The New Information Security Agenda:

Managing the Emerging Semantic Risks

Dr Robert Garigue

Vice President for information integrity
and Chief Security Executive
Bell Canada

Abstract

Today all modern organizations, and in some cases entire societies, are socio-technical structures. These new computationally-intensive structures are in fact operationalized Semiotic Systems. Semiotics systems are defined in three dimensions : pragmatics, syntax and semantics.

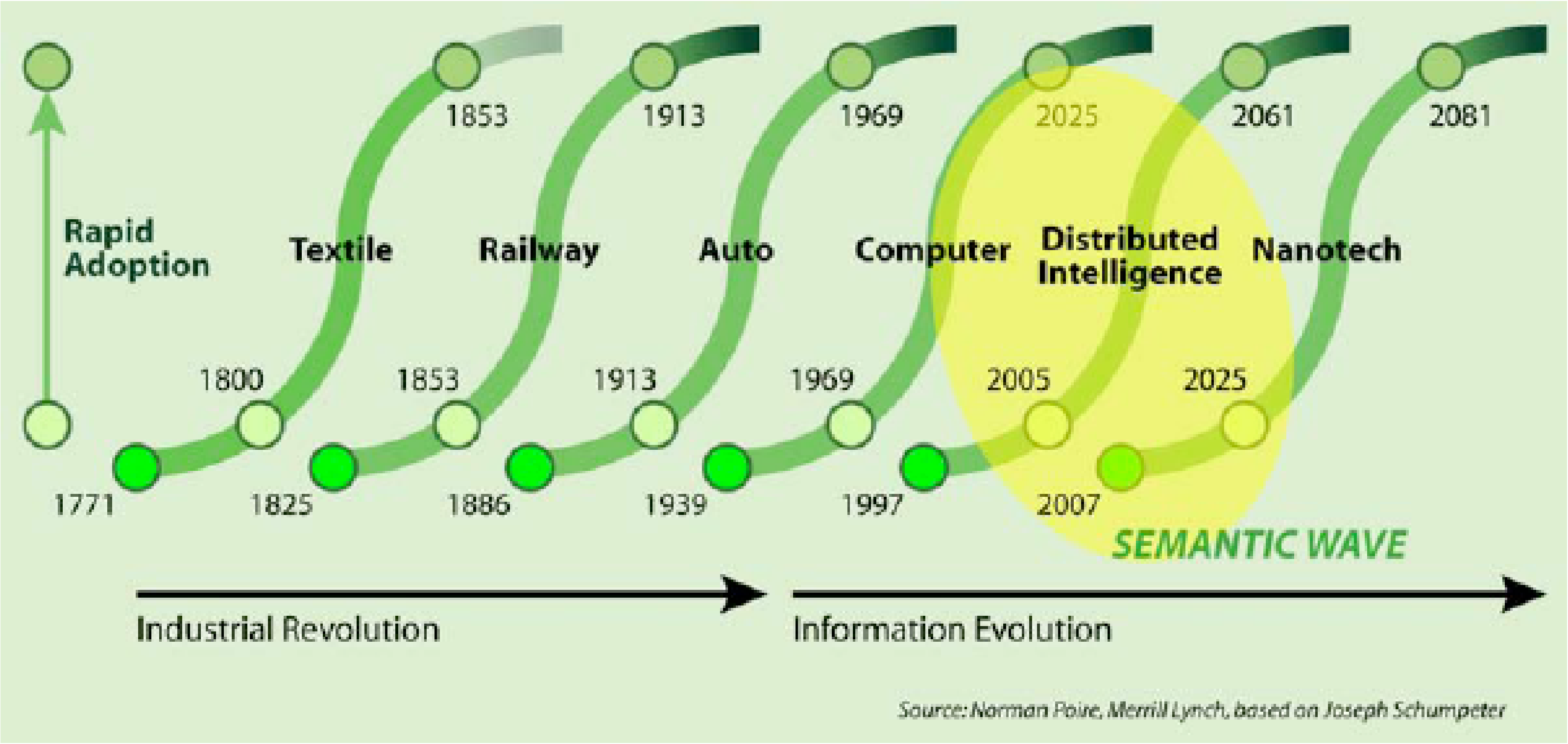
In cyberspace The pragmatics, syntax, and semantics are now very distinct technical layers. Networked wired/wireless devices compose the pragmatic layer. Internet protocols structure a world wide syntax by which all the devices communicate with one another. Finally, the semantics are being derived through the sense making capabilities of advanced search engines and query services. But this is just a start. New semantic technologies are being invented and deployed: semantic capabilities are now positioned to computerize sense-making. Inherent in the use of these new technologies are opportunities and risks.

The emergent risk for societies is how to organizes the sense making capabilities for people, organizations and societies to ensure trustfulness and trustworthiness. The security analysis of this semantic dimension has barely started and yet already there is exploitation and undue control being exercised and recognized.

This brief narrative will position this conceptual framework within the overall security discussions and help identify what new expectancies governance groups such as the information Management, Security, and Operational Risk communities will be called upon to ensure quality, integrity, trustfulness and trustworthiness of our semantically enabled organizations and societies.

The next wave

Long waves of innovation



Source: Norman Poire, Merrill Lynch, based on Joseph Schumpeter

Semiotic Systems

Semiotics is the Formal Doctrine of Signs (CS Peirce):

- Pragmatics (Physical level)
- Syntactic (Protocol level)
- Semantics (Intentional level)

All information is carried by signs of one kind or another

Information Processing and communications in an organization are realized by creating, passing, and utilizing signs.

Ref: Semiotics in Information Systems Engineering by Kechen Liu

Organizations are socio-tech structures

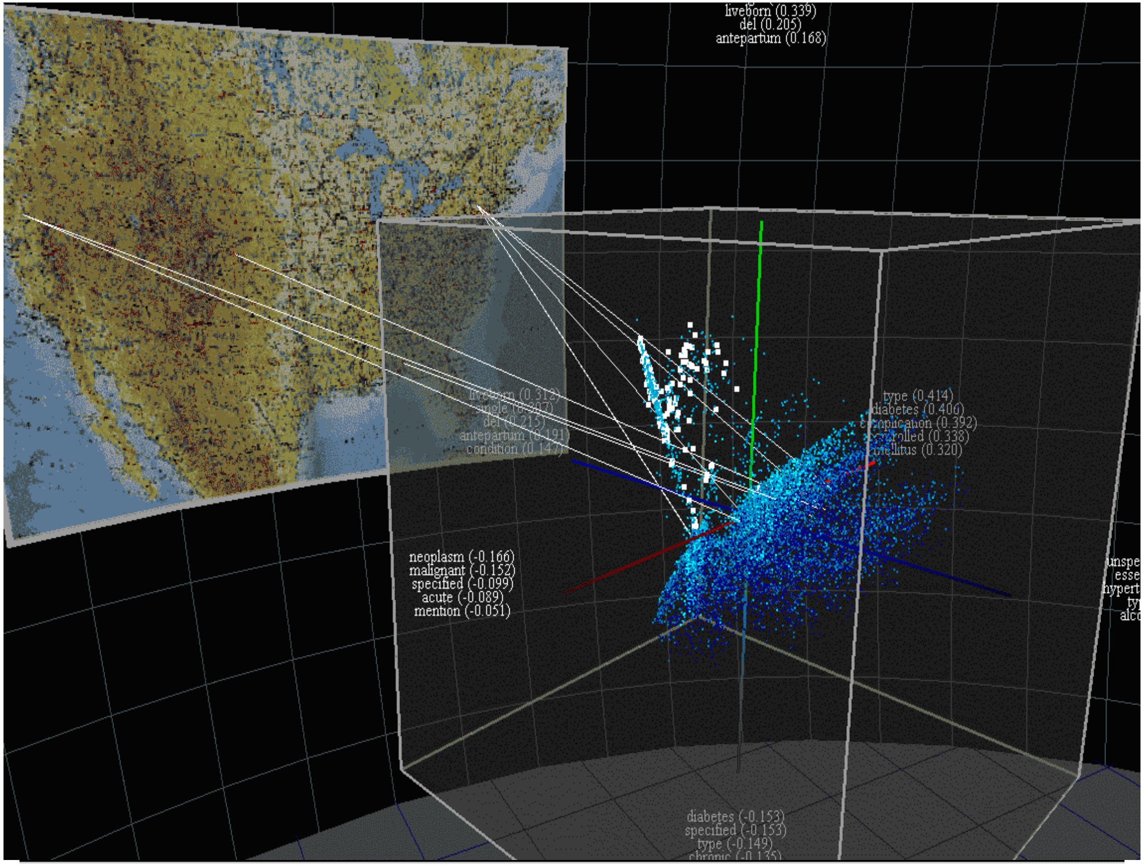
Understanding is computer mediated and Sense making is a computational activity

SEMANTIC systems are composed of actionable informed objects.

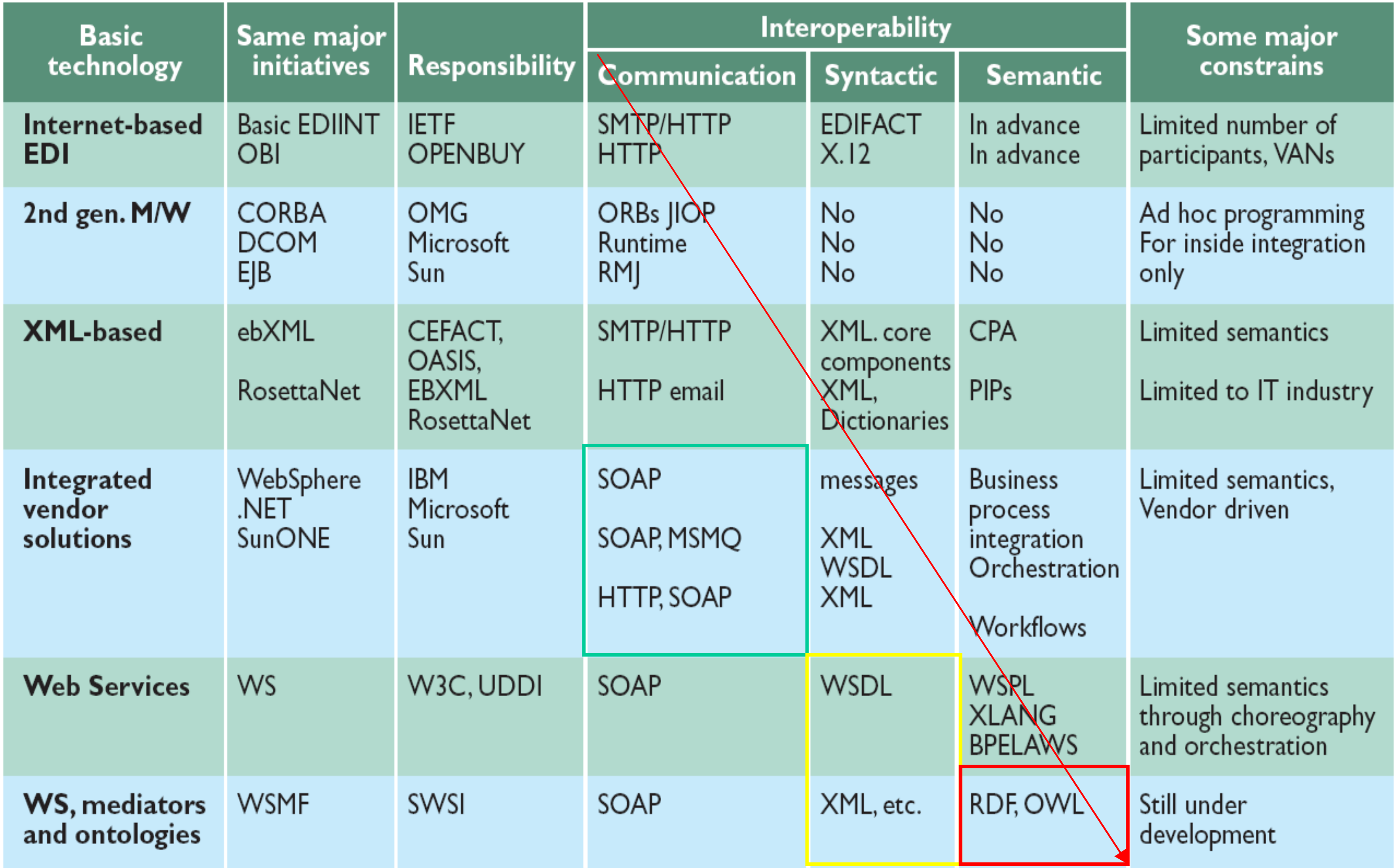
The present structure of the internet

- A <u>pragmatic</u> level composed of the effectors and sensors
- A <u>syntactical</u> level created from within an ecology of processes (requirement for coherence)
- A <u>semantic</u> level from which meaning is derived by applying various context of analysis . Here Beliefs are formed about the world (requirement for correspondence)

The outcome are reasoning systems that are conceptually aligned and interoperable



Present and Future Interoperability Standards: from pragmatics to semantics



Basic technology	Same major initiatives	Responsibility	Interoperability			Some major constrains
			Communication	Syntactic	Semantic	
Internet-based EDI	Basic EDIINT OBI	IETF OPENBUY	SMTP/HTTP HTTP	EDIFACT X.12	In advance In advance	Limited number of participants, VANs
2nd gen. M/W	CORBA DCOM EJB	OMG Microsoft Sun	ORBs JIOP Runtime RMJ	No No No	No No No	Ad hoc programming For inside integration only
XML-based	ebXML RosettaNet	CEFACT, OASIS, EBXML RosettaNet	SMTP/HTTP HTTP email	XML. core components XML, Dictionaries	CPA PIPs	Limited semantics Limited to IT industry
Integrated vendor solutions	WebSphere .NET SunONE	IBM Microsoft Sun	SOAP SOAP, MSMQ HTTP, SOAP	messages XML WSDL XML	Business process integration Orchestration Workflows	Limited semantics, Vendor driven
Web Services	WS	W3C, UDDI	SOAP	WSDL	WSPL XLANG BPELAWS	Limited semantics through choreography and orchestration
WS, mediators and ontologies	WSMF	SWSI	SOAP	XML, etc.	RDF, OWL	Still under development

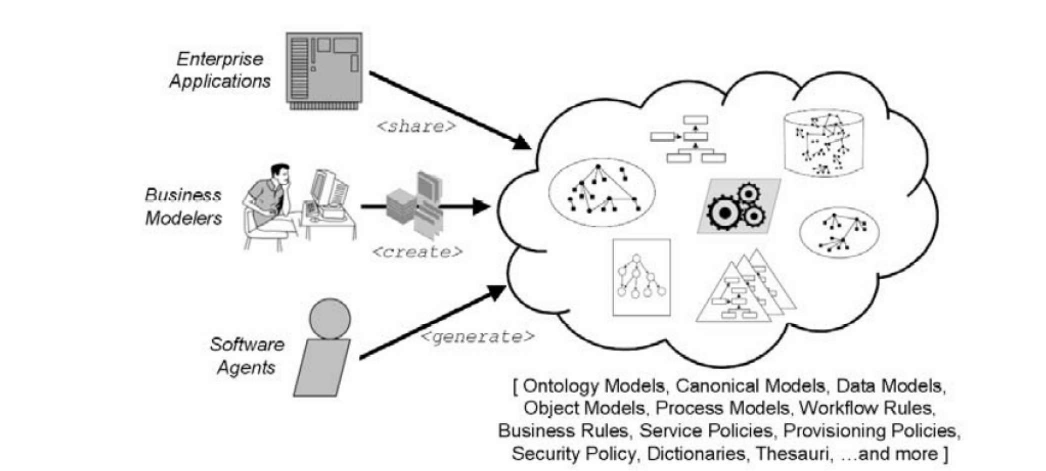
Kajan, Stoimenov *Towards an ontology-driven architectural framework for B2B*, Communication of the ACM Dec 2005 /Vol 48 no 12

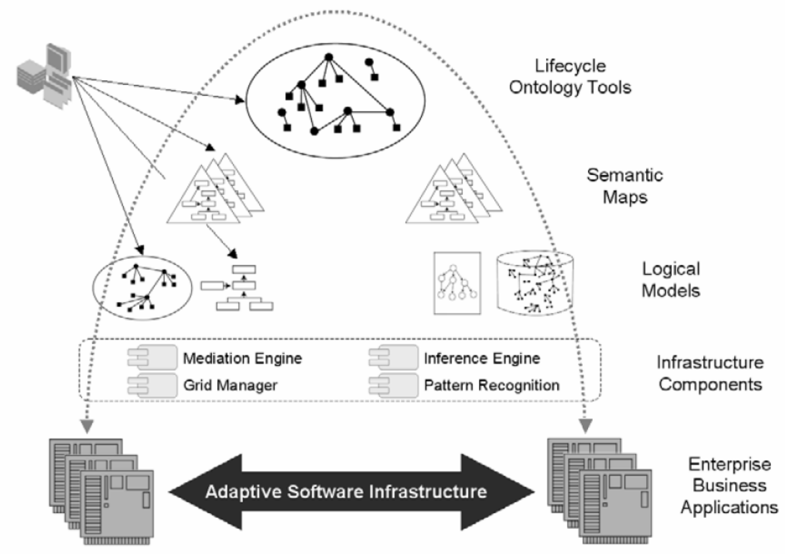
Emergence of ontologies as new types of information assets

Ontologies, common schemas, business models are ultimately the basis for consistency and accuracy:

- Between organizations, misinterpretations in communications are addressed by Ontologies, common schemas, business models help explain and reconcile terminology, jargon, and nomenclature specific to each party

- Between systems, Ontologies, common schemas, business models reconcile metadata standards, XML dialects, and database access mechanisms. Acting as a semantic translator


Enterprise Applications
<share>
Business Modelers
<create>
Software Agents
<generate>
[Ontology Models, Canonical Models, Data Models, Object Models, Process Models, Workflow Rules, Business Rules, Service Policies, Provisioning Policies, Security Policy, Dictionaries, Thesauri, …and more]



Semantically enabled systems need to validate trustworthiness

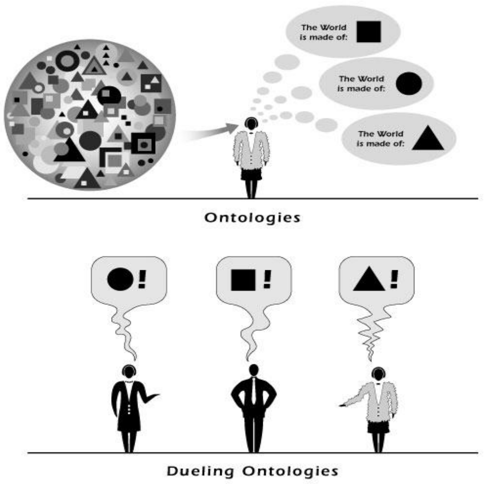
Ontological engineering is used to convert information into ontologies. **Linked ontologies permit very long network of conceptual relationships.**

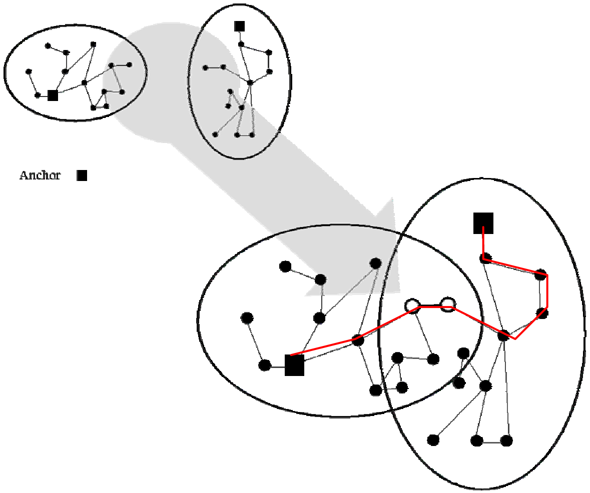
Declarative logic is used to reason across the semantic networks of conceptual relationships. This also mean inference across bodies of knowledge.

The OWL formal semantics specifies how to derive its logical consequences, i.e. facts not literally present in the ontology, but entailed by the semantics.

These entailments may be based on a single document or multiple distributed documents that have been combined using defined OWL mechanisms

New relationships between ontologies enable to explain causal relationships. In this way semantic technologies "help discover" new knowledge.





The Semantic Organization’s Threats Spectrum

Emergent risks

Traditional risks

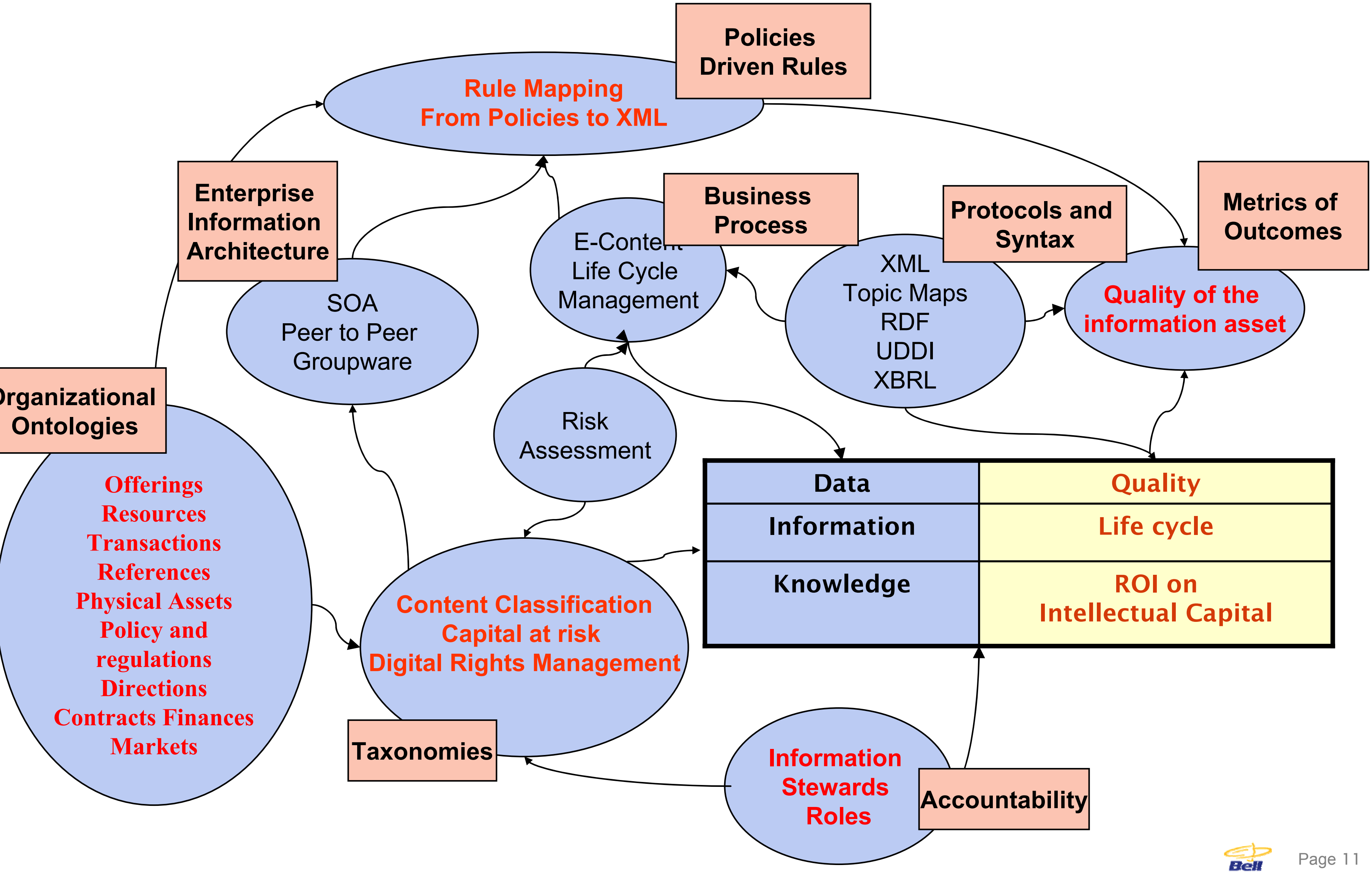
Levels	Target	Objective	Method	Type of Weapon
Semantical	Sense making capability Ontologies Decision Maker	**control of the decision outcome**	Creation, diffusion of self referential, imperative and dogmatic false Propositions UNTRUSWORTHY Content – Reasoning	**Memes and Dramatic Orchestration** **(Today this first generation called phishing attacks)**
Syntactical	Logical Processes	**Modification of a service, degradation of value**	Change in operating parameters UNTRUSWORTHY PROCESSES	**Virus, Trojan, worms** **Malware agencies**
Pragmatic	Physical Infrastructure	**Removal of a capacity for action or perception**	Denial of Service	**Hard steel and explosives**

“Truthfulness and Trustworthiness” are security requirements in semantic systems

“Truthfulness and Trustworthiness” is now played out at a higher level of abstraction: the semantic layer of the internet.

- The capability for creating, transmitting and validating facts are being embedded in the content.
- Sense-Making becomes an individual and organizational strategic survival activity.
- Determining Truthfulness and Trustworthiness rest with those who consume the reasoning.
- Security Tools for evaluation of trustworthiness will be essential.
- These security capabilities do not exist

The new security space in semantic organizations: New roles and new controls



Data	Quality
Information	Life cycle
Knowledge	ROI on Intellectual Capital

It is all about "Values" that are executed by systems

What "values" you specify and build into the systems will be your legacy for the next generation.

For example what are the ontologies associated with privacy to ensure that the machine reasoning associated with privacy are executed correctly.

Without those values embedded in the systems might not be considered trustworthy and will not generate truthfulness….

We need to start research on what are trustworthy ontologies, to ensure that semantic systems reason with the proper "concepts".

And now lets build our collective future….