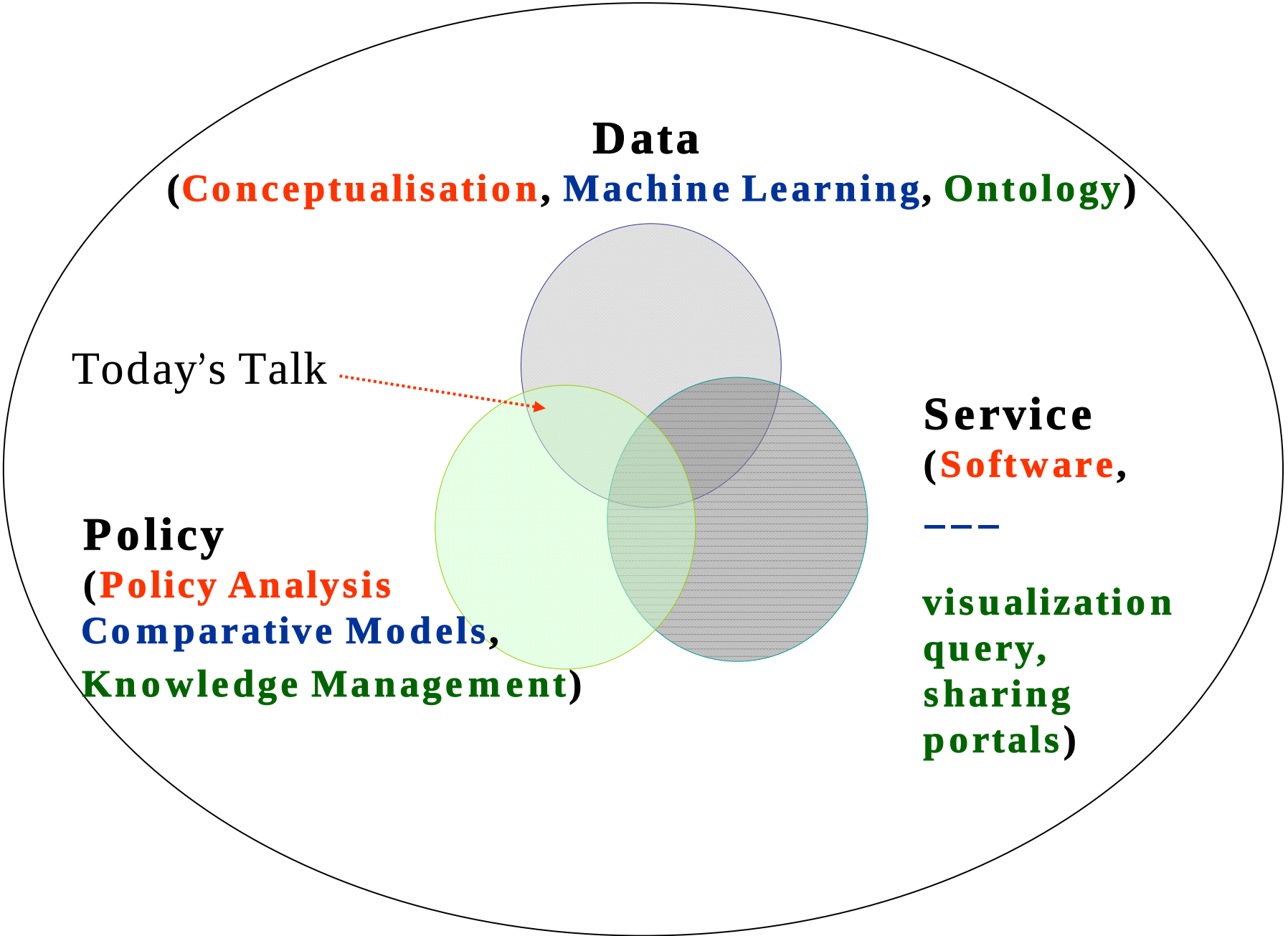
‘Establishing the Baseline’

A Framework For Organizing National Cyber Strategies

Aadya Shukla
Aadya_shukla@hks.harvard.edu

Science, Technology & Public Policy Fellow, Harvard Kennedy School
Affiliate Researcher, Harvard-MIT Minerva Project, MIT
Teaching Fellow, Science, Engineering & Applied Sciences, Harvard University
Microsoft Research Fellow, Department of Computer Science, University of Oxford.

Research (Objective, Approach, Output)



A Baseline: Why?

- **Cyber Policy making needs Interoperation**

  Interoperation and collaboration does not happen at the cost of national interests.

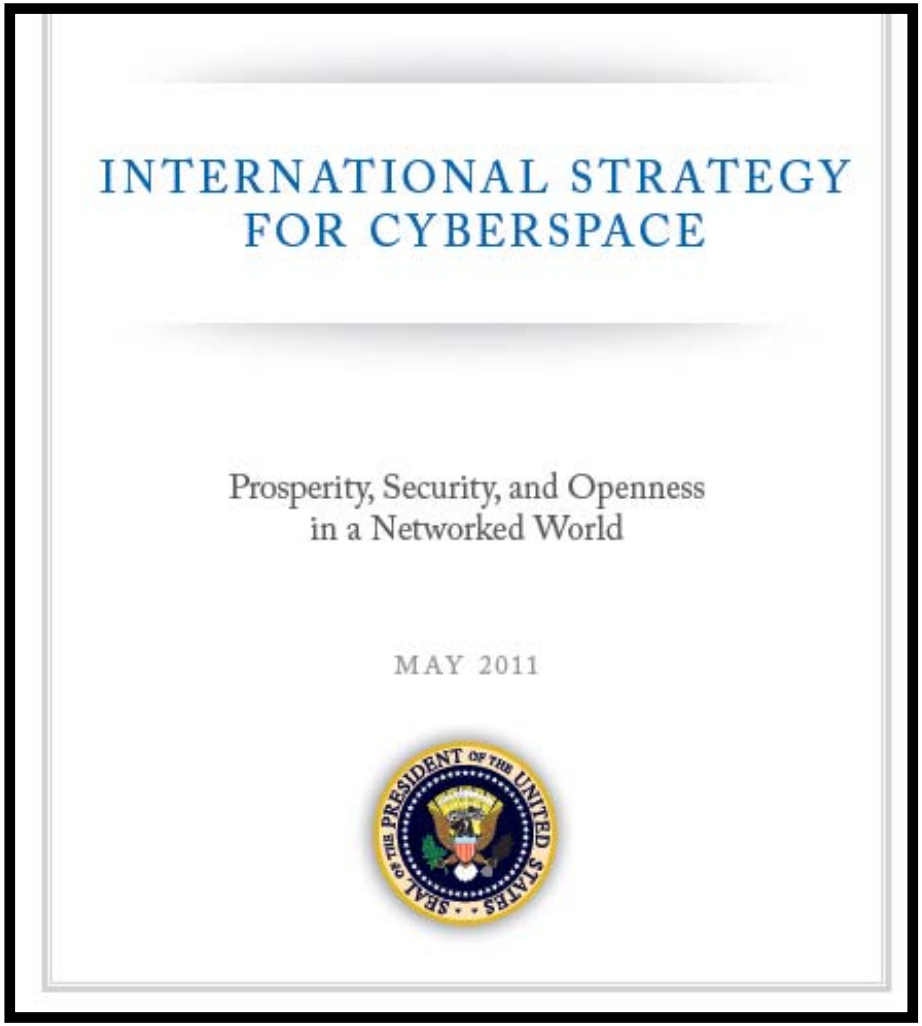
Handshaking **precedes** collaboration.

A clear characterization and communication of stakeholders' concerns across both domestic and international boundaries is a must.

Is that right?

A Baseline: Why?

24th of May, 2011


INTERNATIONAL STRATEGY FOR CYBERSPACE

Prosperity, Security, and Openness in a Networked World

MAY 2011

- Cybersecurity is not an end unto itself; it is an obligation which our governments must take on willingly.
- By Itself internet will not usher in international era of cooperation, That work is up to us to move towards cyberspace which is open and **interoperable**
- United States Cyber Strategy provides the **context for our partners at home and abroad to understand our priorities and how we can come together** to preserve the character of Cyberspace and reduce the threat we face

What about understanding Others?

1. The OECD issued *Guidelines for the Security of Information Systems* (2004).

2. The UN issues resolution (55/63) on combating criminal misuse of Information Technologies (2000 / 2005 amendment).

3. Council of Europe Draft on Cybersecurity (1999)

4. ENISA (European Network and Information Security Agency) Guidelines on Incident Management (2010)

5. Comprehensive Guidelines to combat cyber challenge from Organization of American States (OAS), 2004.

6. UK Government Cybersecurity Guidelines (2009), Revised Cyber Doctrine for the UK is released on 29th of June,2011.

Scaling & Compliance Concern

05/20/2011

UN Agencies Collaborate to Tackle Cybersecurity

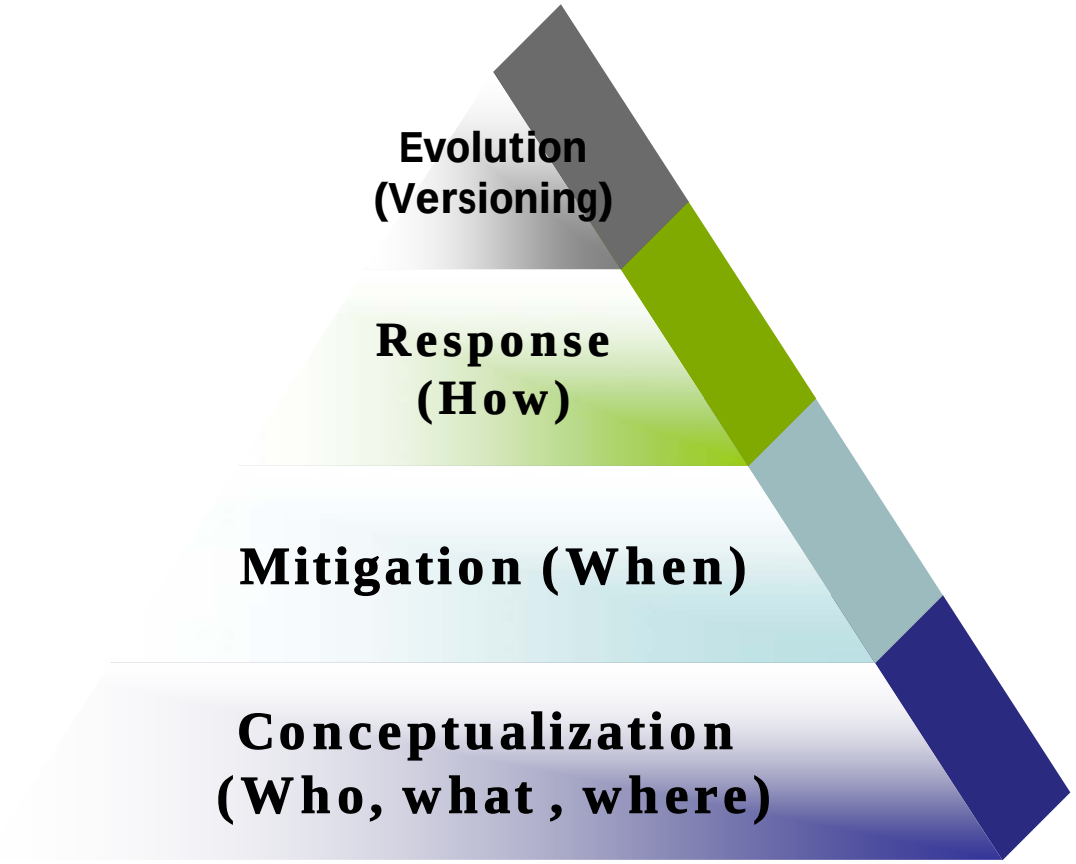
ITU-IMPACT Coalition to expand to 130 countries

Problem for Policy Makers

An Integrated framework to characterize strategies embodied in various national and international initiatives is missing from the policy domain.

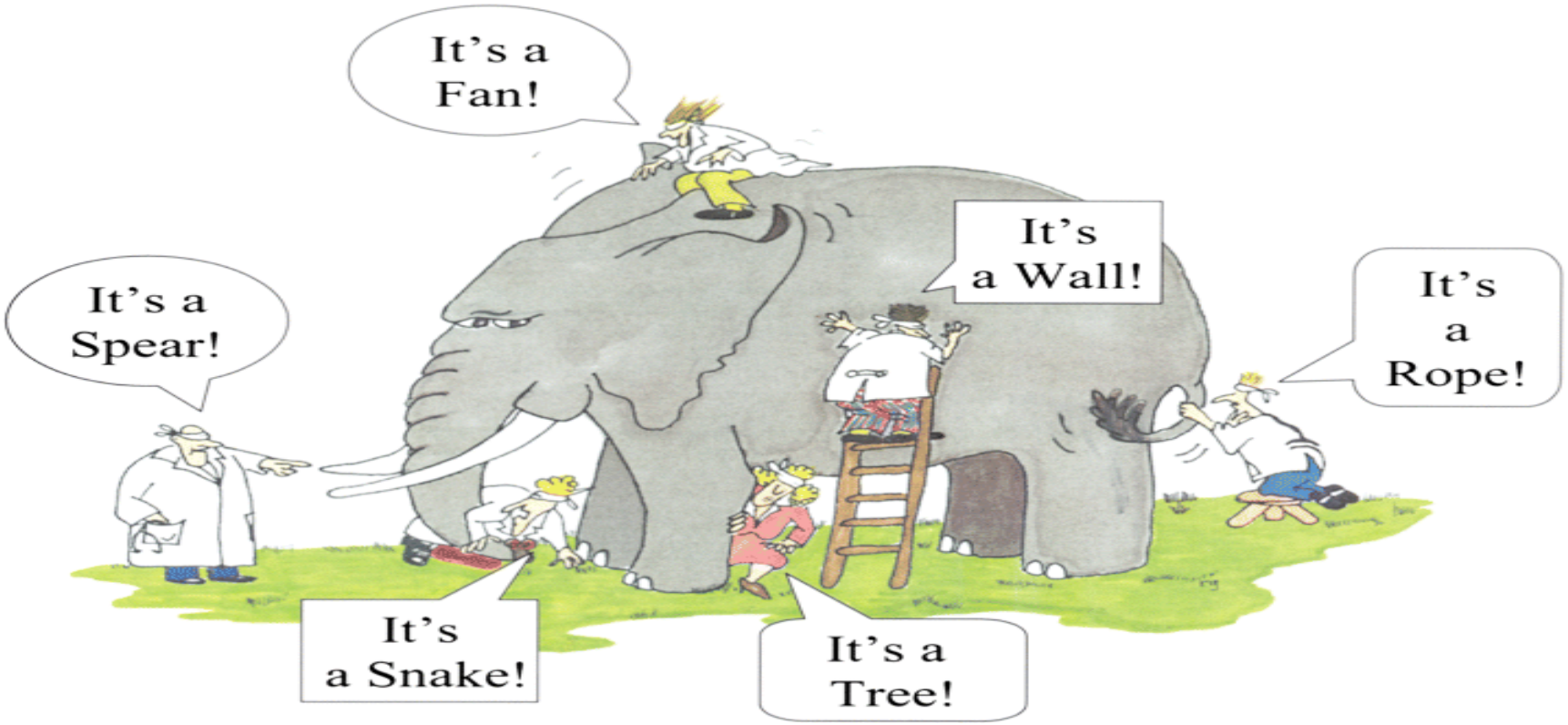
Cyber Strategies need to be systematically understood across four dimensions:

Analysis Dimensions



Policy Questions (Conceptualisation)

Cyberspace: Elephant from the ***Panchatantra** tales*



Mahauts (Policy-makers) need to reign-in (**make rules**) the Elephant (**ever growing cyber incidences)** but there is **no agreement** on the size, temper and how to track the movements of the Elephant in the jungle (**cyberspace**). They are blindfolded therefore, have **partial vision and localized understanding** of the problem.

****Panchatantra – An ancient collection of Indian allegoric tales by author Vishnu Sharma (Image: Google Image Database)**

(Craig Shank / Q-n-A)

- Who are the actors, Roles, What Kind of Models, what kind of priorities, what kind of actions and how? (in the policy space.

- This needs to be understood at higher enough level for policy makers to be well conversant first, before getting deeper into these topics.

Policy Questions (& Dimension)

1. What are specific and generic concerns of the stakeholders in cyberspace? (M & R)

2. How do nation states balance their domestic priorities against need to comply with international guidelines? (M&R)

3. How successful a particular initiative is against a specific type of cyber concern? (R)

4. How does a national strategy scale up with change in cyber priorities with time? (E)

5. What can be learned from other national initiatives? (C/M/R/E)

Policy Questions (Q-n-A)

6. Architecture discussion does not take into account Geopolitical Realities (R)

7. Dealing with unintended aspects of technology (E)

8. Trade-off between Privacy & Security (C)

9. Traditional threat gateways no longer most scary – Hardware (Embedded threat) (R / C)

10. Divorce between Market realities and Technology infrastructure (R / C)

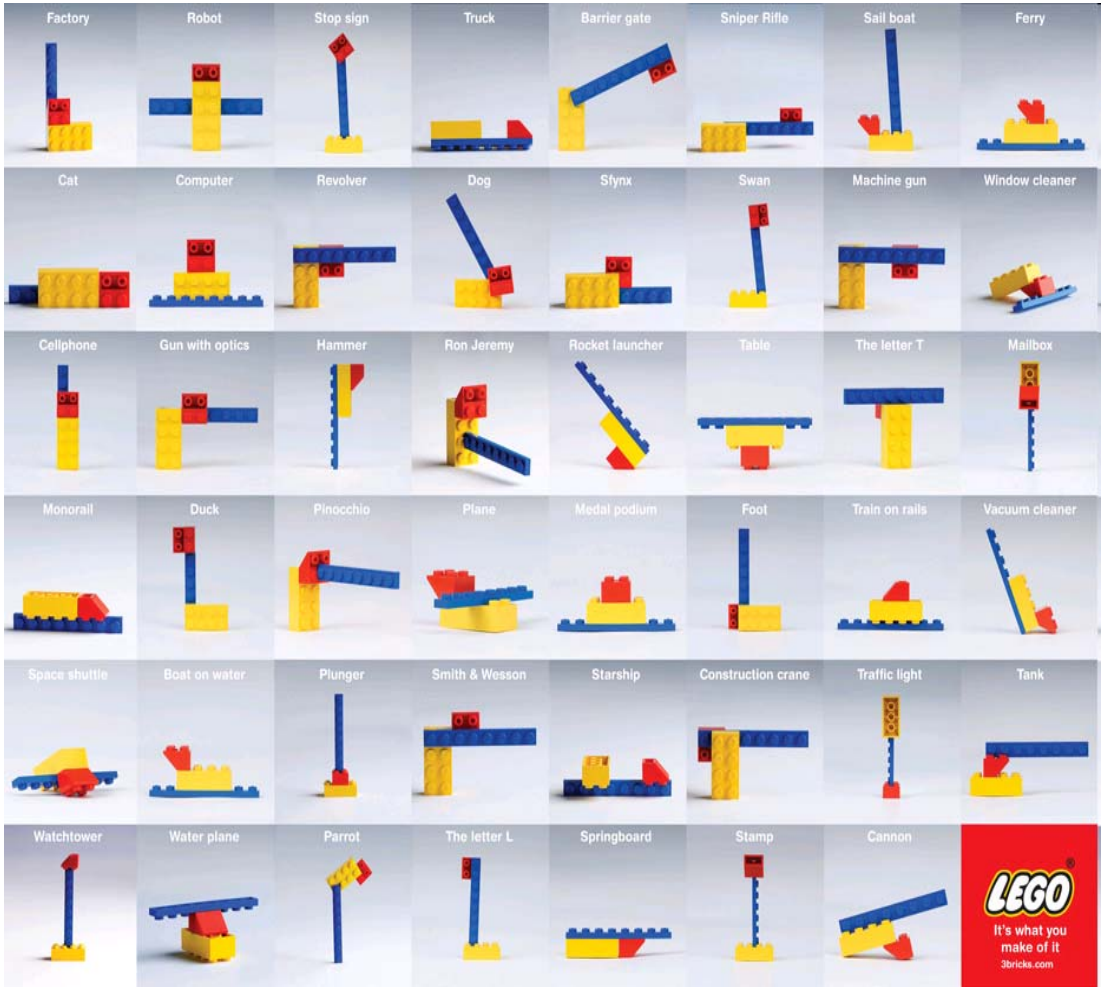
Policy Questions (Q-n-A)

11. What is driving the policy – Politics or Technology? (C/E)
12. Government control of virtual spaces? (R)
13. Liberty versus Security? (C / E)
14. Transparency versus confidentiality? (C / E)
15. Private ownership of public commons? (R)
16. How do you translate polices into actual responses (Dimitri)? (E / R)
17. How do you measure impact of Policies on Business Models? (R/E)
18. Who makes the decisions (actors & their roles) with respect to questions like e-money, air-time, versus simple transaction) (R)
19. How can you best organize response to various concerns? (M / C)

Policy Questions (Q-n-A)

20. How can you become trusted advisor to your customers?
21. How are you performing at the level of local versus national, cross-domain and cross national boundaries
22. Four areas: Freedom, IP, Cybersecurity, Crime
23. Governments are generators of artefacts, how do you manage the relationship between government owned artefacts and non government owned artefacts?
24. Who makes the decisions (actors) with respect to questions like (e-money or simple transaction).
25. What steps should be taken to implement policies?
26. Lost mile, Rise of communication, Rise of search, rise of businesses.
27. Cultural changes which are changing the behaviour of users?
28. Requirement to overlay policy guidelines on physical infrastructure.
29. With exponential growth in technology there is no way you can keep the policy static, what kind of tools and models will assist dynamic policy management?

Solution (Lego Approach)
Have A Strategy to Decipher/Build Strategies



- Common Bricks.
- Connectors.
- Multiple Flexible models.
- You can choose to use a particular colour of brick to represent a particular kind of concept.
- You can derive your own compound shapes by joining existing bricks and use a compound shape as a base shape.

Image Source: Google Image Database

How (Model Driven Framework)

- Build a light weight Metamodel as an integrated framework for cyber strategies to establish the baseline:

- Metamodel will allow to combine separate models based on:

  - Compliance level (Standard, Guideline, Regulation)

  - Types of cyber strategies (Crime, Critical Infrastructure, Military, Civil Society, E-commerce)

What is a Metamodel

- **Metamodel** Model of constructs and their relationships which are used to build models

- **Modeling** Higher level abstraction to combine the observed or expected behavior of a real world phenomenon constrained by different contexts.

- **Metamodeling** Higher level abstraction of constructs which will facilitate the modeling process itself.

Difference between Model and Metamodel levels

If the task were to characterize the phenomenon of *Malware*, then we can use meta level constructs (*Class, Associations and Constraints*), to have a model of models for all malware types.

Example

MODEL LEVEL (M0)

CLASS: Worm

ATTRIBUTE:
activity: binary (malware = 0)
description: string
first-reported: date
affects: enumerated-types

OPERATION:
violation_signature: function

instance_of ***instance_of***

STUXNET **STAR**

METAMODEL LEVEL (M1)

1. Class = Concept Malware

2. Property = {Template to capture attributes of a class}

Description of the concept by defining its attributes.

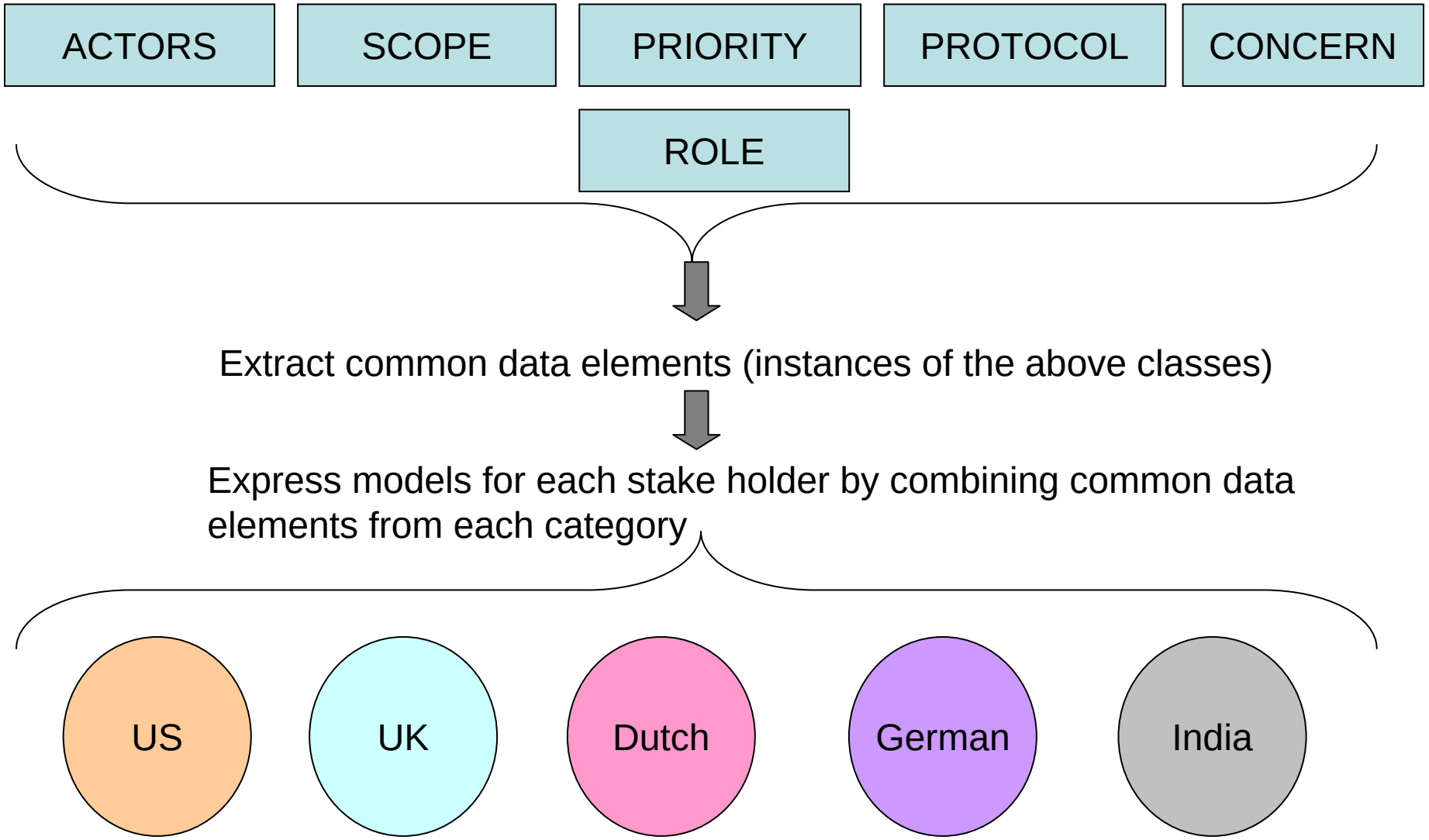
3. Relationship How do concepts relates to real world objects?

Data Level

Framework Component (CLASS)

- **‘Actor’ C**ategories of stakeholders.
- **‘Scope’** class defines boundaries of relevance: Geographical (national, regional, international); Application (Crime, Security, Commerce, Society); Technical (hardware, software, network).
- **‘Priority’** defines weights of cyber concerns in a cyber strategy.
- **Protocol** defines processes, documents and nodes (human & machine) required to deploy a given cyber strategy.
- **Concern** defines types of cyber concerns (different concerns are modeled as sub-classes).
- **Role** What roles do these actors play?

High Level Framework Architecture



Metamodel Component (Association Relationships)

Two types of relationship

- **is-a** : defines relationships between class instances in different contexts (roles)

  Is-a (**ENISA, (Owner, document number ####').**

- **part-of**: defines the subsumption of instances

  part-of (policy, policy-clause)

  (both arguments of the relationship function belong to the same class (here the class is Protocol)

Metamodel Component (Constraints)

Constraints: Rules defined to check the validity of relationships between objects OR to imposes assertions on elements of our model

Constraint is defined using four components:

- A context that defines the limited situation in which a relationship is valid (can be a document, text, or another model, or a class)
- A property that represents some characteristics of the context (e.g., if the context is a class, a property might be an attribute)
- an operation (e.g., arithmetic, set-oriented) that manipulates or qualifies a property,
- Conditional: IF, THEN, ELSE, AND, OR, NOT, IMPLIES

A Simple day-to-day Example

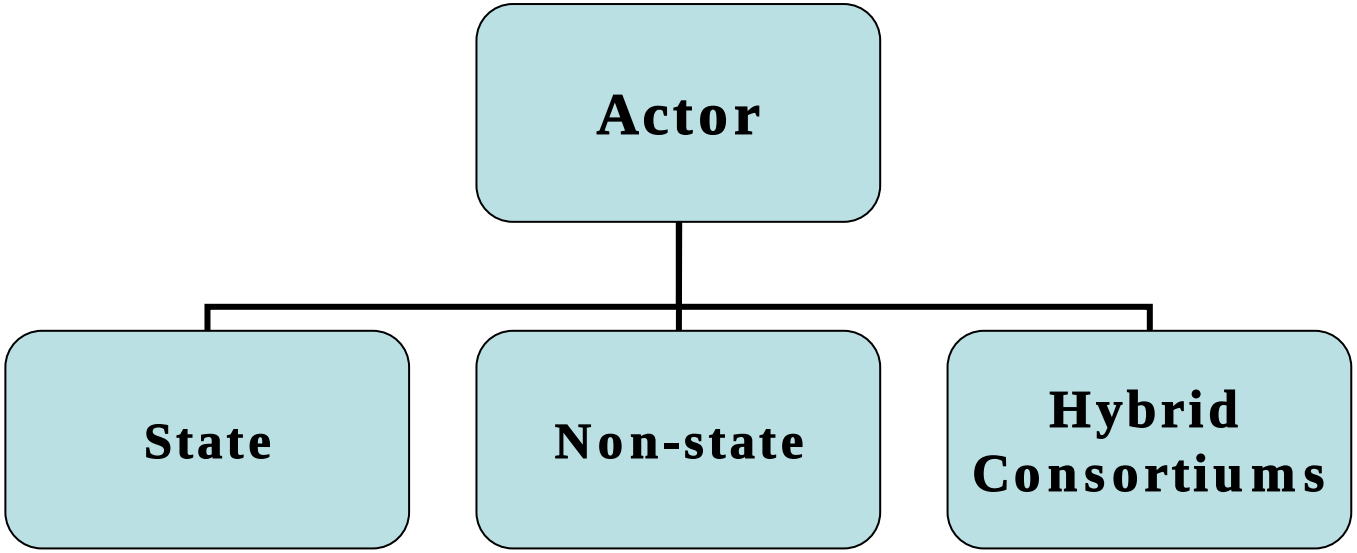
A match can only involve players who are accepted in the tournament

```
context Match
inv: players->forAll(p|
p.tournaments->exists(t|
t.matches->includes(self)))
```

We can easily model the following constraints in the context of cyberspace using this notation.

- A treaty can only involve clauses which are authorised by a legislation / MOU ELSE the treaty is invalid.
- For a threat to be qualified as a DDOS attack to be identified certain human and network components have to be present.
- An attack can be attributed to a country only if there is evidence for state-funding or authorisation
- Policy ‘X’ is to be executed when PRE-CONDTION SET ‘Y’ is true.
- A violation has happened only if some pre and post conditions were not executed in a given order.

Class :: Actor



Actor have attributes:

Origin, Affiliation, Life-span (legacy / current), Orientation (hostile / non-hostile), Authorised_by .

Case Study: Netherlands (Summary)

National cyber security strategy of the Netherlands was released in January, 2011. The strategy emphasizes the following points:

- Connect and Strengthen existing initiatives.
- Invest in Public-Private collaborations.
- Personal responsibility (referring to end-users protecting their own systems).
- Division of Responsibilities of the various Departments.
- Active international collaboration.
- All actions to be undertaken are proportional.
- Self-regulation if possible, legislate if not.

An application of the meta modelling has led to a better understanding of this initiative:

Actors

Four main actors : (NCSC, NCSCEN, GOVCERT,OTC)

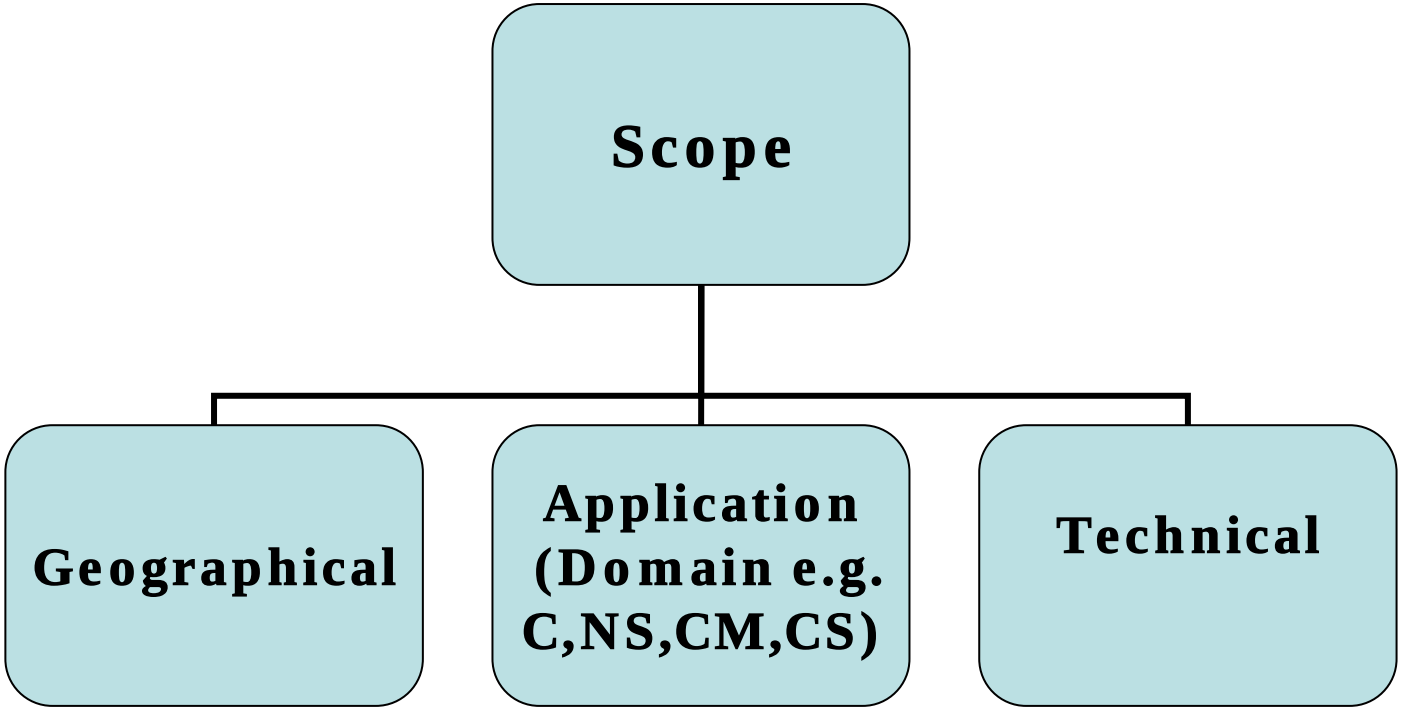
- Analysis of the document reveals that the Dutch cabinet has established that caring for Cyber Security is now a burden for a multitude of organizations and departments, but the effort has to be monitored in a centralised-decentralised manner. Therefore, they wish to unify all these efforts under these bodies:

1. The National Cyber Security Council
2. National Cyber Security Center
3. Dutch government computer emergency response team
4. CPNI (Informatieknooppunt Cybercrime Agency)
5. Cyber Education & Training center (OTC)

Analysis: Need for Compound Actor in the future

- The Security Council is the new organization where the strategy will be monitored, maintained and established by representatives of all involved parties. The Cyber Security Center will essentially be its executing branch, and act as a place where information, knowledge and expertise is shared amongst the participants. The CPNI is an old initiative and how it is going to be merged with the new initiatives is not clear from the strategy. This list of actors is likely to increase as the cyber strategy document indicates the intention on the part of the Dutch government to build stronger public-private partnerships.

Class :: Scope



Sub-Class Properties:

Technical sub-class attributes are defined as Resilience, Response and Management which can assume values of three enumerated types (Hardware, Software or Network).

Class: Scope / Subclass: Technical

Resilience (H): A Responder Kit (accompanied by a manual) has been created for Cyber Espionage so that companies can increase their own resilience.

Response (N): At the end of 2011, 80% of the departments, agencies and companies in the vital sector Public Order & Security (Openbare Orde en Veiligheid) as well as Public Management (Openbaar Bestuur) should have access to a continuityplan that includes large scale internet connectivity breakdown scenarios.

Management:

- ***Centralization(S)***: Establishing one security framework of Information Security for all government agencies as well as creating a government-wide control cycle to enforce it.

- ***Privacy management (H)***: Somewhere in 2011 the cabinet will decide if it is possible to include an electronic ID in travel documents that holds up to the highest security standards, so that Dutch citizens can reliably ID themselves over the Internet and digitally sign documents while safeguarding the citizens´ privacy.

- ***Data-sharing (N)***: The government proposes to implement the European mandatory reporting of dataleaks in the Telecom sector. They will also draft a proposal for mandatory reporting of all loss, theft or abuse of personal data for all services in the ´Information Society'.

Scope (contd.)

Application Level Policy

Components of the Dutch Strategy which are aimed at Crime (C), National Security (NS), Commerce (CM), Civil Society (CS)

- The policy document states that choices will be made by the cabinet with regards to processing of personal data. European norms will be guiding these choices (CS).

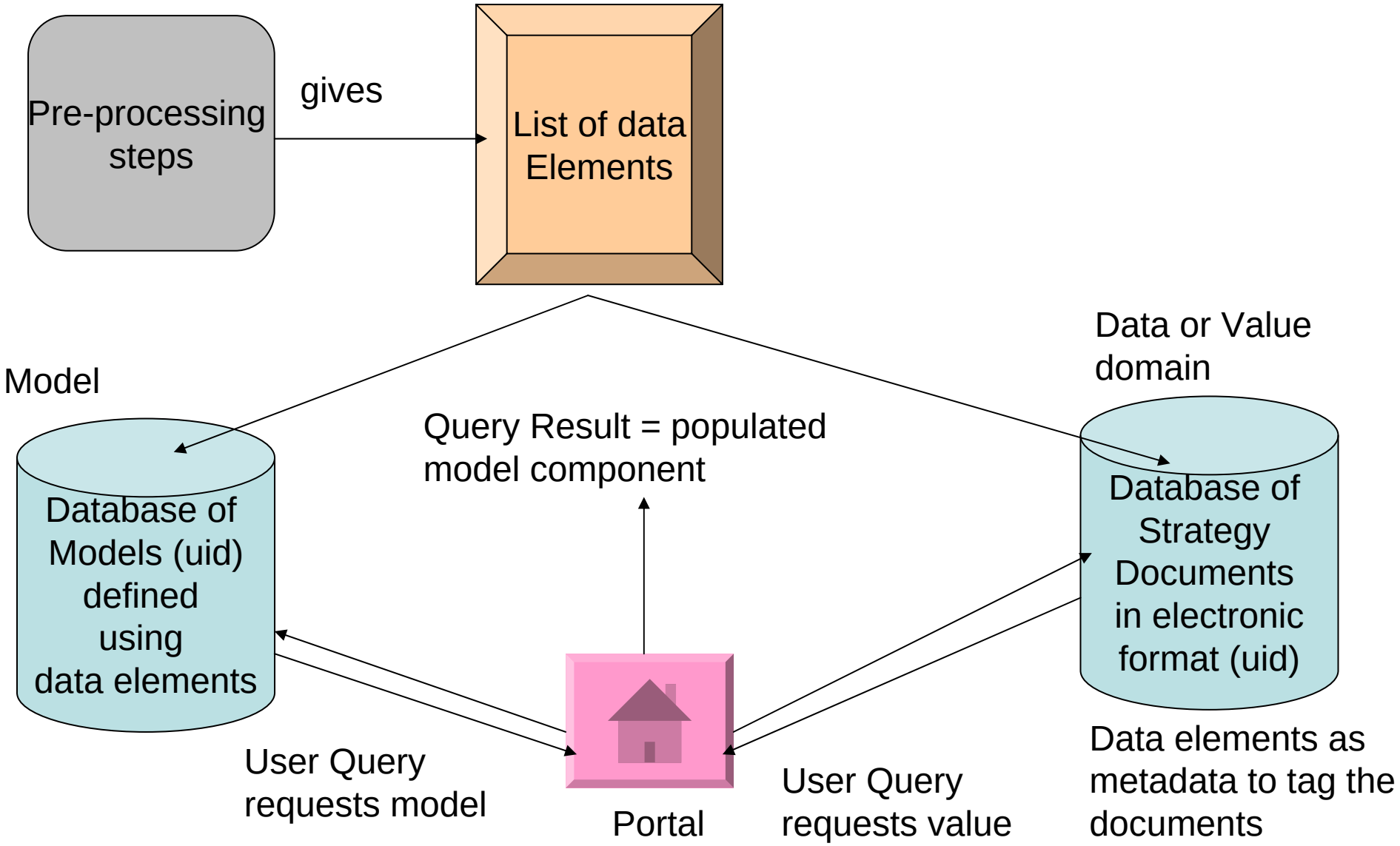
- The cabinet wishes work with IT vendors to look into increasing security in hardware and software and will also look to joining international efforts in this field. The Netherlands will also play an active role in the Internet Governance Forum to increase global internet security (CM).

- In concert with suppliers, the government wishes to better inform its citizen users with regards to security. The result will be national ad campaigns surrounding current events or threats (CS).

Framework Application Matrix

Challenges	Meta Framework Component Analysis
What are specific and generic concerns of the stakeholders in cyberspace?	Actor-Actor Relationships & Actor Class Constraints
Dealing with unintended aspects of technology in the future?	Actor-Scope relationship
How do you measure impact of Policy on business?	Actor-Priority-Scope Relationship
Who is doing what & How?	Actor-Role-Protocol Relationship
Policy update migration issues / Tracking Legacy Decisions	Metamodel approach allows capture of context, versioning and swift policy model changes.
Key trade-offs (Privavcy vs Security)	Priority-Protocol-Concern Relationship

Application (Policy Portal)



Next Steps

- **Add Analysis**
  Model US, UK, RUSSIA(?), Norway, India, Canada, Denmark, (China?) and Finish Cyber strategies using six classes discussed above.

- **Modeling**
  Express the model in Unified Modelling Language. Populate the model.

- **Cyber Policy Portal**
  Create a search-enabled repository / portal to store, share, and search these models based on different criteria.

- **Strategy-Response Mapping**: Depending upon the data availability a useful exercise will be to see how feasible a strategy model is in terms of its day-to-day deployment.

Interim Outcomes

- National (Dutch, German and British) and regional cyber strategy (EU) were analyzed to enable better characterization of these initiatives.
- Comparison of the EU Model with the rest demonstrates that evolution of regional strategy and national strategies of the members of the regional alliance happens at different scales.
- Comparison of national initiatives highlights further categories required for Interoperation and improvements among nation states.
- A clean way to separate the generic and specific cyber concerns of nation states by annotating policy statements as class instances.
- Metamodel can be used to aggregate initiatives by cyber concerns to identify partners and allies in cyberspace.
- **Helps to decipher cyber strategy initiatives in a technology independent manner**.

Obstacles

- Some cyber strategy documents are not available in English.
- Where to get the response data from for assessing Strategy-Response Gap (this is not published any where).
- How to get policy issues data from corporate actors operating in civil, military, technology and commerce domains?

Your help will be greatly appreciated!

Acknowledgement

Minerva Consortium
STTP Programme, Harvard Kennedy School

aadya_shukla@hks.harvard.edu