure: https://www.dds-foundation.org

The Data Distribution Service (DDS)

- DDS allows large systems to be assembled freely from any components, from any suppliers
  - components that use one vendor's middleware are able to work with other systems running different middleware
  - this enables a competitive market for subsystem components
- DDS systems can add, modify, restart or update new modules without redesigning other interfaces
  - system integration is done one component at a time without impacting other components
  - automatic discovery eliminates most configuration control issues and supports networks that change at runtime
  - even live systems can be dynamically updated

C4ISR system security

Security is a system problem (involves hardware, software, humans, procedures).

C4ISR systems must be interconnected, but these interconnections multiply many-fold the opportunities for an adversary to attack them.

Two dimensions of security:

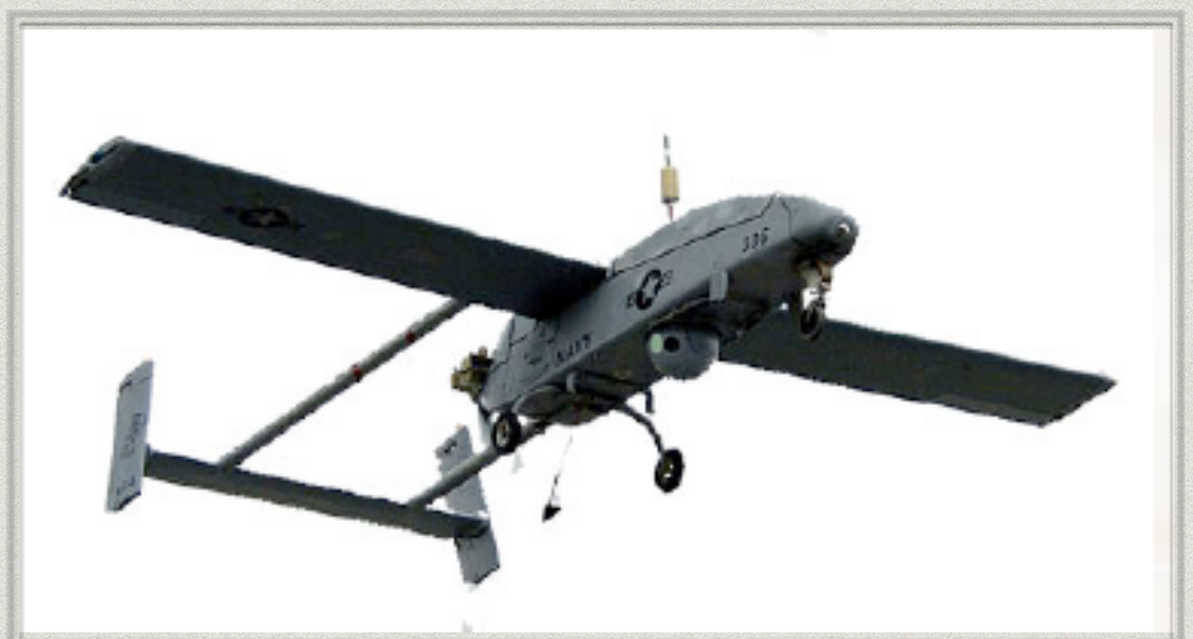
- Security at the physical level: protect the computers and communications links as well as command and control facilities from being physically destroyed or jammed.
- Information system security:
  1. Secure the data-centric bus (interoperability challenge)
  2. Integration of security across domains
  3. Securing the operating system
  4. Securing the hardware & software configuration

Focus of this presentation.

C4ISR security requirements

- **Authentication**
  - required to allow any principal to carry out an operation or to access any part of the system
  - ensures that the principal is indeed the one who he/she claims to be
- **Access control**
  - provides different levels of access (e.g. deny/permit) based on (i) the identity of the principal needing the access and (ii) the kind of operation or the system part needing to be accessed
- **Confidentiality**
  - restrict access to any information to authorised principals only, and prevent others from being able to access
- **Non-repudiation**
  - digitally sign any access/operation to render impossible to deny that it took place
- **Availability**
  - information is not denied to authorised principals for any reason

Data security example: UAV



	Authentication	Access control	Integrity	Non-repudiation	Confidentiality
UAV health data	X		X		
Remote commands	X	X	X	X	X
Sensor data	X	X	X		X

Net-centric security model for C4ISR

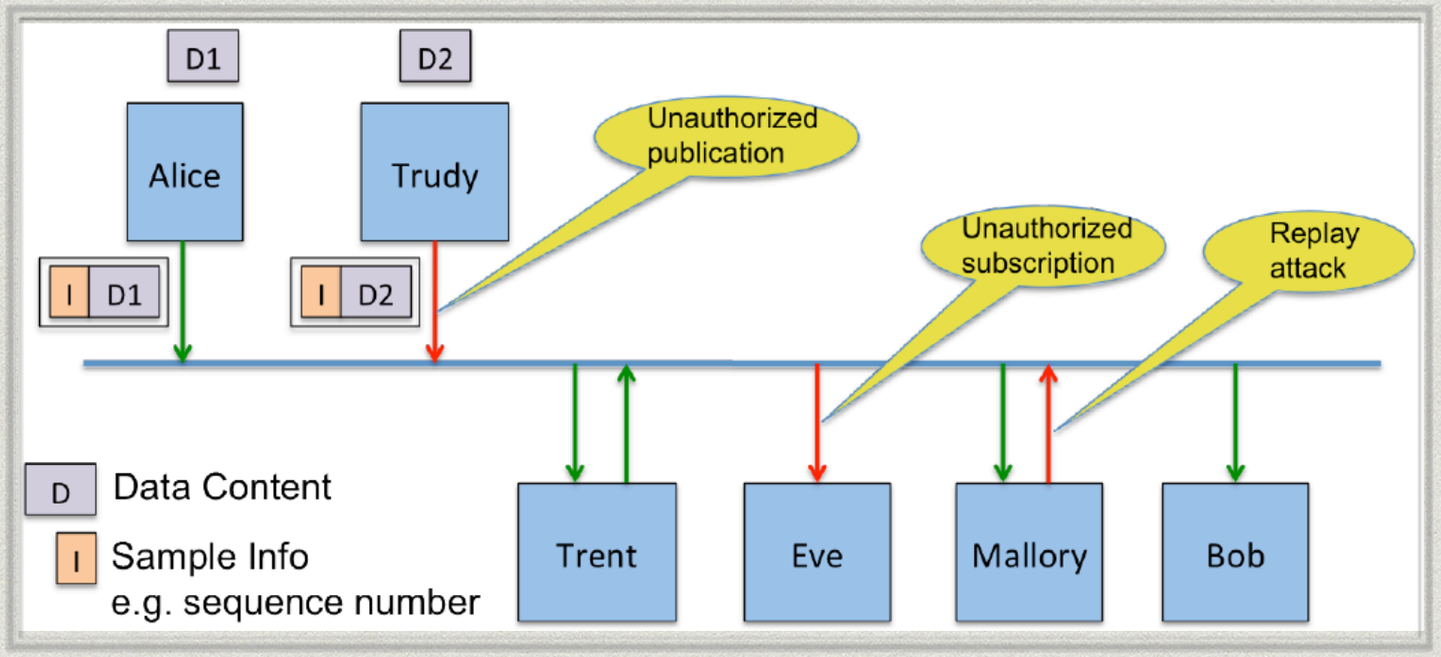
- DDS-based systems work over a global data space where anybody can access the information it needs, whereas publishers are unaware of subscribers and vice-versa
  - this does not mean loss of access control to the information (similarly to access control policies for file systems)
  - possible to enforce access control per topic with read and write permissions
- The C4ISR global data space must have an associated security model and use standard PKI and cryptographic techniques to enforce the security policies.

Security Model for DDS

- The Security Model defines the principals, the objects to be secured, and the operations on the objects to be restricted. Securing the DDS global data space means:
  - Confidentiality of the data samples
  - Integrity of the data samples and the messages that contain them
  - Authentication of DDS writers and readers
  - Authorisation of DDS writers and readers
  - Message-origin authentication
  - Data-origin authentication
  - Non-repudiation of data
- Applications that use DDS must first be authenticated.
- Next step is to enforce access control decisions by cryptographic techniques so that information confidentiality and integrity can be maintained (this requires an infrastructure to manage and distribute the necessary cryptographic keys).

Cyber-security threats

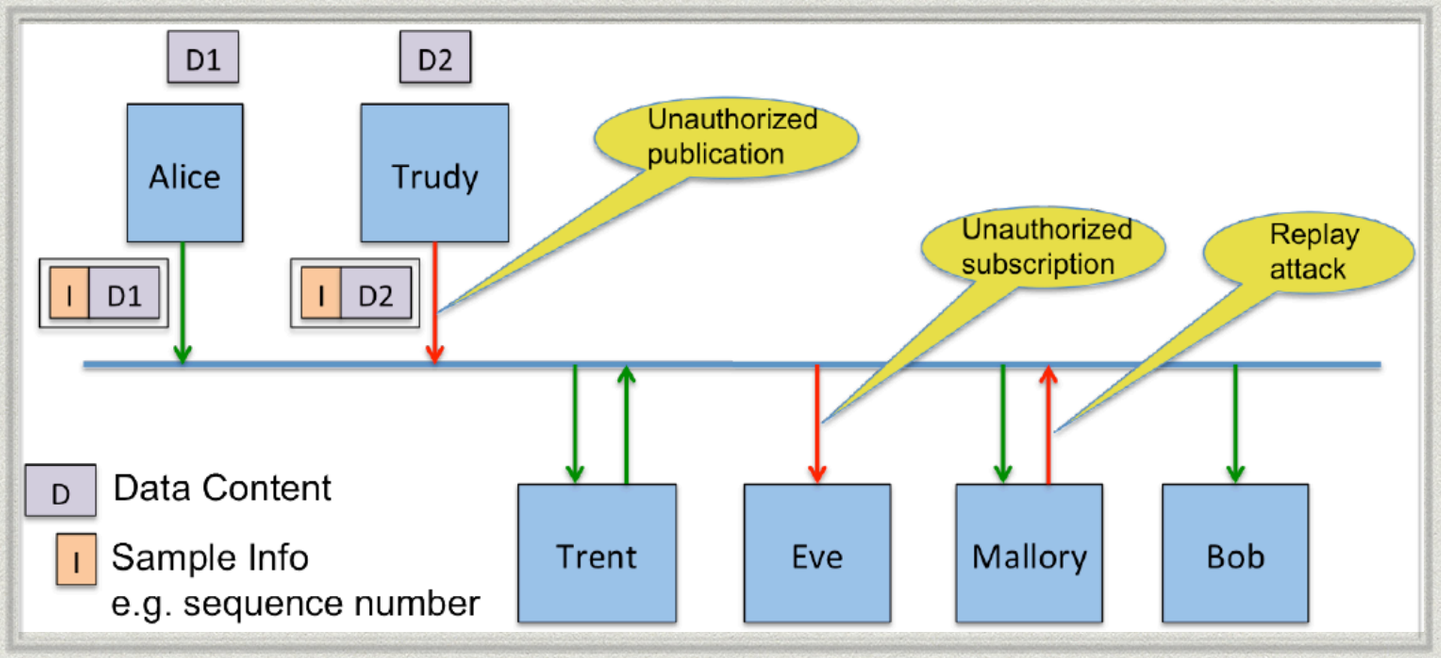
- **Alice**. DomainParticipant authorised to publish data on a Topic T.
- **Bob**. DomainParticipant authorised to subscribe to data on a Topic T.
- **Eve**. An eavesdropper; **not authorised** to subscribe to data on Topic T, but is connected to the same network and trying to see the data.
- **Trudy**. A DomainParticipant intruder; **not authorised** to publish on Topic T, but is connected to the same network and trying to send data.
- **Mallory**. Malicious DomainParticipant, authorised to subscribe to data on Topic T, but **not authorised** to publish on Topic T. Tries to convince Bob that she is a legitimate publisher.
- **Trent**. A trusted service (e.g. relay service) who needs to receive and send information on Topic T (not trusted to see the content of the information).



Cyber-security threats

- **Unauthorised subscription**. DomainParticipant Eve is connected to the same network infrastructure and is able to observe the network packets despite the fact that the messages are not intended to be sent to Eve.
- Protection

Alice has to encrypt the data she writes using a secret key that is only shared with authorised receivers such as Bob, Trent, and Mallory.

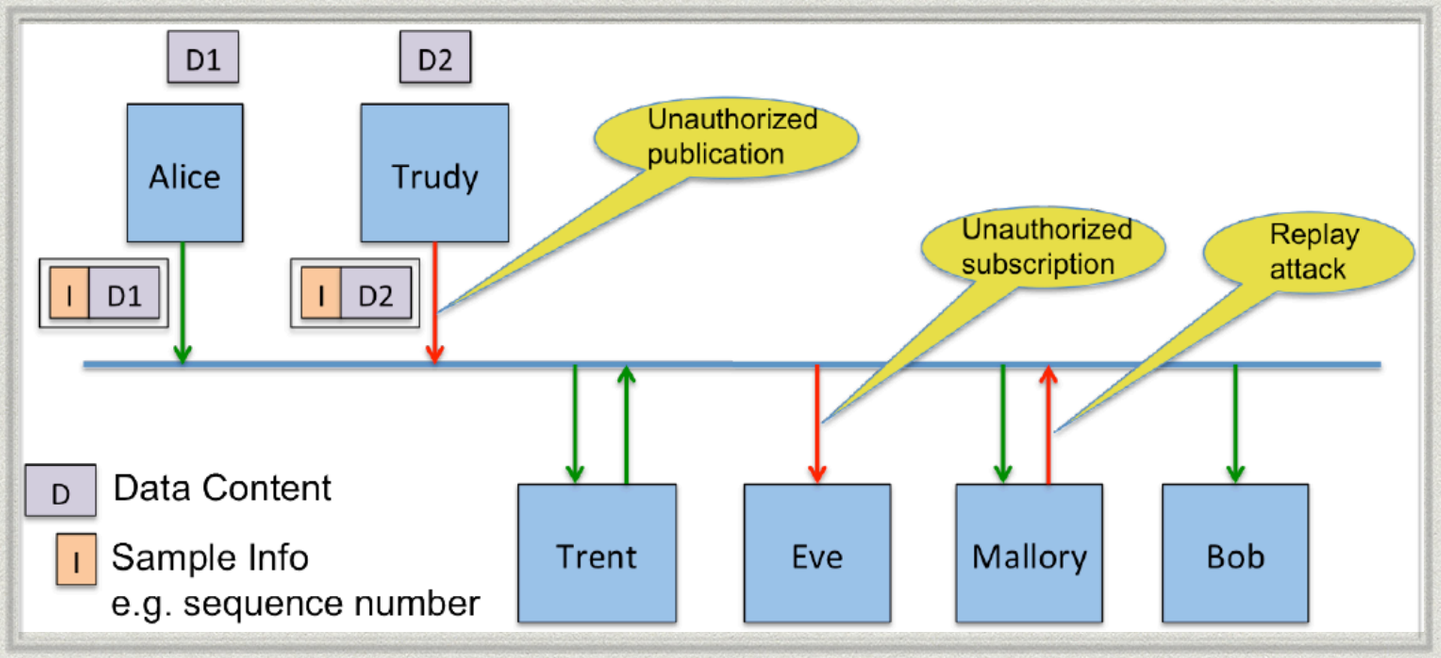


Cyber-security threats

- **Unauthorised publication** DomainParticipant Trudy is connected to the same network infrastructure and injects network packets with any data contents, headers and destination she wishes (e.g., Bob). The network infrastructure will route those packets to the indicated destination.
- Protection

  Bob, Trent and Mallory need to realise that the data is coming from someone not authorised to send data on Topic T and therefore reject (i.e., not process) the packet.

  The protocol will have to require that the messages include either a hash-based message authentication code (HMAC) or digital signature.



Cyber-security threats

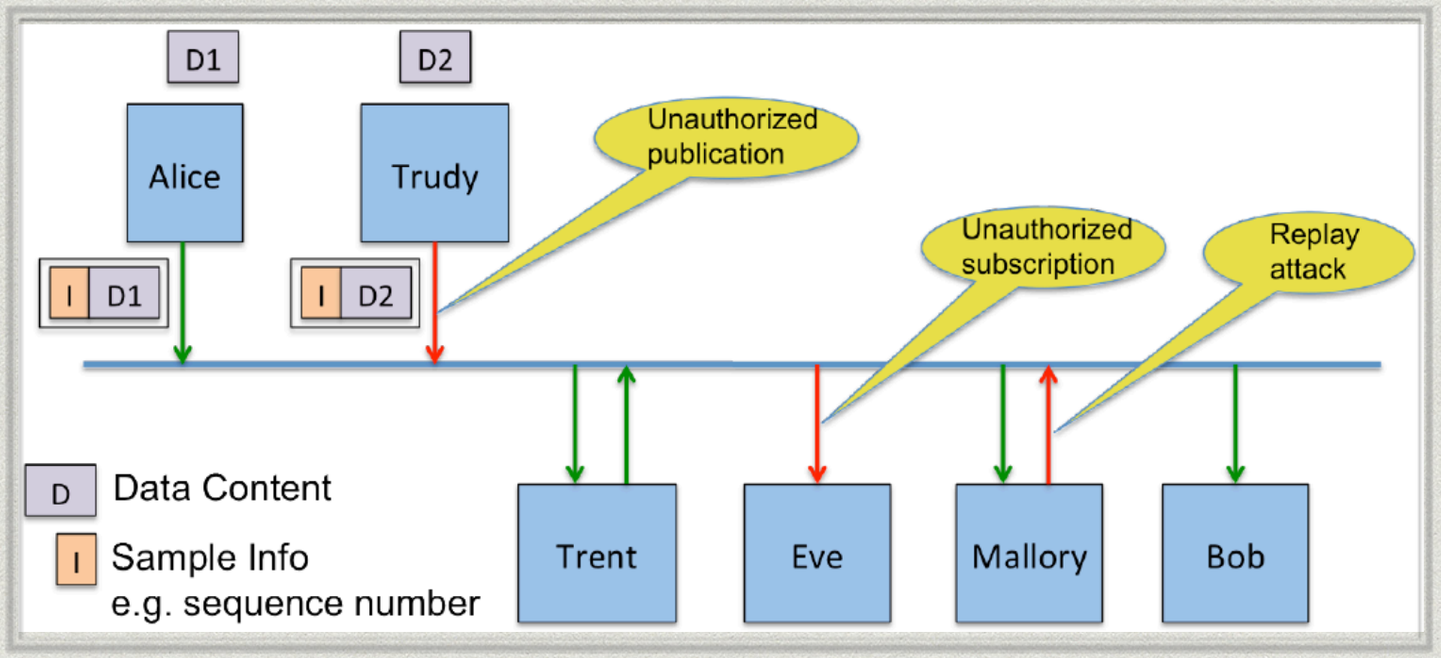
- **Tampering and replay**. Mallory is authorised to subscribe to Topic T. Therefore, Alice has shared with Mallory the secret key to encrypt the topic and also, if an HMAC is used, the secret key used for the HMAC.

  Mallory can use her knowledge of the secret keys used for data encryption and the HMACs to create a message on the network and pretend it came from Alice.

  Bob and the others will have no way to see that the message came from Mallory and will accept it, thinking it came from Alice.

- Protection

  Alice must share a **different secret key** for the HMAC with each recipient. Then Mallory will not have the HMAC key that Bob expects from Alice and Mallory's messages to Bob will not be misinterpreted as coming from Alice.



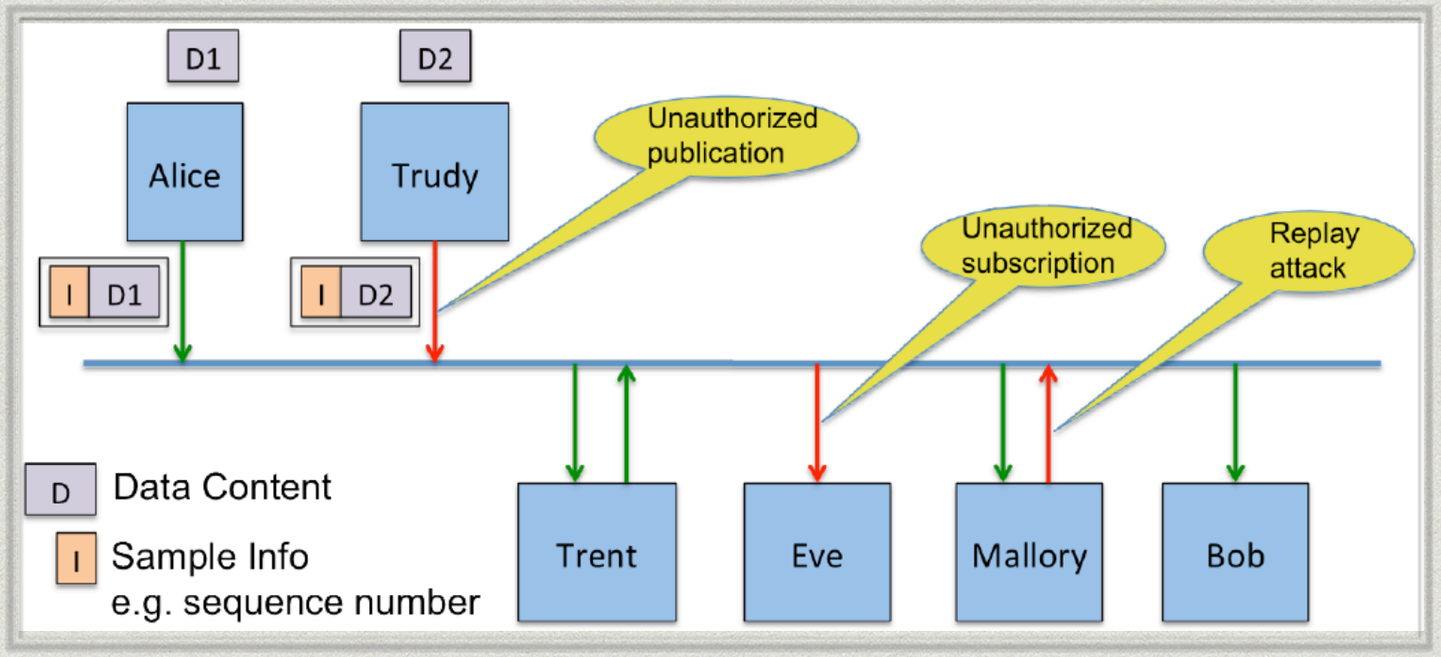
Cyber-security threats

- **Unauthorised Access to Data by Infrastructure Services**
  Infrastructure services (e.g. persistence or relay services) should be able to receive messages, verify their integrity, store, and send them to other participants on behalf of the original application.

  These services (like Trent) can be trusted not to be malicious; however, often it is not desirable to grant them the privileges to allow them to understand the contents of the data.

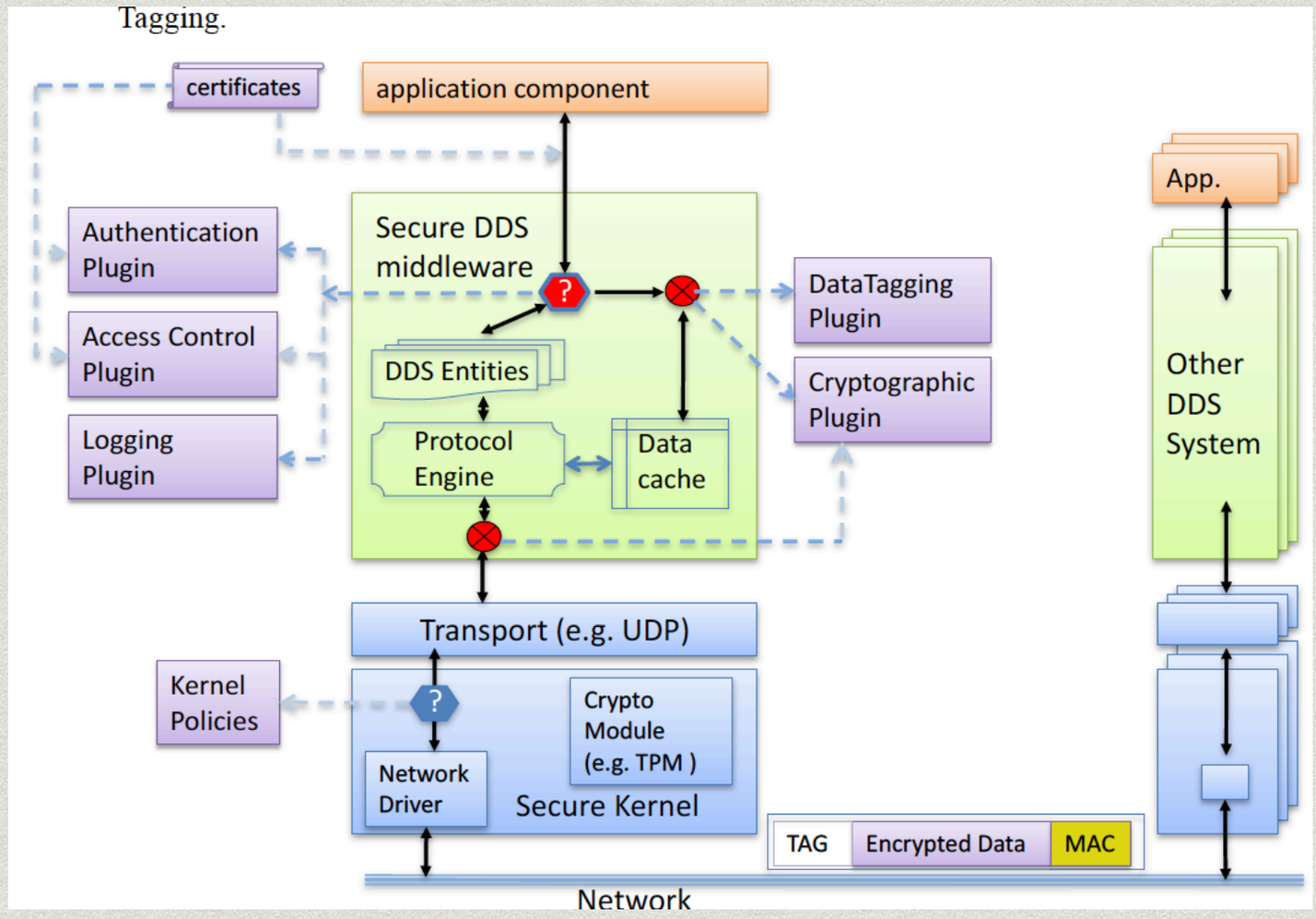
- Protection

  Alice needs to accept Trent as a valid destination for messages on T and share the secret key to compute the HMAC for Trent, but not the secret key used to encrypt the data itself.



The DDS Security standard

- Defines the Security Model and Service Plugin Interfaces (SPIs) used to enforce the security model.
  - SPI implementations enable out-of-the box security and interoperability between applications.
  - SPIs allow to customise the behaviour and technologies used for Authentication, Access Control, Encryption, Message Authentication, Digital Signing, Logging and Data Tagging.



Conclusion

- C4ISR systems are by definition
  - integrated and interoperable information systems
  - based on rapidly advancing computing & communications technology
  - driven by commercial DDS standard-based solutions (publish-subscribe)
  - aiming to share data in a timely, reliable manner that is operationally useful, and must operate across service or agency boundaries
- There are trade-offs between security and interoperability.
- We reviewed the threats and standard-based means to protect the C4ISR data-centric bus and develop/adopt
  - out-of-the box security policies
  - advanced technologies for Authentication, Access Control, Encryption etc.

Bibliography

- Realizing the Potential of C4I: Fundamental Challenges, National Research Council, 1999
- Data Distribution Service Version 1.4, Object Management Group, March 2015
- DDS Security Version 1.1, Object Management Group, July 2018

Thank you!

https://depend.csd.auth.gr

E-MAIL: katsaros@csd.auth.gr