How many shades of NIS?

Understanding organizational cybersecurity cultures and sectoral differences

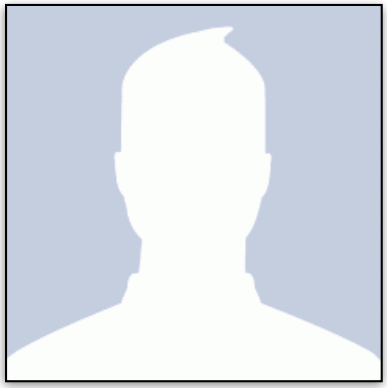
How many shades of NIS?

Understanding organizational cybersecurity cultures and sectoral differences

Prof. Awais Rashid

Dr. Dirk van der Linden

Dr. Sveta Milyaeva



+1

International and professional partners:

THALES
CYBER AND CONSULTING

CYBER
BRISTOL & BATH

CCLP
המרכז לחקר סייבר משפט ומדיניות
THE CENTER FOR CYBER LAW & POLICY

1. *Managing security risk*: Appropriate ***organizational structures, policies, and processes*** are ***in place*** to understand, assess and systematically manage security risks to the network and ISs supporting essential services.

2. *Protecting against cyber attack:* Proportionate security measures are in place to protect essential services and systems from cyber attack.

3. *Detecting cybersecurity events:* Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.

4. *Minimizing the impact of cybersecurity events:* Capabilities to minimise the impact of a cyber security incident on the delivery of essential services including the restoration of those services where necessary.

NCSC's *The NIS Guidance Collection*, https://www.ncsc.gov.uk/guidance/nis-directive-top-level-objectives

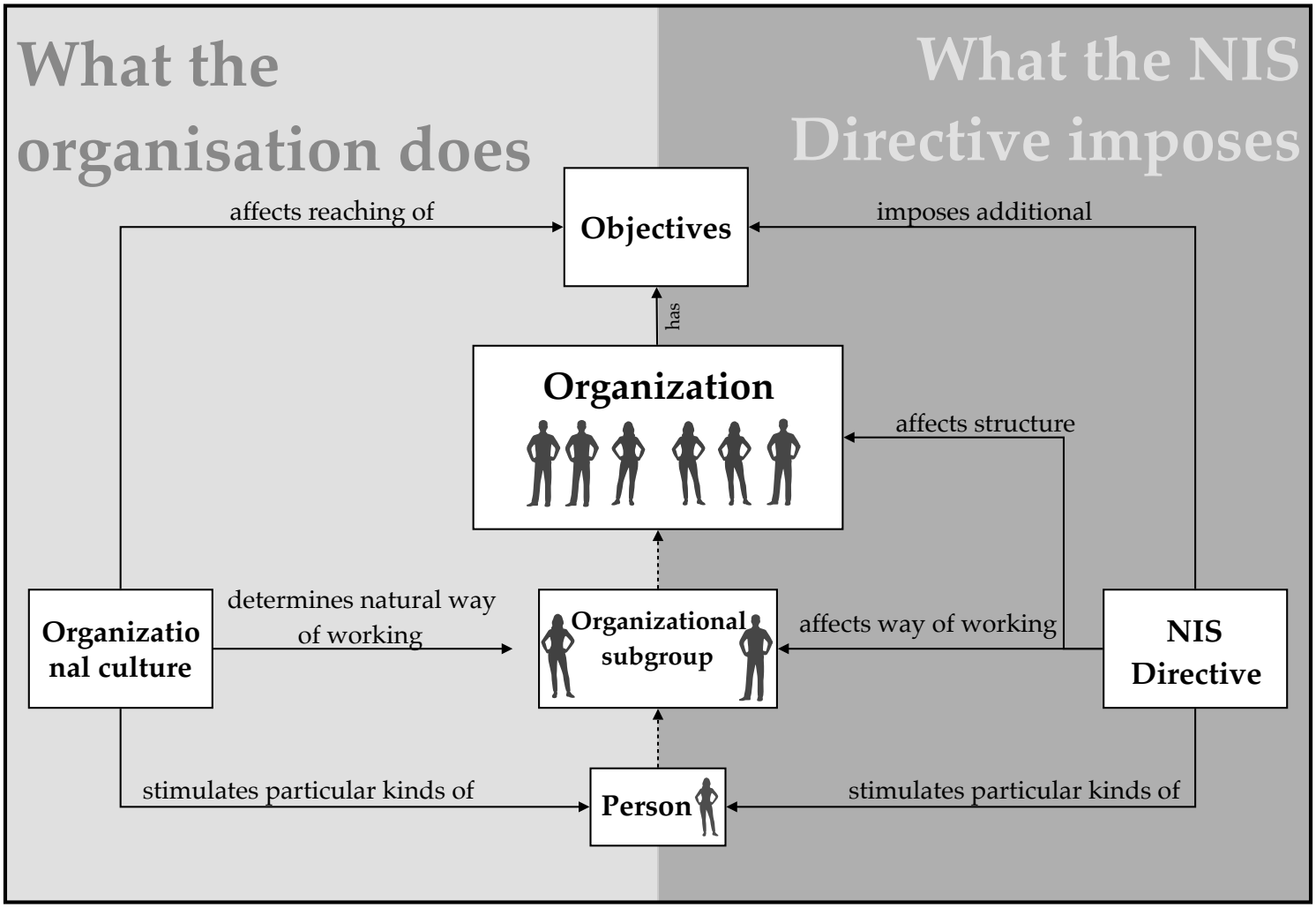


Figure 1. Conceptual framework: imposition of the NIS Directive may *complement* and *clash* on several layers: the way people work, the way the organisation is structured, and how its objectives are achieved.

Our goal is to establish a baseline of cybersecurity efforts in essential infrastructure sectors in the UK, by *investigating*

1. *What* **cybersecurity practices** *are observed in organizations providing essential infrastructures?*

2. *What is the* **organizational culture** *in groups responsible for security in these organizations?*

3. *Is there significant difference between organizations or sectors in the practices they observe?*

4. *Is there significant difference between organizations or sectors in the cultures they have?*

5. *What is the relation, if any, between cybersecurity organizational culture and practices?*

6. *What practices, if any, are positively or negatively affected by specific organizational cybersecurity culture?*

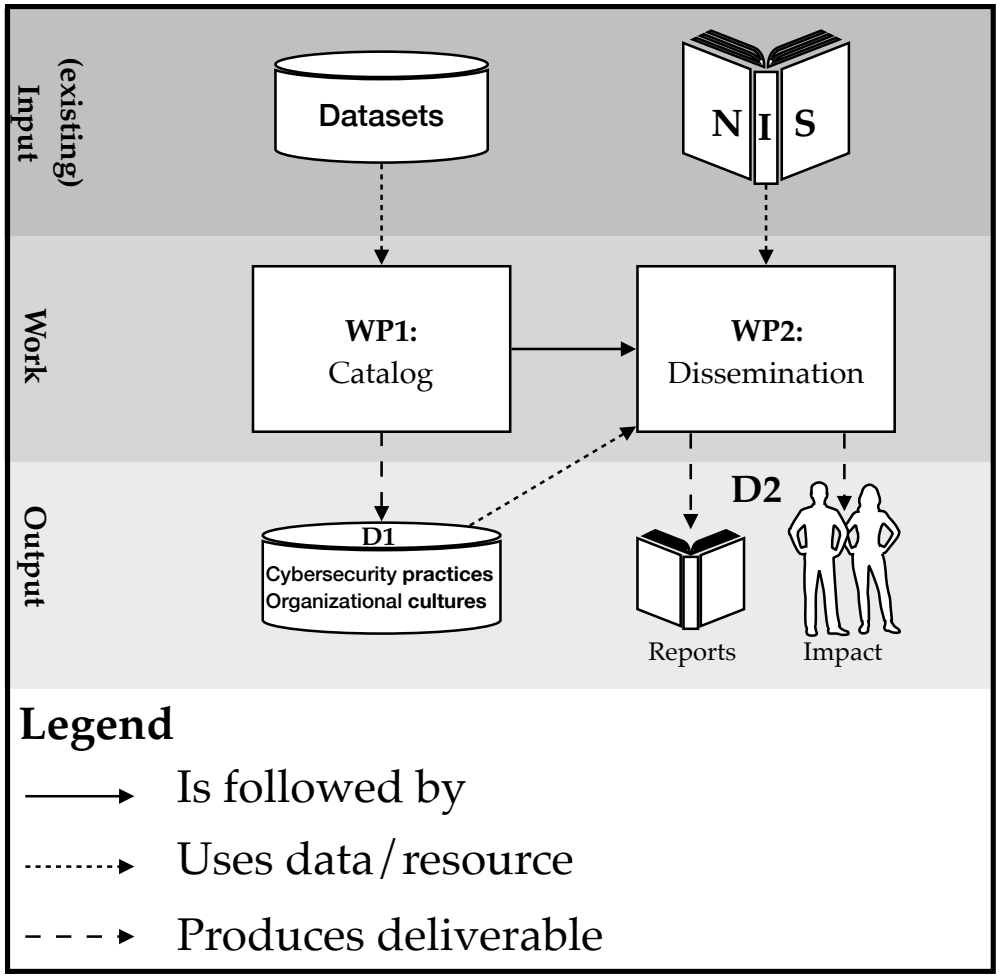


Figure 2. Workplan, showing work packages, existing inputs, and deliverables.

Our method is to use organizational **etnography** to gather rich data translatable into **policy recommendations**.

or, to summarize:

NIS vs the Real World