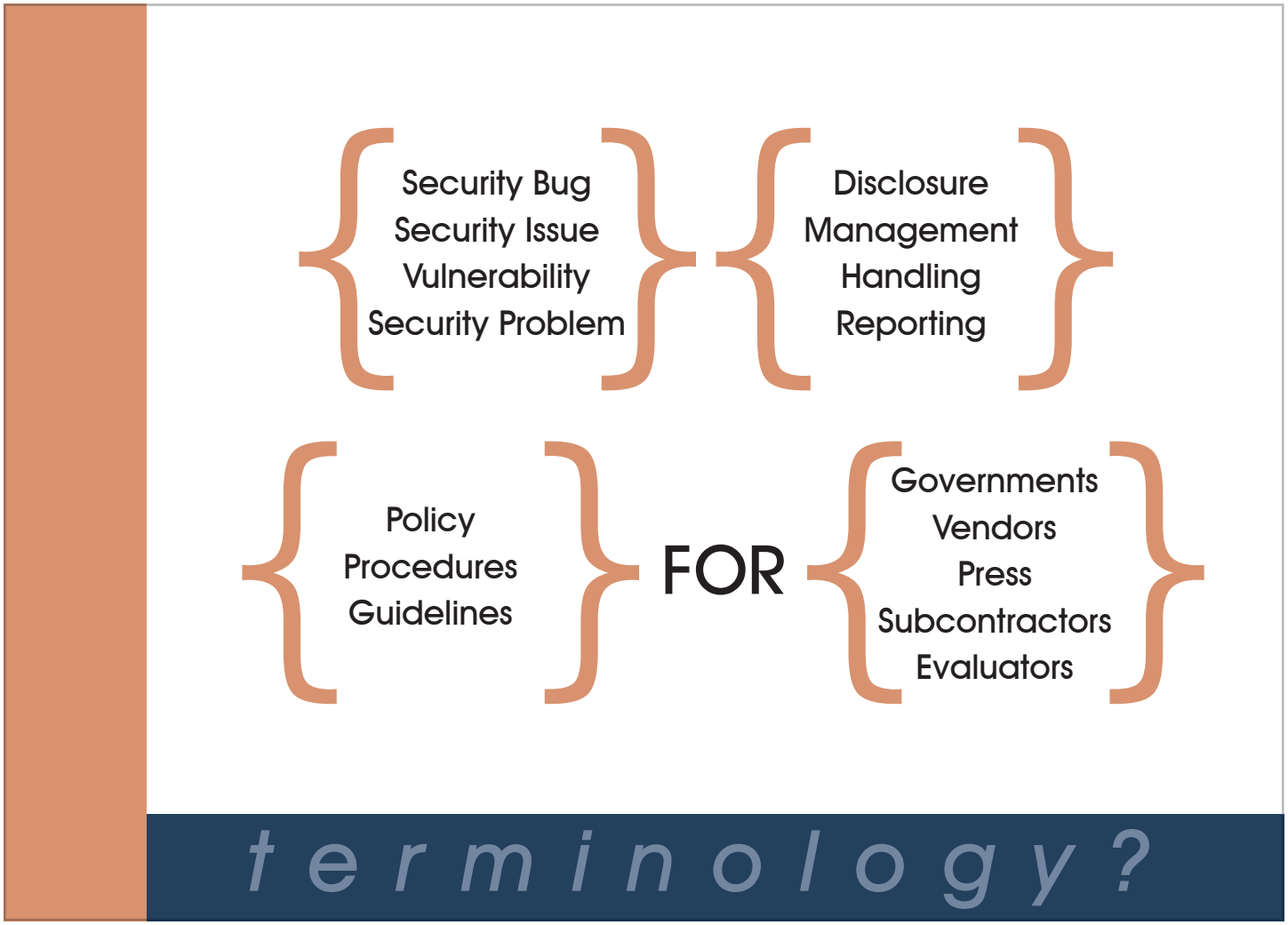
Checklist for Designing a Vulnerability Disclosure Policy

Tiina Havana, Marko Laakso, Pasi Kemi, Juha Röning

Oulu University
Secure Programming
Group

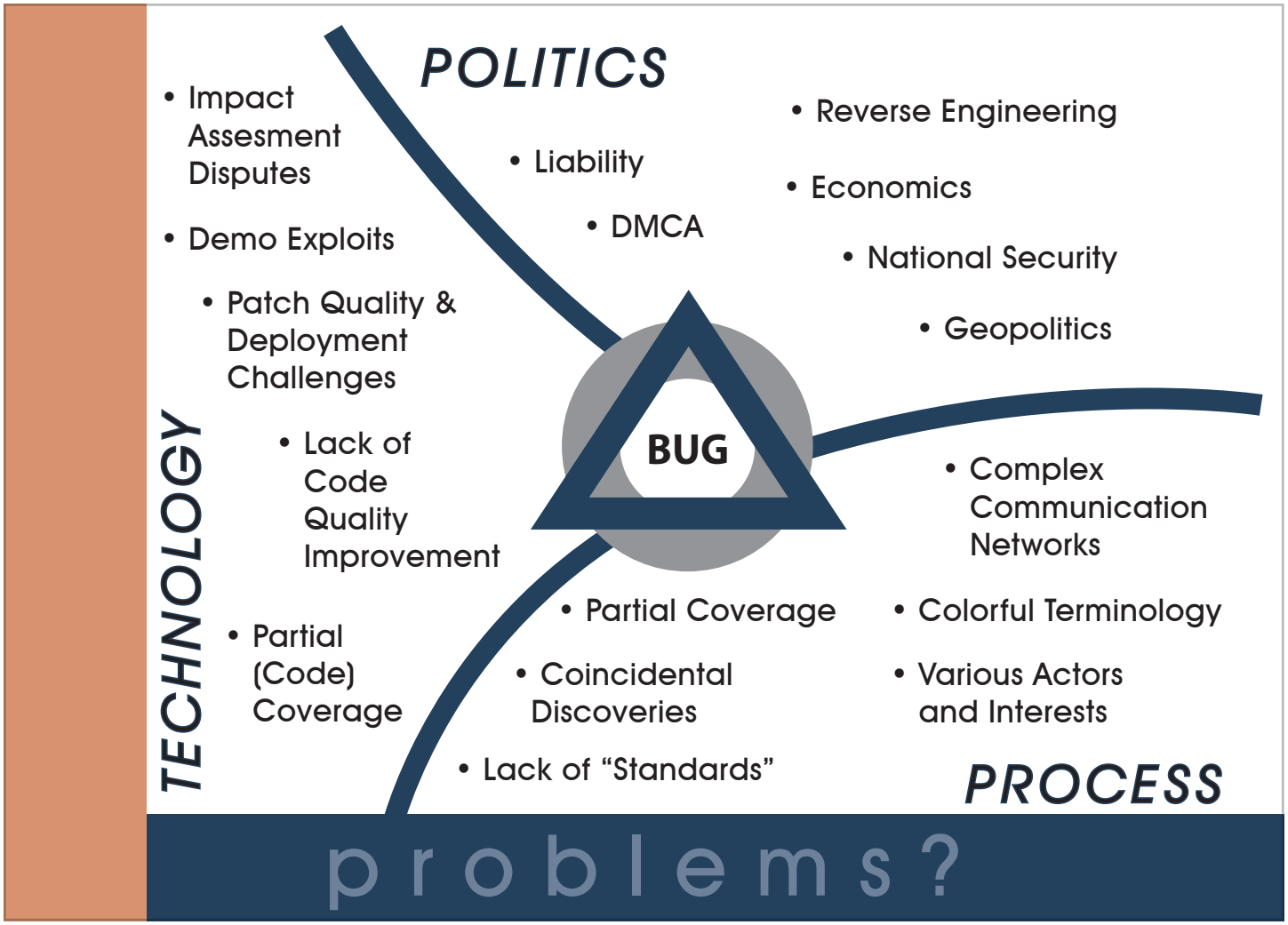
ABSTRACT

Vendors, governments and information security researchers are creating vulnerability disclosure, handling and management policies, procedures and guidelines. We perceive a risk of considering the involved aspects too narrowly, and thus there is danger of missing the big picture. The purpose of this presentation is to provoke evaluation of vulnerability disclosure policy in its context. The presentation illustrates actors that are involved, the communication networks that they form as well as values and beliefs people taking part in the communication process may have towards it. This presentation offers collections of issues and perspectives which support evaluating and constructing a vulnerability disclosure policy.



SLIDE 2: Terminology?

We have	**- different actors**
speaking in	**- different terms**
trying to solve	**- different goals**
from	**- different viewpoints.**
For vulnerability work they share	**- a common ground.**



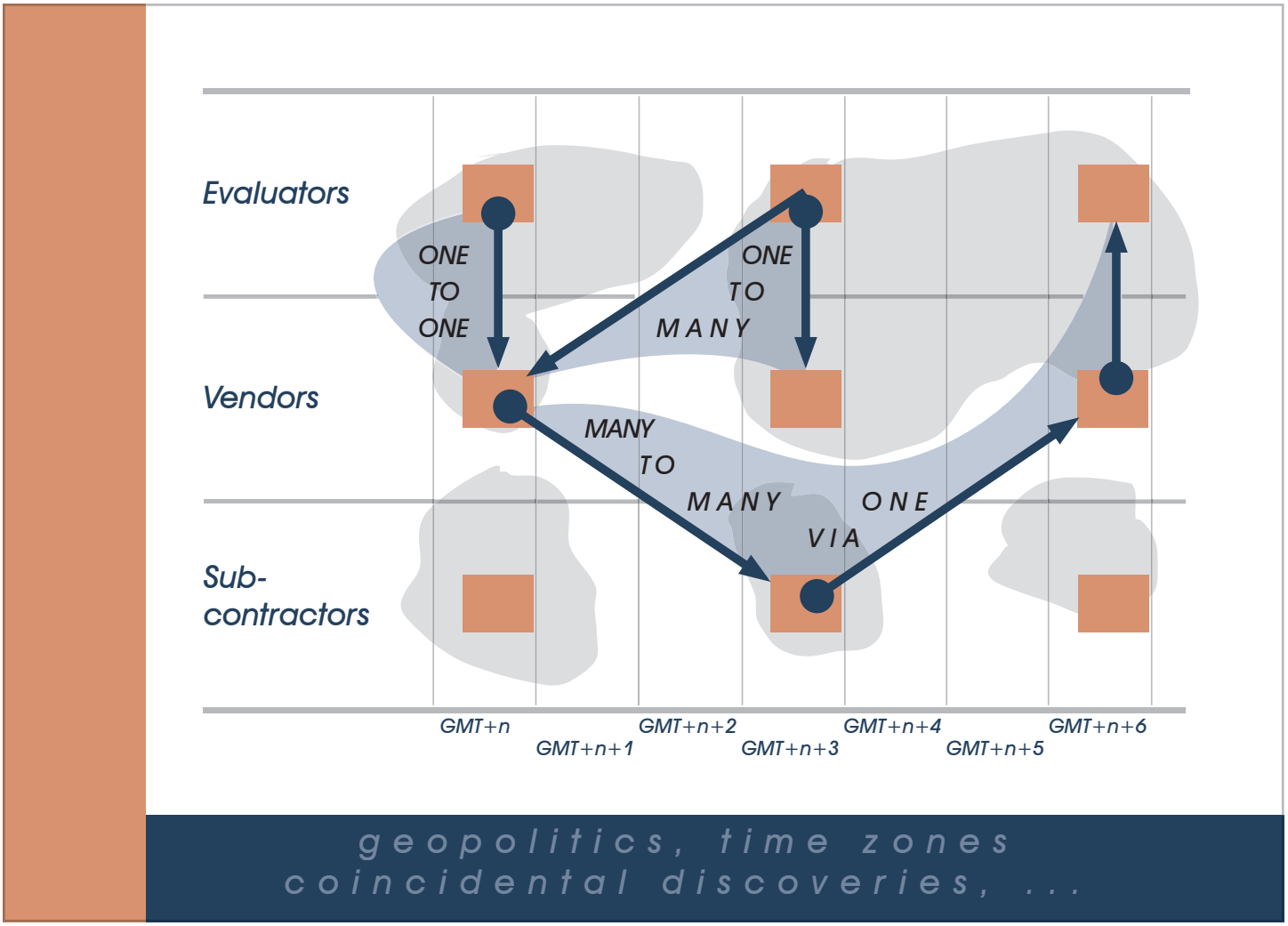
SLIDE 3: Problems?

We share "the buzz on the bug" and problems swarming around it.

When designing a vulnerability policy you should take a look at the known problem areas of the field and decide:

- a problem does not apply to your policy
- a problem is relevant:
  - your policy addresses the problem in proactive way or
  - your policy addresses the problem in reactive way

On more abstract level you can weight different problem sectors.

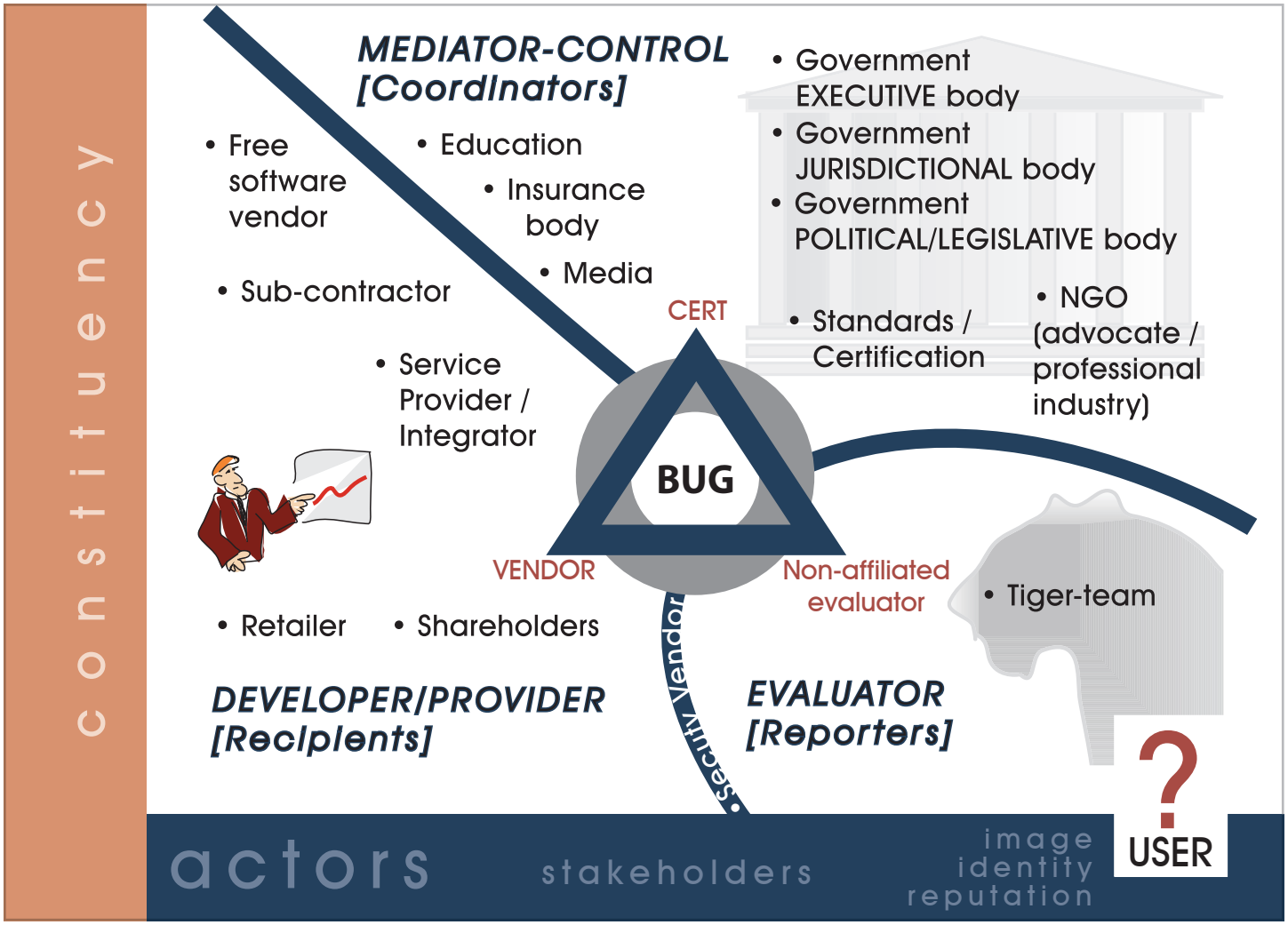


SLIDE 4: Geopolitics, time zones, coincidental discoveries ...

With some of problems taken as examples, does your policy deal with:

- Geopolitics:
  - what if you have various vendors that should be informed, and there are vendors from politically unstable countries among them. Should they be informed as well?
- Time-zones:
  - delays, timings and grace periods
- Coincidental discoveries:
  - someone else finds the same thing at the same time and points out even more vendors that are affected
- Complex communication networks:
  - you tell a vendor, who tells a subcontractor who tells another vendor, who uses the same broken subcontracted code, who releases an advisory

Should your policy deal with - these problems?
If yes - just in these scenarios?
If no - should it explicitly say so?
= planning your crisis management



SLIDE 5: Actors, stakeholders, constituency

If the problematics on the previous slide appear simple, what happens when we take a look at the whole scene?

- What is your constituency? (who do you represent with your policy?)
- Who are the active actors? (interaction/ interface?)
- Who are the stakeholders? (an interest in your policy?)

When constructing your policy, it helps to realize:

- What is the area you can systemise?
- What is the area you can influence?

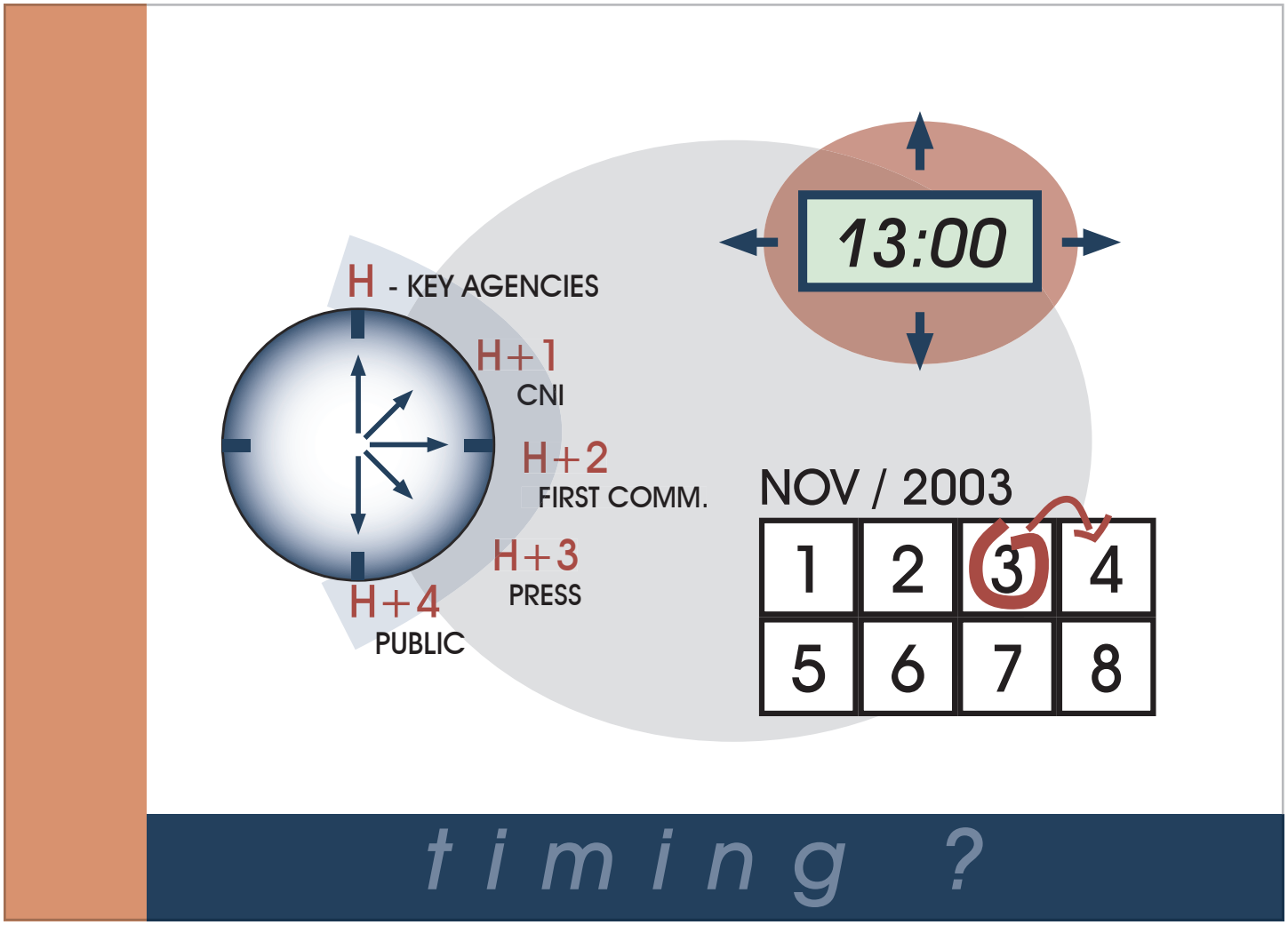
E.g. policy that dictates behaviour of those you don't control nor steer.

Reputation: How others see who you are
Identity: How you see yourself
Image: How you would want others to see who you are

Before constructing your policy you might want to check if you already have a reputation in the vulnerability business:

- If you have a good reputation on the field, why? Should those things be left unchanged
- If you have reputation problems, could your policy promote image that would improve things?

Is your policy constructed more for image than identity? On the other hand if you are doing fine publishing your identity maybe good for your image.



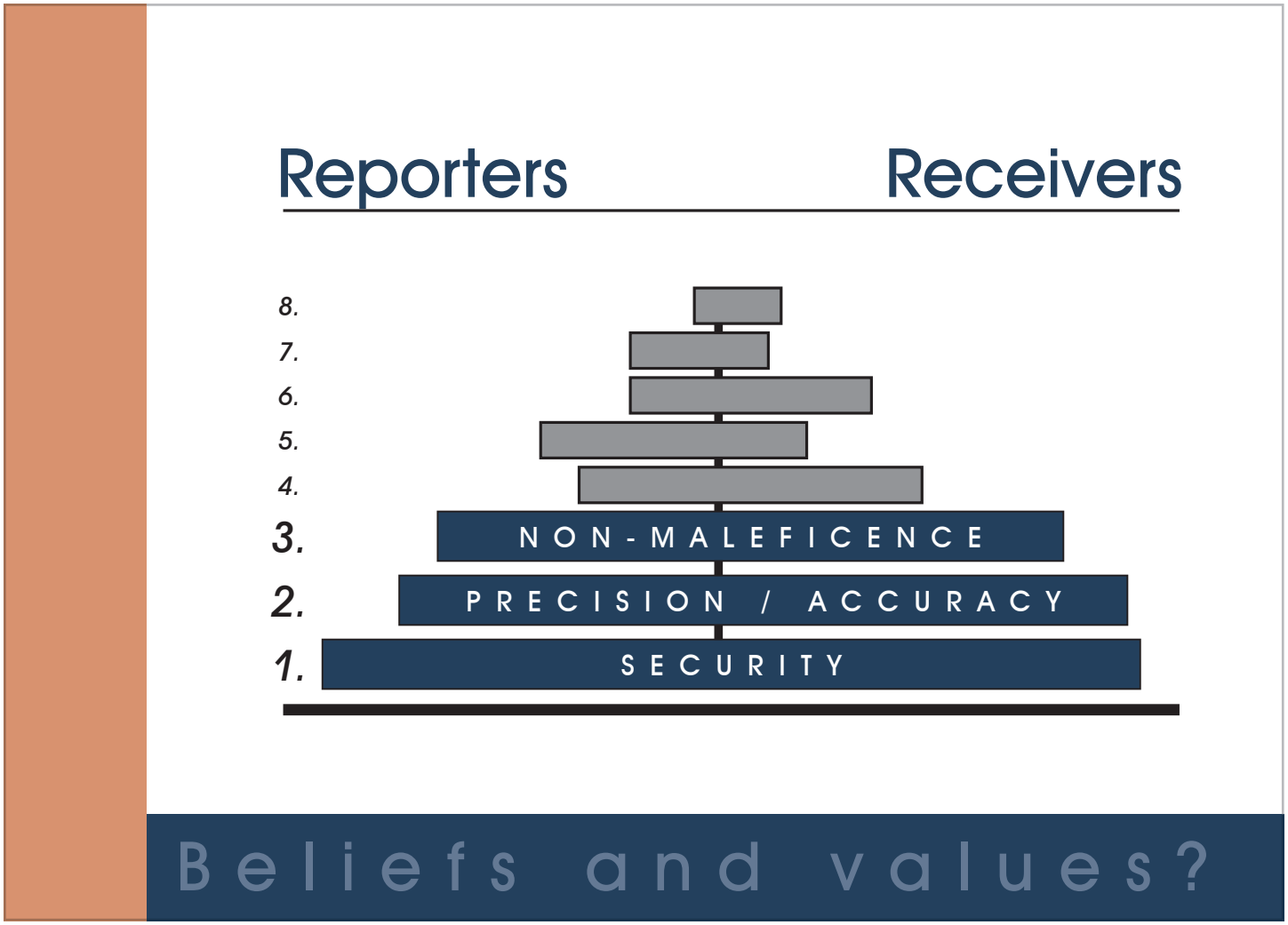
SLIDE 6: Timing?

Try considering at least one aspect of your policy in context of dimensions brought up on the previous slide. How is the timing of the information dissemination affected?

- The easiest way out: synchronous release?
  - However, you cannot necessarily systemise/influence the wide audience.

- The other possibility: different actors valued differently?
  - Makes the model more complex and conflicts of interests more obvious.

- A third case you can collide with when planning the timing issues is e.g. the possibility that someone wants to postpone the release, which again makes the disclosure more challenging.



SLIDE 7: Beliefs and values?

- Consolation after all this complexity.
- Besides Common problems, we also share common goals and values.
- These were found to be common to reporters and receivers in 2002 survey.
- Wouldn't it be interesting to survey the opinions of all these actors?

SLIDE 8: Strategy?

"Public be fooled",
"Vendor be cooperated with",
"Reporter be informed" and
"Government be damned"?

- The basis of the division presented on the slide lies in the communication theory.
- Originally this was a somewhat provocative model about an organisation's potential relationships to publicity. The division was presented by John Fiske.
- Can also be extrapolated to describe the relationships to other stakeholders.
- When you have your policy ready, take this is multiple choice test and say what is your strategy.

SLIDE 9: The End

References:

- http://www.ee.oulu.fi/research/ouspg/

- http://www.ee.oulu.fi/research/ouspg/sage/disclosure-tracking/

- Havana T., Röning J. “Communication in the Software Vulnerability Process”. In proceedings of the 15th FIRST Conference on Computer Security Incident Handling. Ottawa, Canada. June 22-27, 2003.
http://www.ee.oulu.fi/research/ouspg/protos/sota/FIRST2003-communication/
http://www.ee.oulu.fi/research/ouspg/protos/sota/reporting/

- Laakso M., Takanen A., Röning J. “The Vulnerability Process: a tiger team approach to resolving vulnerability cases”. In proceedings of the 11th FIRST Conference on Computer Security Incident Handling and Response. Brisbane. 13-18 June, 1999.
http://www.ee.oulu.fi/research/ouspg/protos/sota/FIRST1999-process/

- Laakso M., Takanen A., Röning J. “Introducing constructive vulnerability disclosures”. In proceedings of the 13th FIRST Conference on Computer Security Incident Handling. Toulouse. June 17-22, 2001.
http://www.ee.oulu.fi/research/ouspg/protos/sota/FIRST2001-disclosures/