NATO Communications and Information Agency

Cyber Security Information Sharing

Oscar Serrano
NCI Agency
Cyber Security Service Line

DeepSec 2014, Vienna, 21 November 2014

Cyber Security In NATO

- NATO in a nutshell:
  - Collective defence
  - Interoperable capabilities
  - Policies for sharing information
  - NATO has its own systems to protect
  - NATO relies on National systems for its missions and operations
- NATO's 2010 Strategic concept
  - Cyber security is a key concern
- NATO Computer Incident Response Capability (NCIRC)
  - Coordination Centre (CC)
  - Technical Centre (TC)
- Annual Cyber Coalition Exercise
- Many ongoing initiatives on cyber security information sharing

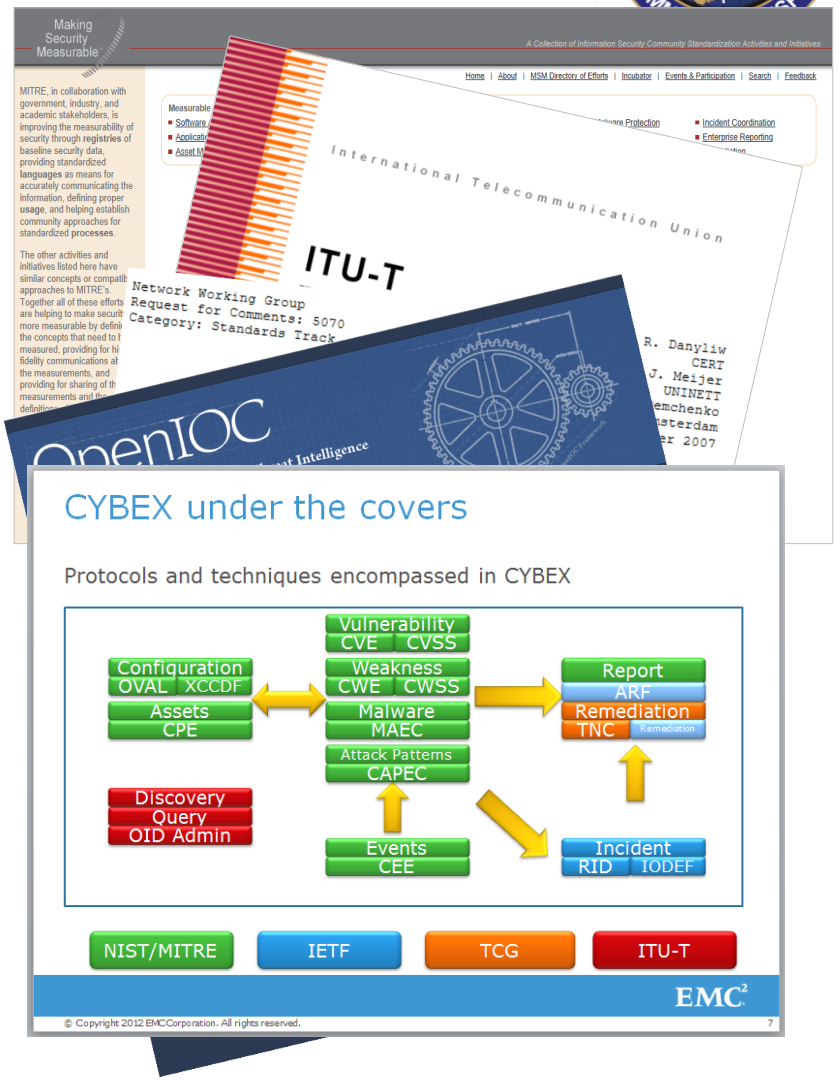
Cyber Security Data Overload

Drivers for Information Sharing

- Strategic drivers
  - CCDCOE's National Cyber Security Strategy Manual
  - NATO's new Cyber Defence Policy
  - U.S. Executive Order on Improving Critical Infrastructure Cybersecurity
  - UK's Cyber Security Information Sharing Partnership
- Operational drivers
  - Common systems, threats and vulnerabilities
  - Trusted communities
  - Too few qualified personnel
- Enablers
  - Standardization efforts
  - Commercial and open source software

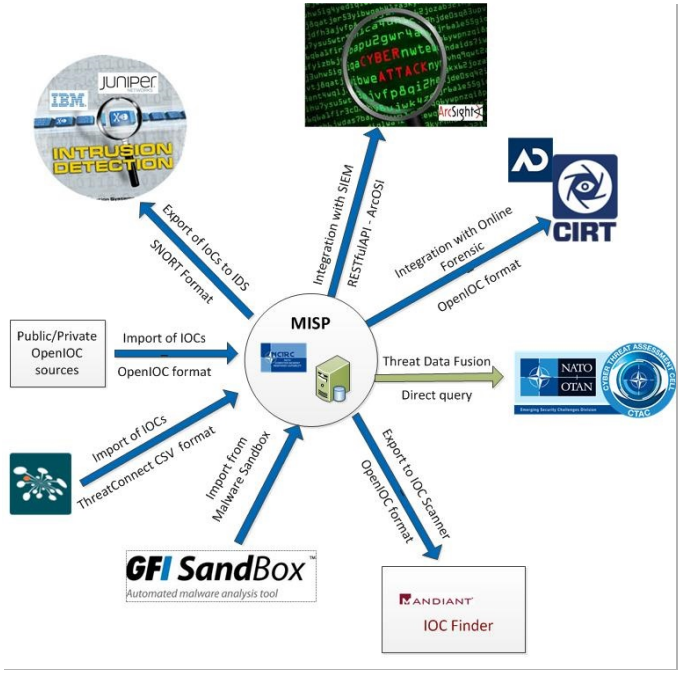
Standardization Efforts

- Standards:
  - US Govt / MITRE's “Making Security Measurable” program
  - ITU-T’s X.1500 CYBEX
  - IETF’s Incident Object Description and Exchange Format (IODEF) and Real-time Inter-network Defence (RID)
  - Vendor Formats
    - Proprietary or Open source
- Most are interoperable!



Existing Capabilities

- Platforms / Systems / Services / Organizations:
  - FS-ISAC Avalanche / Soltra Edge
  - Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA)
  - Microsoft's Interflow
  - Collective Intelligence Framework (CIF)
  - ITU's IMPACT
  - NATO's Malware Information Sharing Platform (MISP)
- Many efforts in other domains (e.g. bioinformatics)



Challenges !

- Policy and legal issues
- Many data sources available
- Timeliness requirement competes with quality requirement
- Multi-lateral, differentiated sharing is a requirement
- Sensitive data requires dissemination controls
- Current processes and technologies do not support well burden-sharing collaboration and outsourcing
- Managing uncertainly
- No direct financial benefit

Ongoing efforts must be continued,
but they must also be complemented !

Addressing the Challenges…

- Previous efforts have looked the formats for expressing the information to be exchanged and the transport mechanism…
- In cyber security, there are many challenges in the management and exploitation of exchanged data…
- In cyber security, these challenges are mostly common to all…

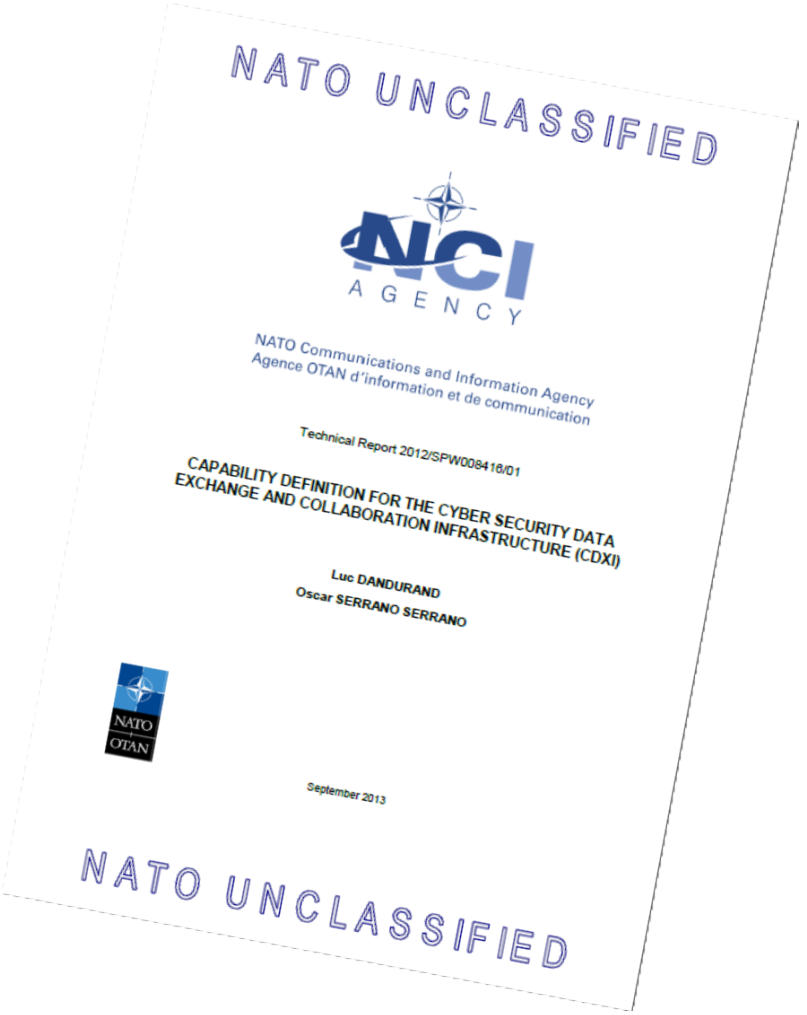
Shouldn't we aim for a common platform?

Manage, Share, Automate

- Collaboration is key
- Timely, high-quality information is critical
- Well-defined exchange policies
- Wide-scale sharing

CDXI Capability Definition Document

- Identifies 11 High-Level Requirements
  - Both necessary and sufficient
- Is publically available on request



High-Level Requirements (HLRs)

HLR #1: Provide a flexible, scalable, secure and decentralized infrastructure based on freely available software

HLR #2: Provide for the controlled evolution of the syntax and semantics of multiple independent data models and their correlation

HLR #3: Securely store both shared and private data

HLR #5: Enable the exchange of data across non-connected domains

HLR #4: Provide for customizable, controlled multilateral sharing

HLR #6: Provide human and machine interfaces

HLR #7: Provide collaboration tools that enable burden sharing on the generation, refinement, and vetting of data

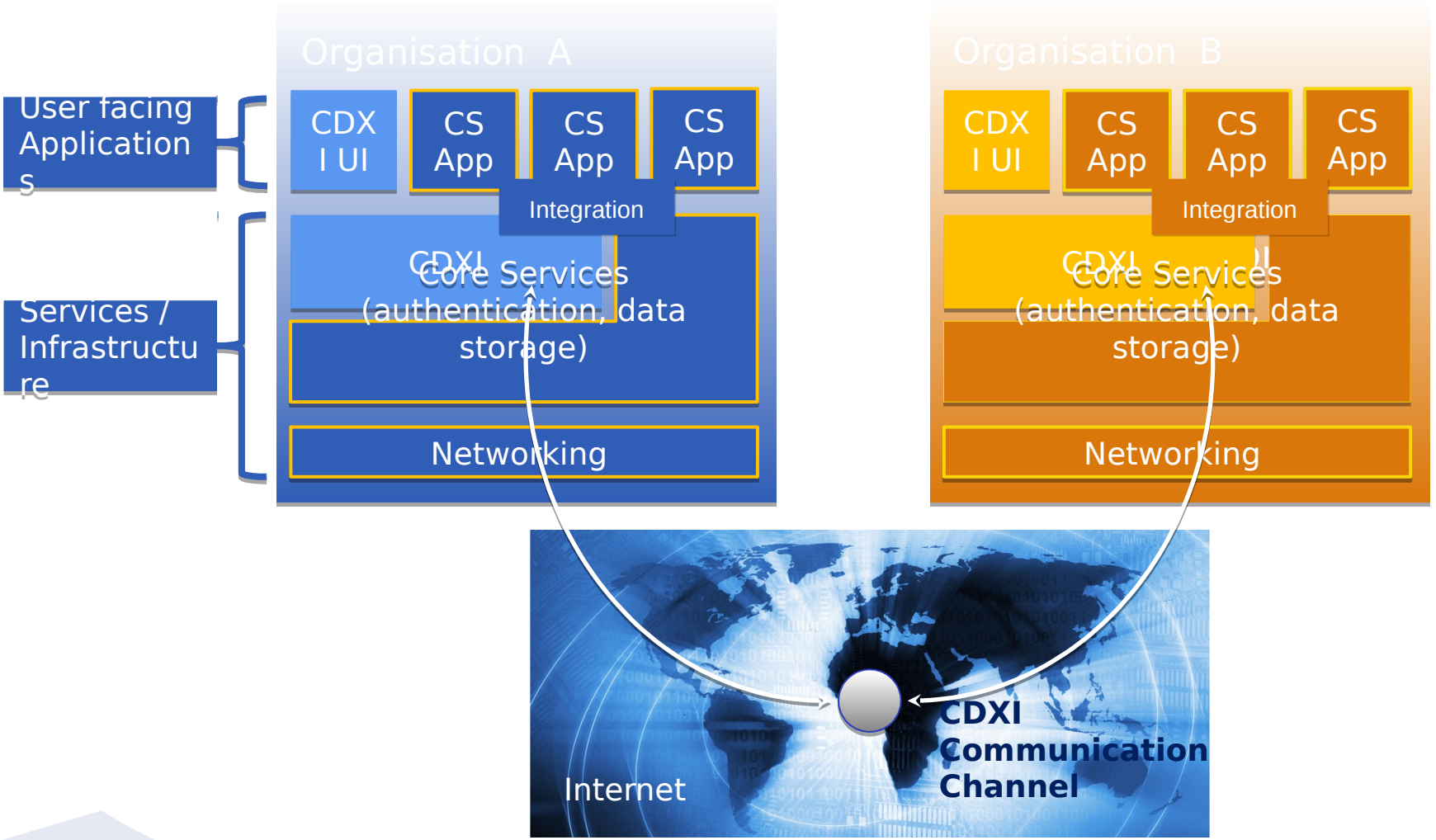
HLR #8: Provide customizable quality-control processes

HLR #9: Expose dissension to reach consensus

HLR #10: Support continuous availability of data

HLR #11: Enable commercial activities

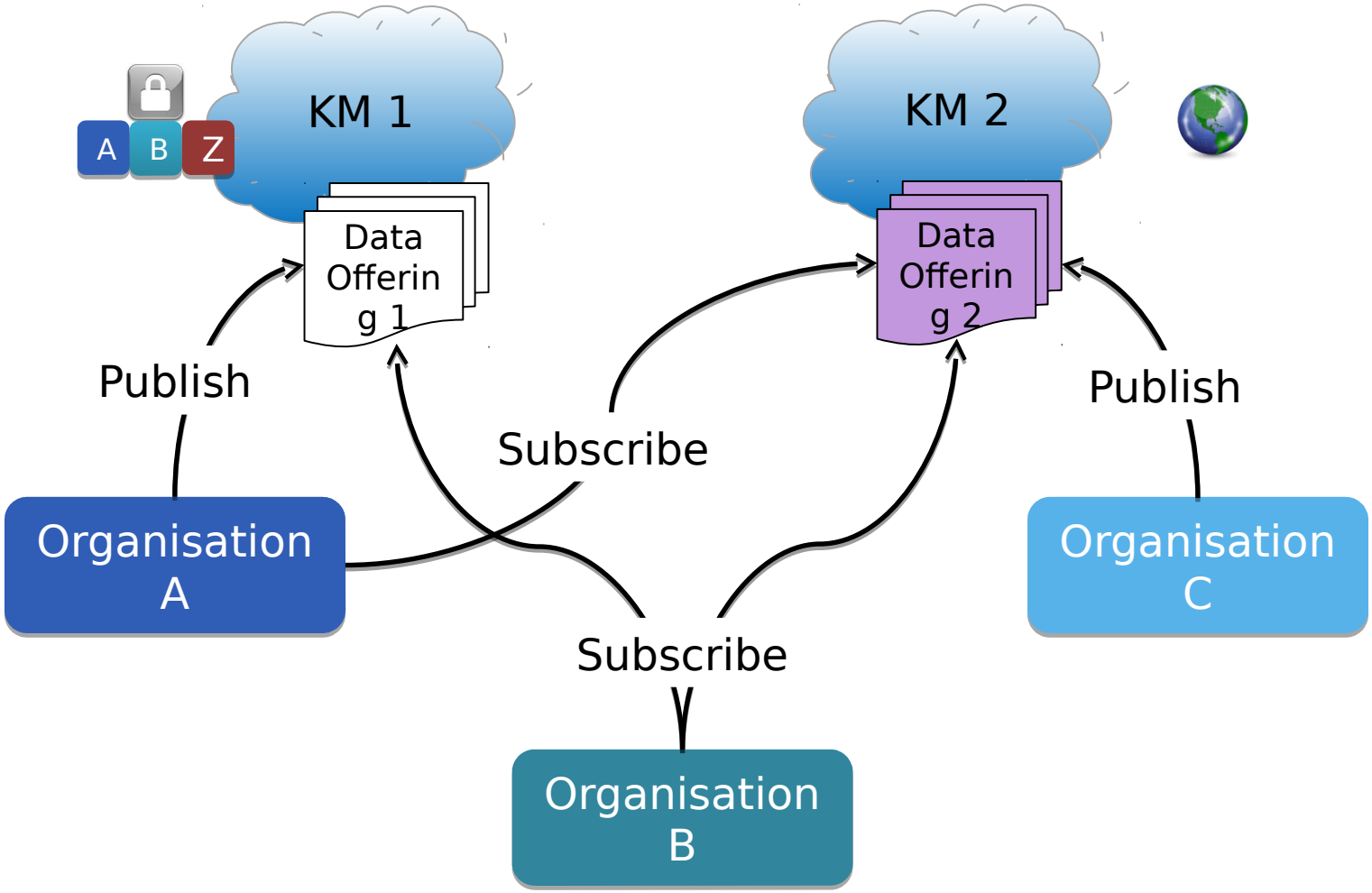
Deployment and integration



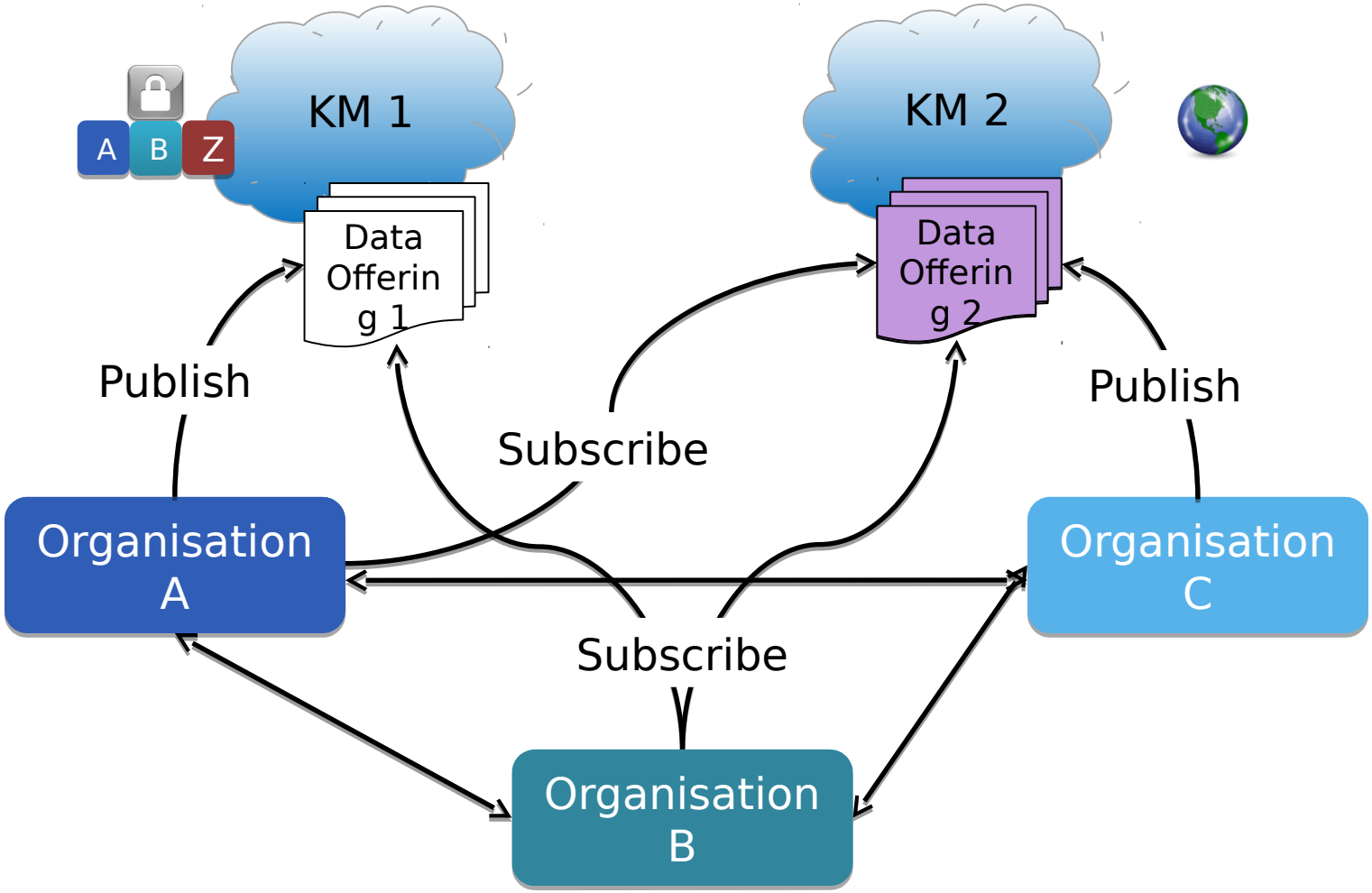
Information Exchange Policies

- Created at any organizational level
- For a data set or individual item
- Approved by legal departments
- Machine-readable encoding

Knowledge markets



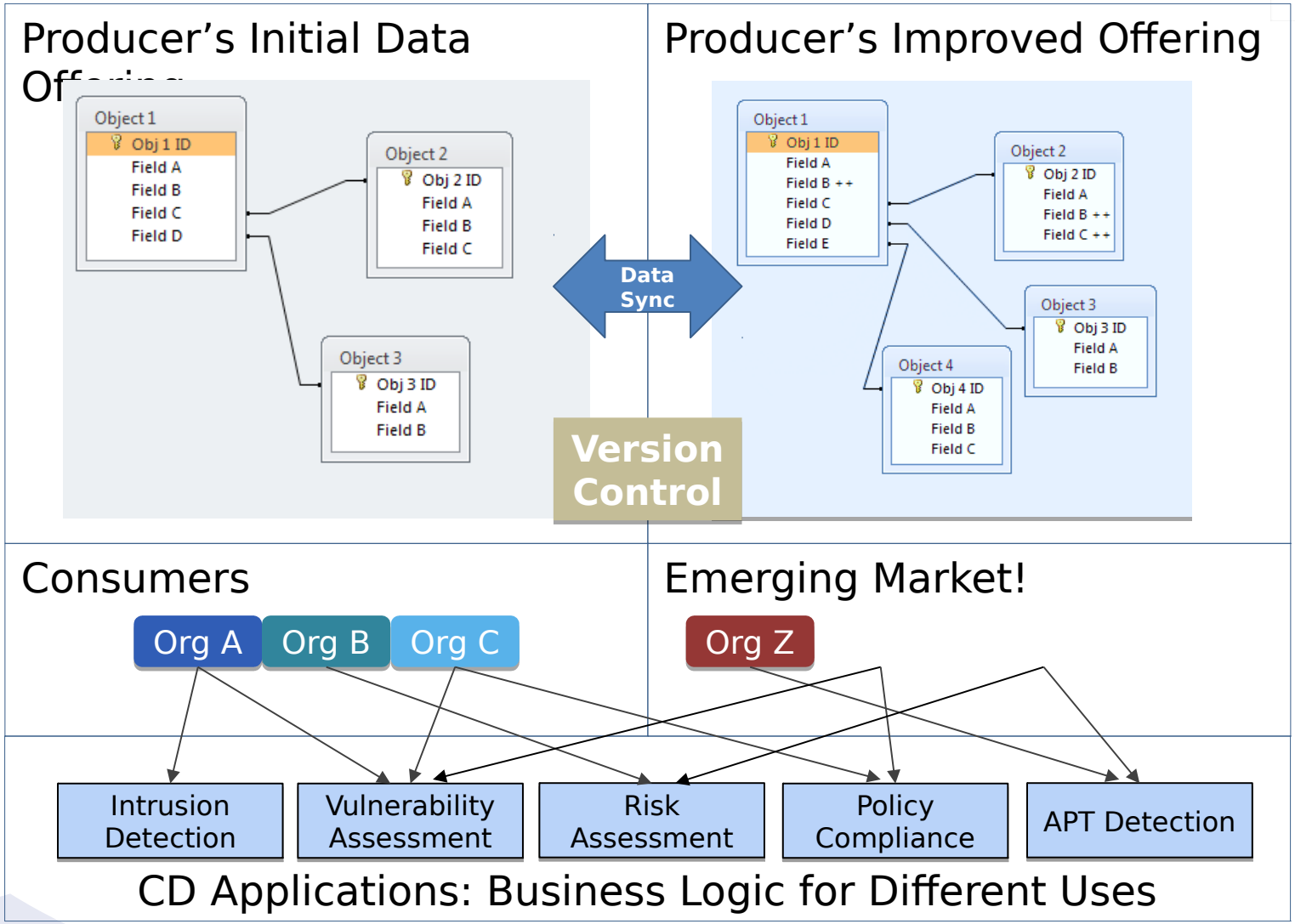
Knowledge markets



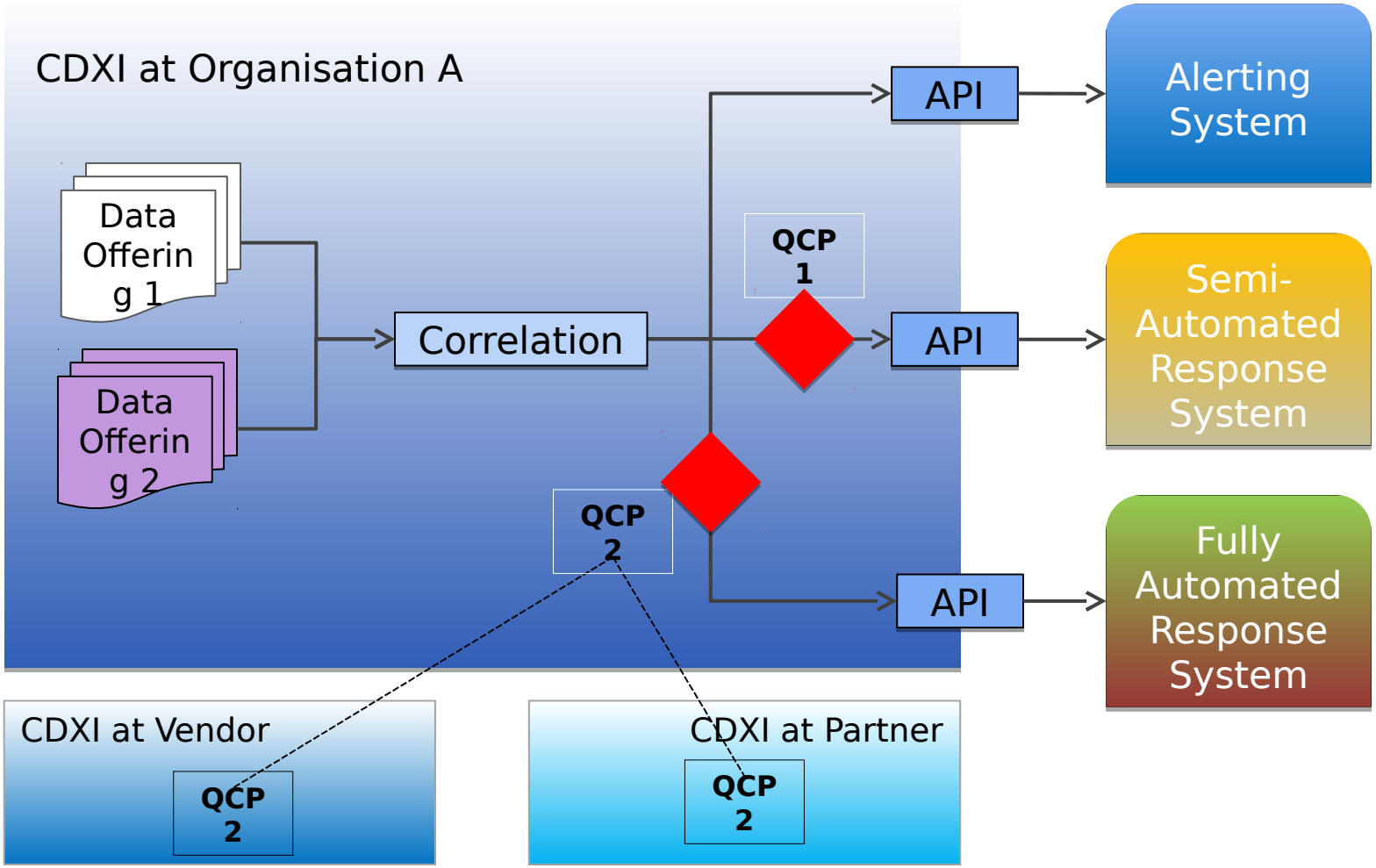
Ontologies

- Multiple, overlapping, evolving ontologies
- Aiming for one ontology is impractical
- Evolving size, scope, and depth of ontologies must be supported

Agile data model



Enabling automation



Other features

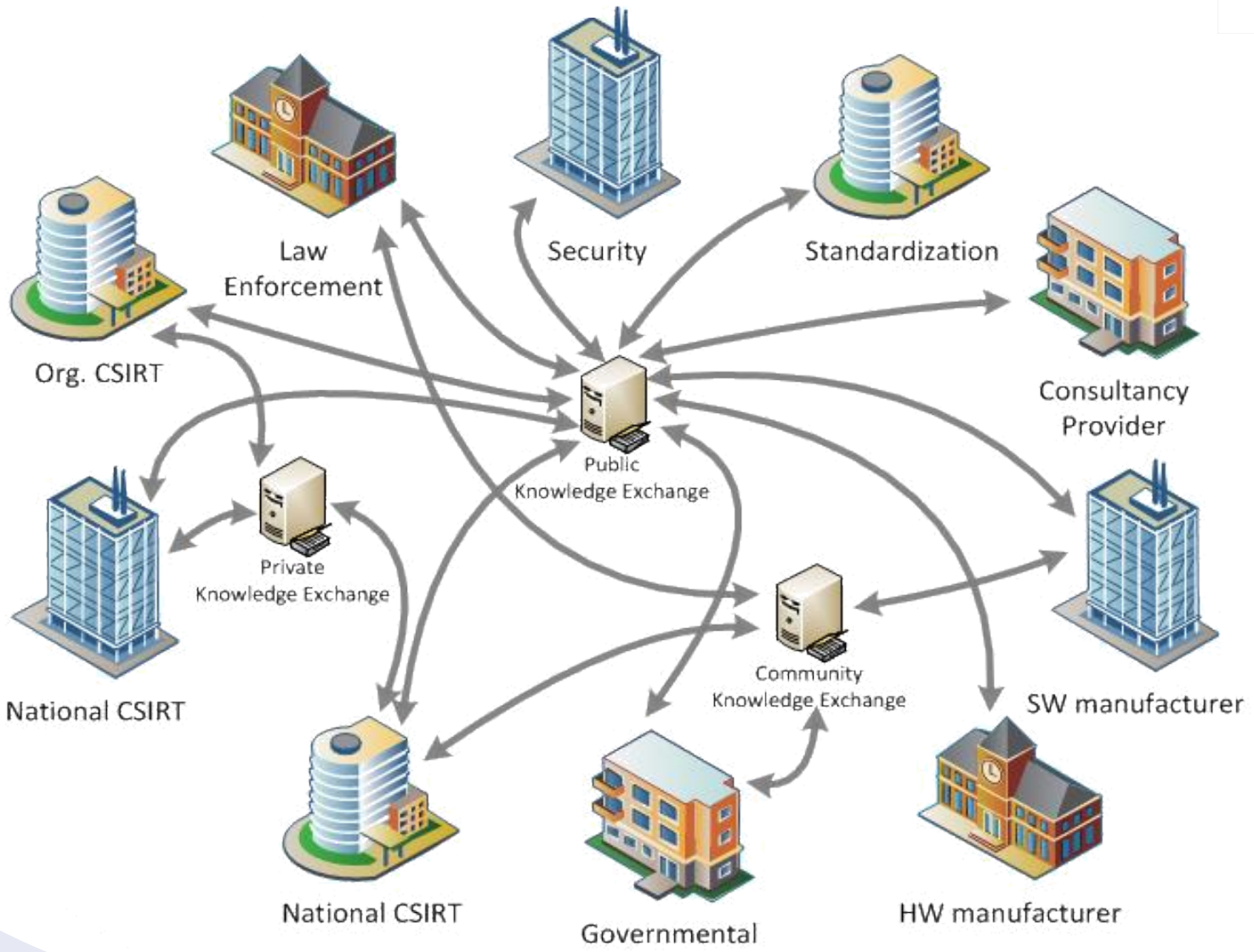
- Anonymisation
  - Attribute sanitation

- Management of uncertainty
  - Attribution, attacker motivation, etc
  - Multiversioned DBs

Conclusion

- There is a need for a knowledge management platform specifically designed to address the information sharing issues of the Cyber Security domain
- NATO is seeking feedback
- CDXI implementation will be considered by NATO Nations in 2015
- Possible collaboration on refining use cases:
  - NCIA: Manisha Parmar (Manisha.Parmar@ncia.nato.int)

Questions


Law Enforcement
Security
Standardization
Org. CSIRT
Consultancy Provider
Public Knowledge Exchange
Private Knowledge Exchange
National CSIRT
Community Knowledge Exchange
SW manufacturer
National CSIRT
Governmental
HW manufacturer

NATO Communications and Information Agency

Cyber Security Information Sharing

Oscar Serrano
NCI Agency
Cyber Security Service Line

DeepSec 2014, Vienna, 21 November 2014

Cyber Security In NATO

- NATO in a nutshell:
  - Collective defence
  - Interoperable capabilities
  - Policies for sharing information
  - NATO has its own systems to protect
  - NATO relies on National systems for its missions and operations
- NATO's 2010 Strategic concept
  - Cyber security is a key concern
- NATO Computer Incident Response Capability (NCIRC)
  - Coordination Centre (CC)
  - Technical Centre (TC)
- Annual Cyber Coalition Exercise
- Many ongoing initiatives on cyber security information sharing

Cyber Security Data Overload

we are overloaded with data.

governments that need to coordinate on cyber defense information

industry sectors working to protect themselves from cyber criminal threats

We have law enforcement following criminal networks

And we have large military organizations that must maintain a strong cyber defense posture.

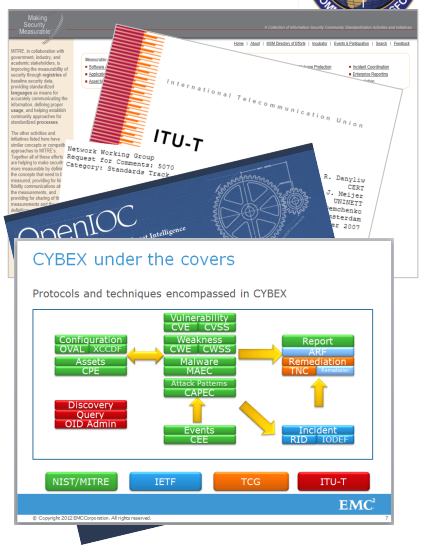
while we gather so much data, we still wonder what we are missing, and we find we want more. The irony is that there is too much data but there is not enough data at the same time.

Drivers for Information Sharing

- Strategic drivers
  - CCDCOE's National Cyber Security Strategy Manual
  - NATO's new Cyber Defence Policy
  - U.S. Executive Order on Improving Critical Infrastructure Cybersecurity
  - UK's Cyber Security Information Sharing Partnership
- Operational drivers
  - Common systems, threats and vulnerabilities
  - Trusted communities
  - Too few qualified personnel
- Enablers
  - Standardization efforts
  - Commercial and open source software

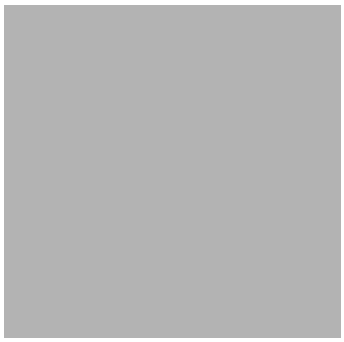
Standardization Efforts

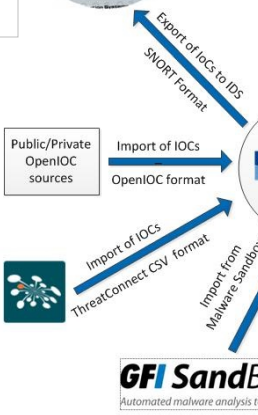
- Standards:
  - US Govt / MITRE's “Making Security Measurable” program
  - ITU-T’s X.1500 CYBEX
  - IETF’s Incident Object Description and Exchange Format (IODEF) and Real-time Inter-network Defence (RID)
  - Vendor Formats
    - Proprietary or Open source
- Most are interoperable!



Existing Capabilities

- Platforms / Systems / Services / Organizations:
  - FS-ISAC Avalanche / Soltra Edge
  - Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA)
  - Microsoft's Interflow
  - Collective Intelligence Framework (CIF)
  - ITU's IMPACT
  - NATO's Malware Information Sharing Platform (MISP)
- Many efforts in other domains (e.g. bioinformatics)





Challenges !

- Policy and legal issues
- Many data sources available
- Timeliness requirement competes with quality requirement
- Multi-lateral, differentiated sharing is a requirement
- Sensitive data requires dissemination controls
- Current processes and technologies do not support well burden-sharing collaboration and outsourcing
- Managing uncertainly
- No direct financial benefit

Ongoing efforts must be continued,
but they must also be complemented !

Addressing the Challenges…

- Previous efforts have looked the formats for expressing the information to be exchanged and the transport mechanism…
- In cyber security, there are many challenges in the management and exploitation of exchanged data…
- In cyber security, these challenges are mostly common to all…

Shouldn't we aim for a common platform?

Manage, Share, Automate

- Collaboration is key
- Timely, high-quality information is critical
- Well-defined exchange policies
- Wide-scale sharing

02/12/14 NATO UNCLASSIFIED

Organizations have identified the partners with whom they want to share

Need internally and external information to have the full picture.

collaboration usually plays out with time consuming, manual processes, using ad hoc exchange mechanisms – for example, phone calls or emails within small groups.

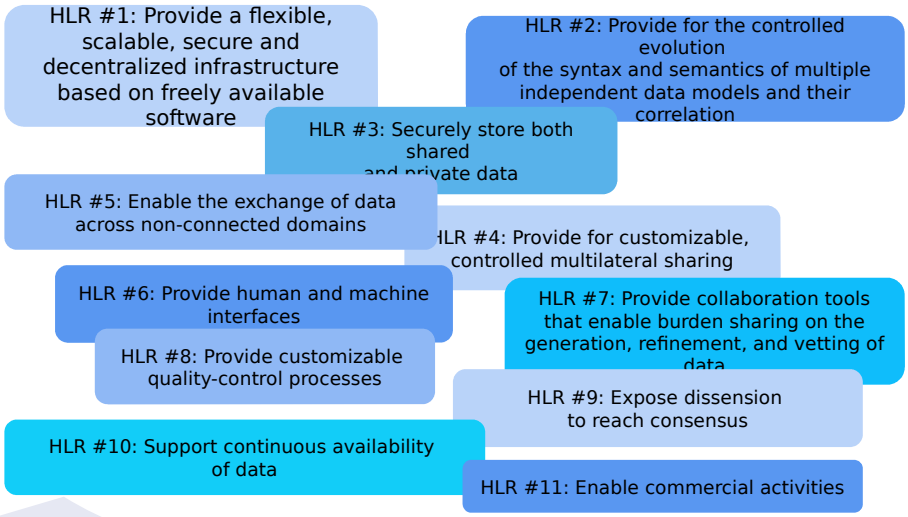
We can see, that more fluent information sharing is a major requirement and research area for the cyber security community.

To examine proposed solutions to these problems, we have considered what people

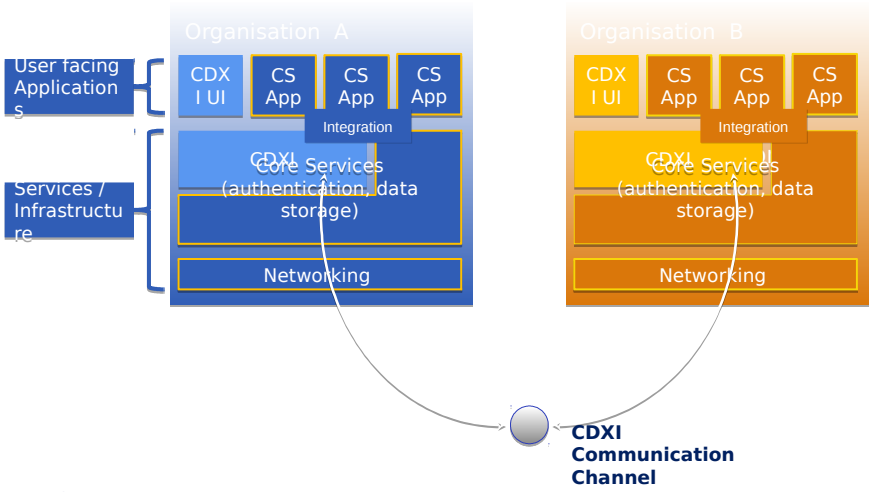
CDXI Capability Definition Document

- Identifies 11 High-Level Requirements
  - Both necessary and sufficient
- Is publically available on request

High-Level Requirements (HLRs)



Deployment and integration



Information Exchange Policies

- Created at any organizational level
- For a data set or individual item
- Approved by legal departments
- Machine-readable encoding

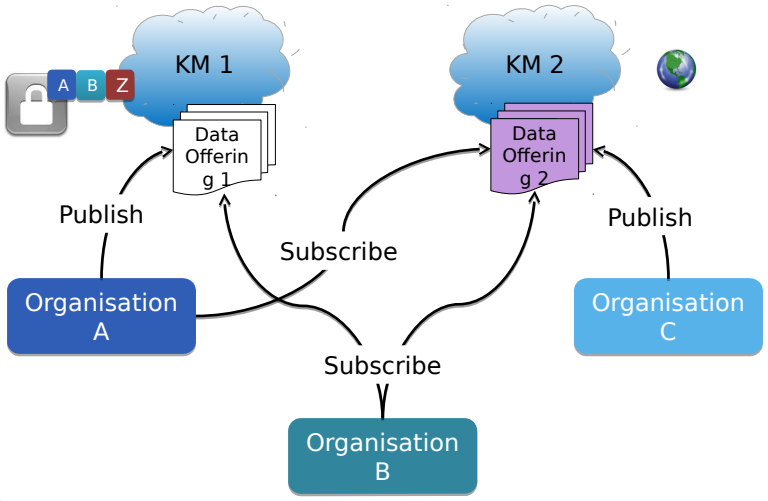
NATO UNCLASSIFIED

Our proposal, then, is to manage and enforce legal and policy requirements and sharing agreements through the use of “Information Exchange Policies (IEPs)”. These would be

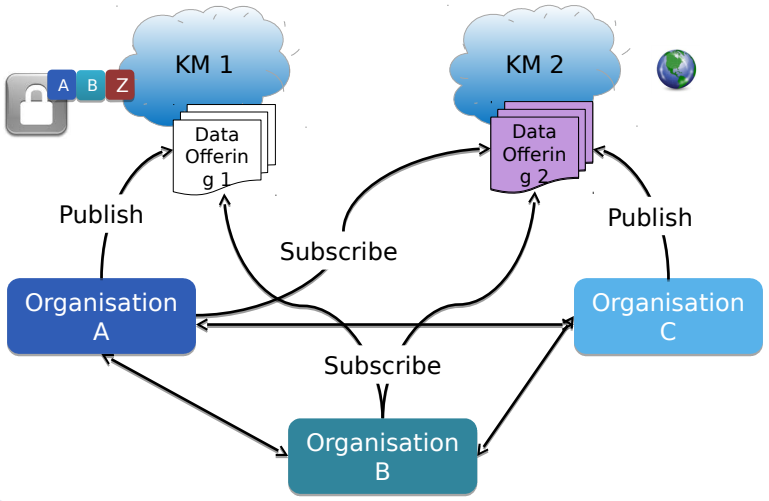
- Created at any organizational level and could specify sharing complete data sets or a specific data item
- Specify things like the scope of an information sharing agreement, the participants and joining rules, handling requirements, whether data can be modified and redistributed, etc.
- Have approval from the legal responsibilities of an organization.
- Encoded in a machine readable format and linked to the data in the cyber sharing system, to enable automated sharing in accordance with legal frameworks and organizational policies for auditing, enforcement, and correlation.

To the best of our knowledge, IEP concepts are not in use by cyber security sharing systems. Most likely, organizations see the complexity of designing and implementing such a solution and may be skeptical about the resulting benefits. We see solving this problem as important for addressing the legal impediment to information sharing.

Knowledge markets



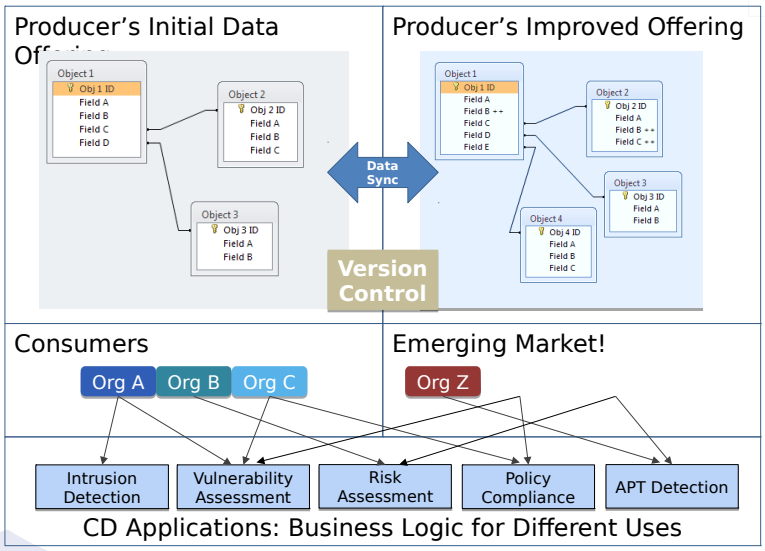
Knowledge markets



Ontologies

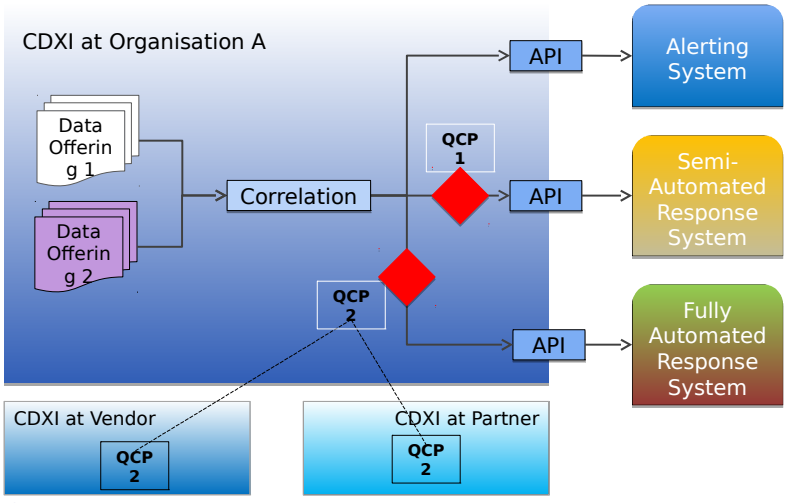
- Multiple, overlapping, evolving ontologies
- Aiming for one ontology is impractical
- Evolving size, scope, and depth of ontologies must be supported

Agile data model



NoSSQL: Hadoop based system

Enabling automation



Other features

Anonymisation

- Attribute sanitation

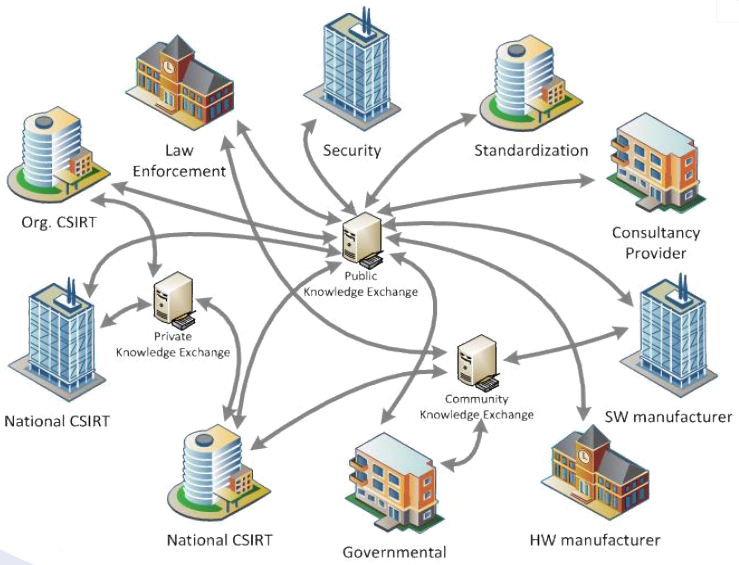
Management of Uncertainty

- Attribution, attacker motivation, etc
- Multiversioned DBs

Conclusion

- There is a need for a knowledge management platform specifically designed to address the information sharing issues of the Cyber Security domain
- NATO is seeking feedback
- CDXI implementation will be considered by NATO Nations in 2015
- Possible collaboration on refining use cases:
  - NCIA: Manisha Parmar (Manisha.Parmar@ncia.nato.int)

Questions


Law Enforcement
Security
Standardization
Org. CSIRT
Consultancy Provider
Public Knowledge Exchange
Private Knowledge Exchange
National CSIRT
Community Knowledge Exchange
SW manufacturer
National CSIRT
Governmental
HW manufacturer