MUNI
FSS

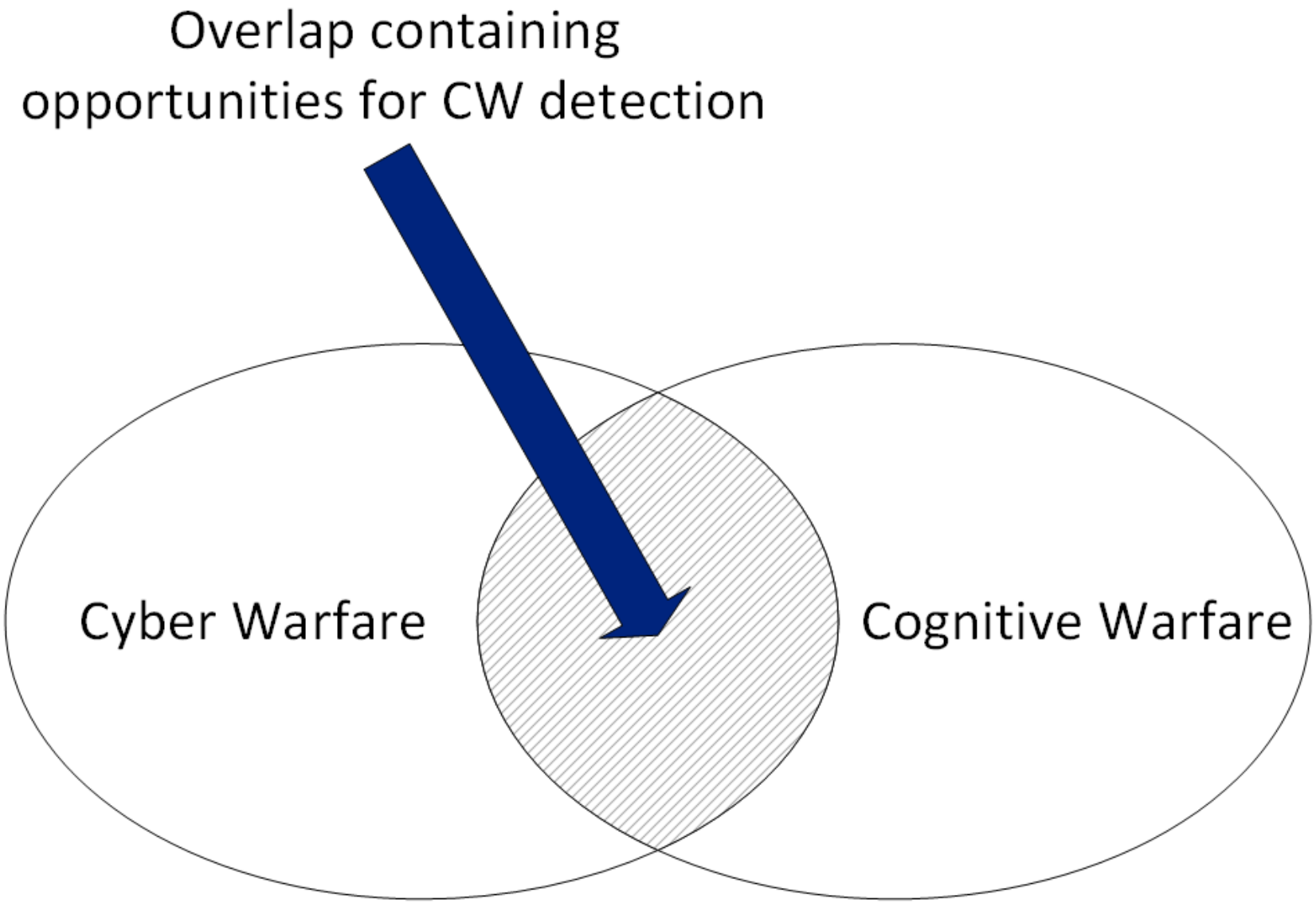
Detection Tools for Cognitive Warfare

Leveraging the Cyber Domain

Cognitive Warfare

- „An unconventional form of warfare that uses cyber tools to alter enemy cognitive processes, exploit mental biases or reflexive thinking, and provoke thought distortions, influence decision-making and hinder actions, with negative effects, both at the individual and collective levels“ (Claverie, Cluzel 2022)
- Jacques Ellul‘s *Propaganda* (1973) as inseparable part of technological society → a fitting parallel to Cognitive Warfare
- CW more dangerous with new knowledge and technologies

MUNI FSS


Overlap containing
opportunities for CW detection
Cyber Warfare
Cognitive Warfare

MUNI
FSS

Cyberspace – Opportunity for CW Detection

- Existing experience and tools
- Cyber warfare and CW often in concert
- Edge over adversaries by fast development based on repurposing of cyber monitoring tools, solutions and academic works
- Points for consideration:
  - Relatedness to Cognitive Warfare
  - Automatization potential

MUNI FSS

Where to Look?

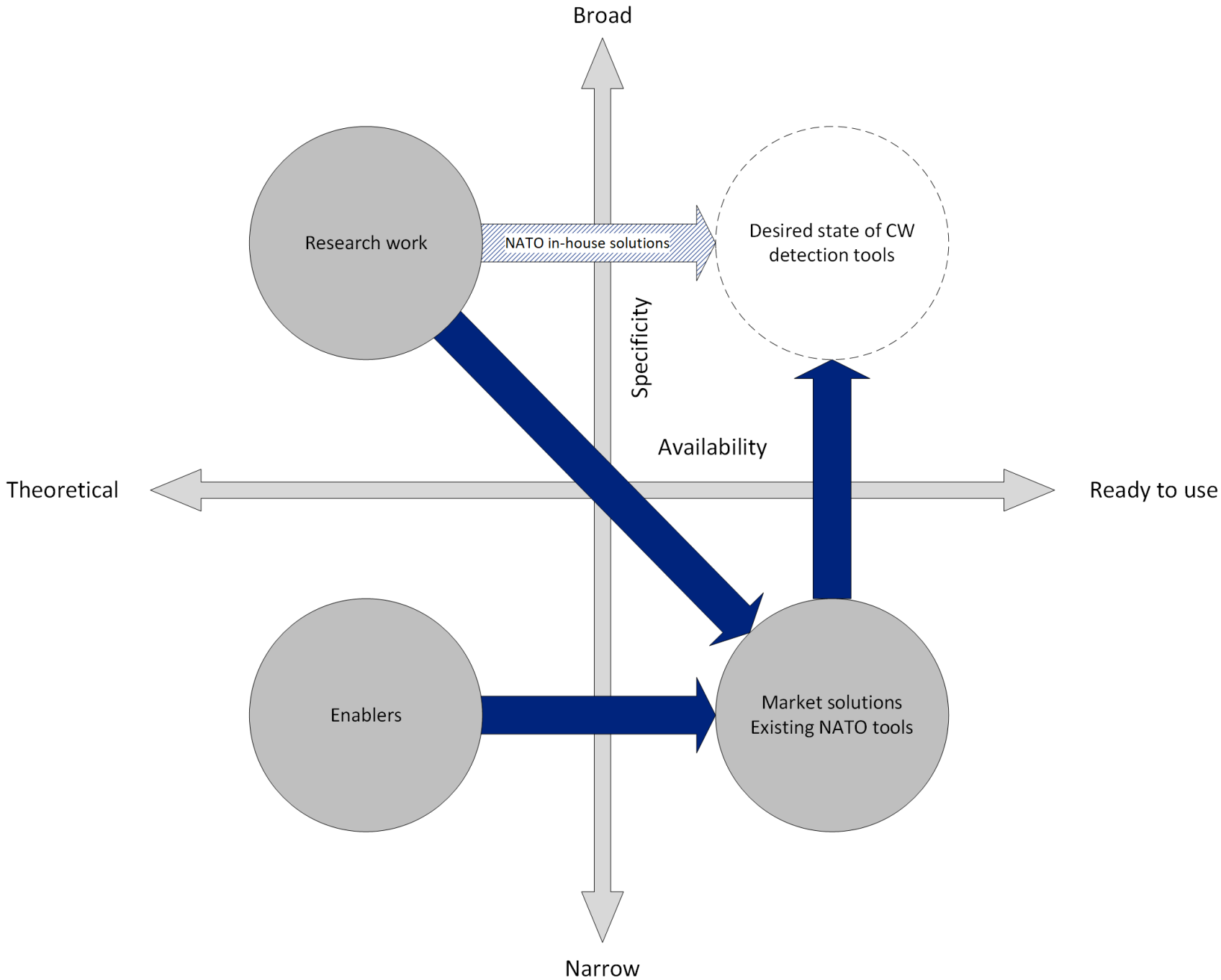
- Research / Academia
  - Innovative x Slow pace
- Open Market
  - Available x Inflexible + potential risk

Two primary axes for detection tools knowledge and tools:

(1) Specificity

(2) Availability

MUNI FSS


Broad
Research work
NATO in-house solutions
Desired state of CW detection tools
Specificity
Availability
Theoretical
Ready to use
Enablers
Market solutions
Existing NATO tools
Narrow

Ensemble Learning

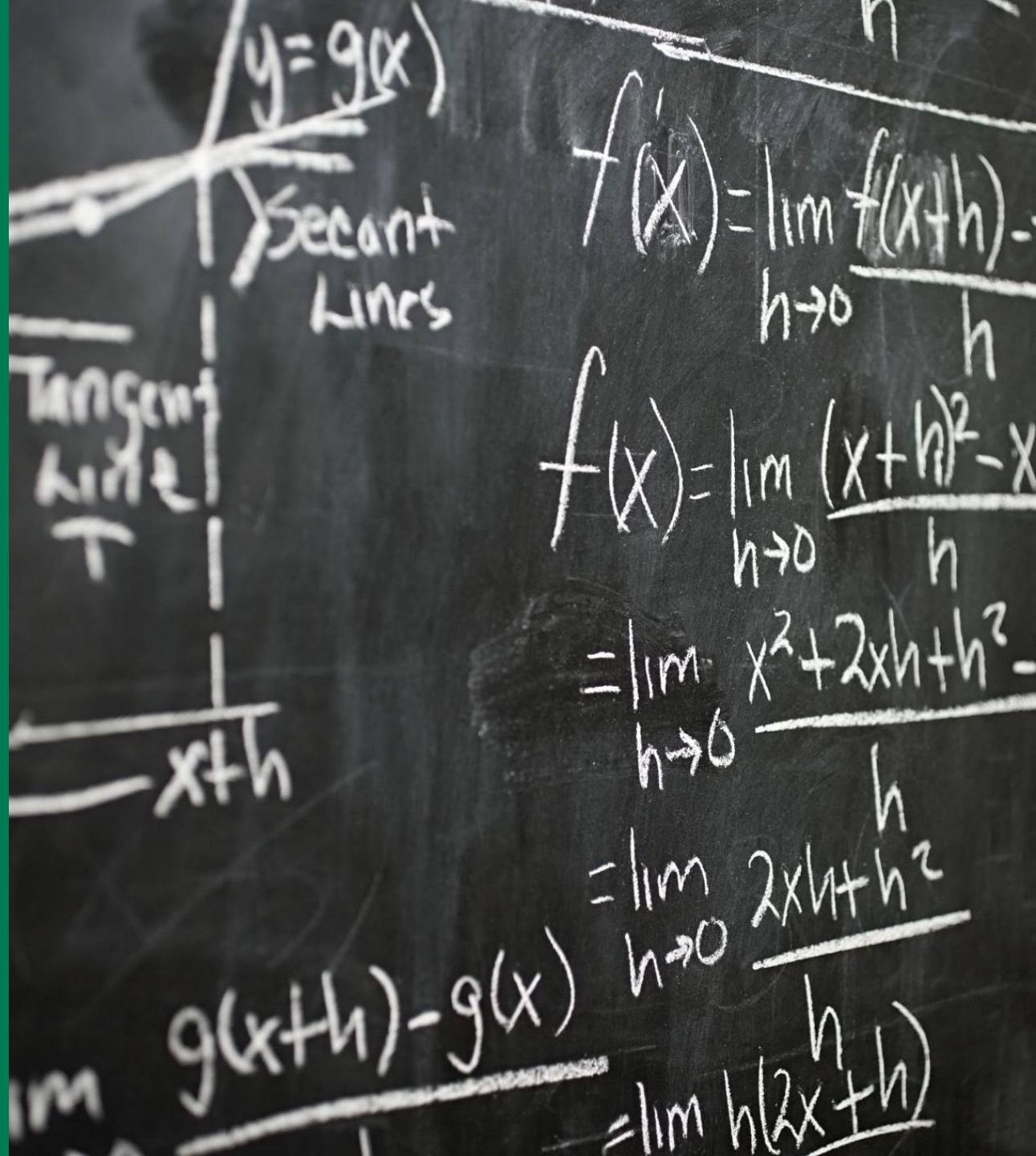
- Combining two or more machine learning algorithms to achieve better and more accurate results
- Primary learning methods:
  - Bootstrap aggregation
  - Stacking Generalization
  - Boosting
- Possible combination with deep learning
- Can demand high resources

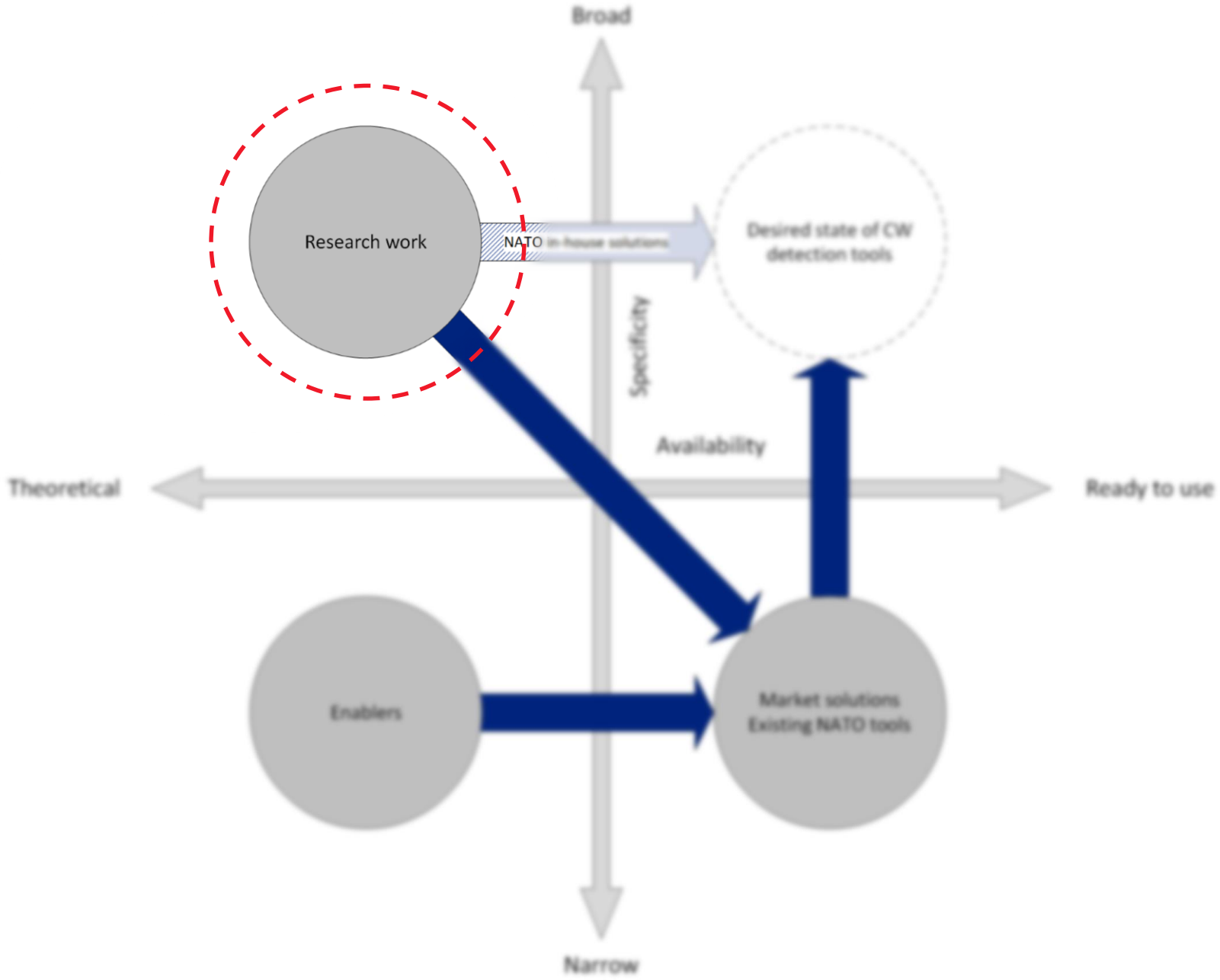
Deep Learning

- Machine learning enables computers to learn **without explicit programming**.
- Large datasets needed for training
- Various learning methods: supervised, unsupervised, semi-supervised, reinforcement learning methods.
- Different datasets for training and testing

MUNI
FSS

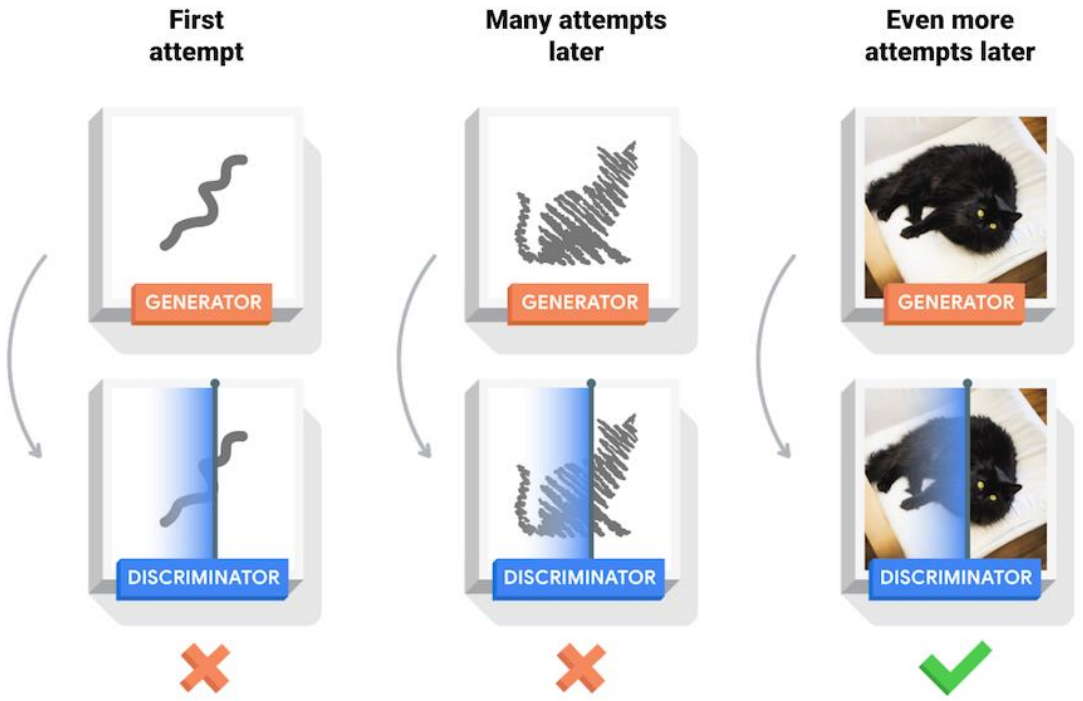
Methods




Broad
Research work
NATO in-house solutions
Desired state of CW detection tools
Specificity
Availability
Theoretical
Ready to use
Enablers
Market solutions
Existing NATO tools
Narrow

Methods

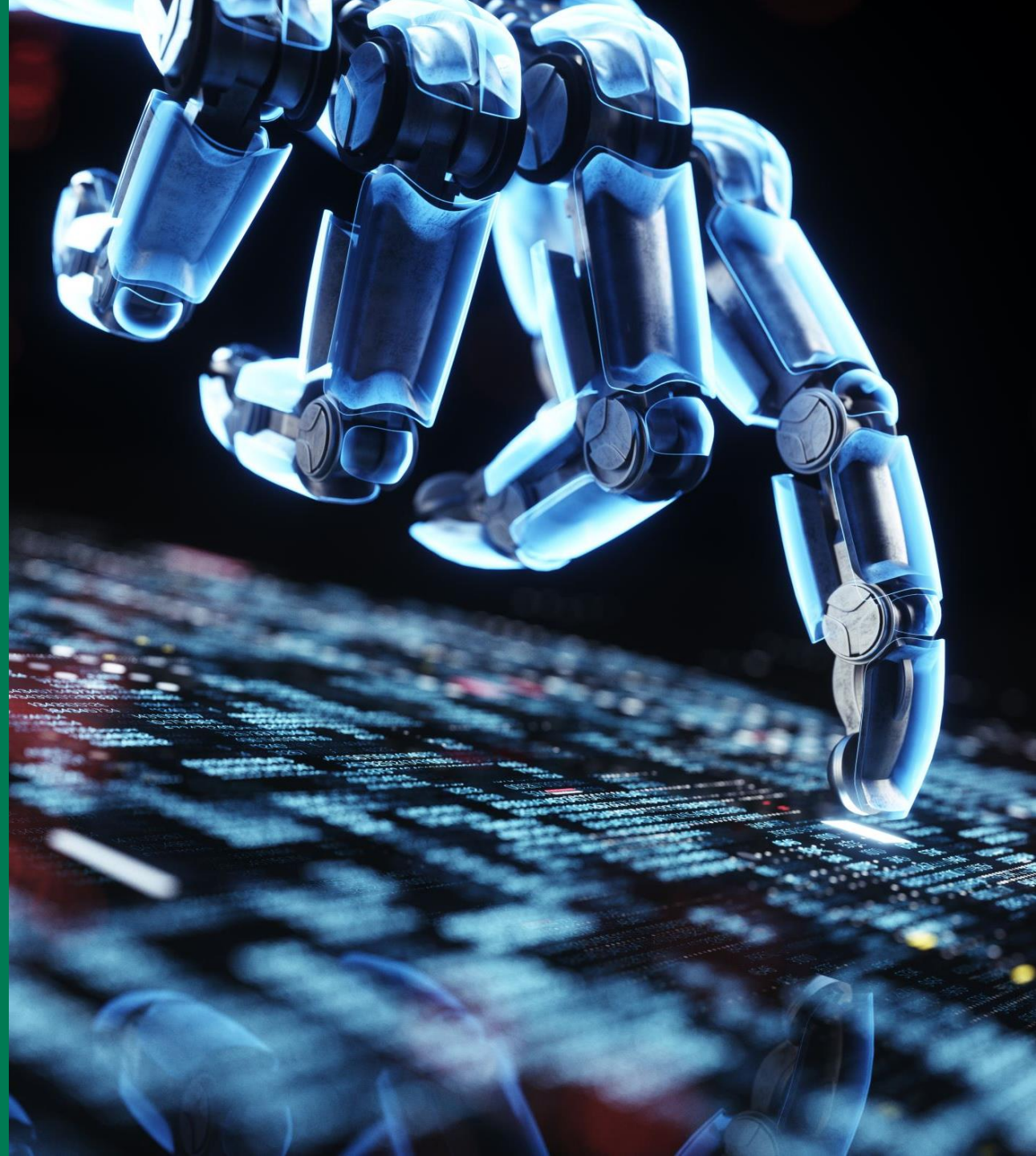
- Decision Tree & Random Forest
- Generative Adversarial Networks
- Shades of Truth
- Social Network Analysis
- Multimodal Content

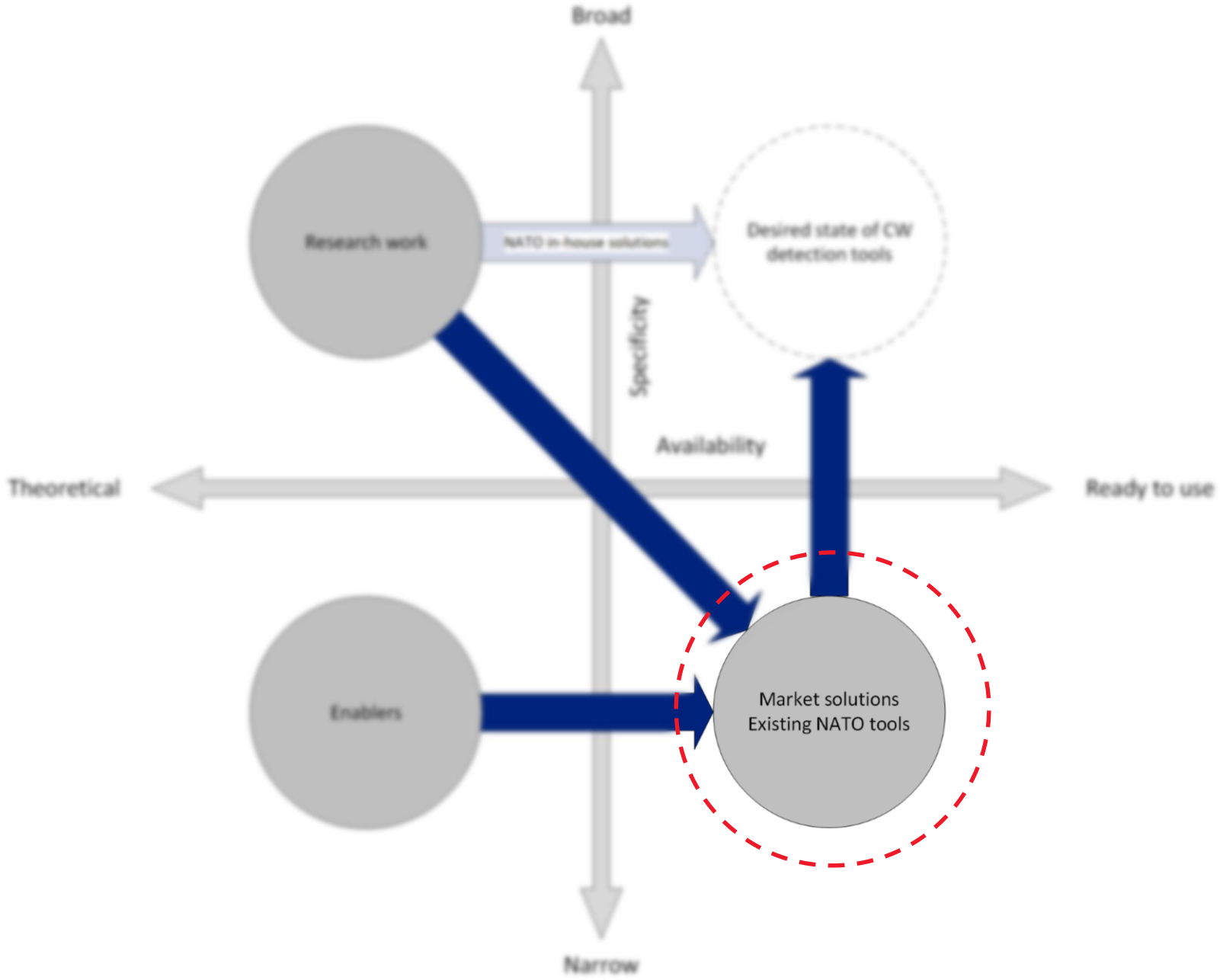


MUNI FSS

MUNI
FSS

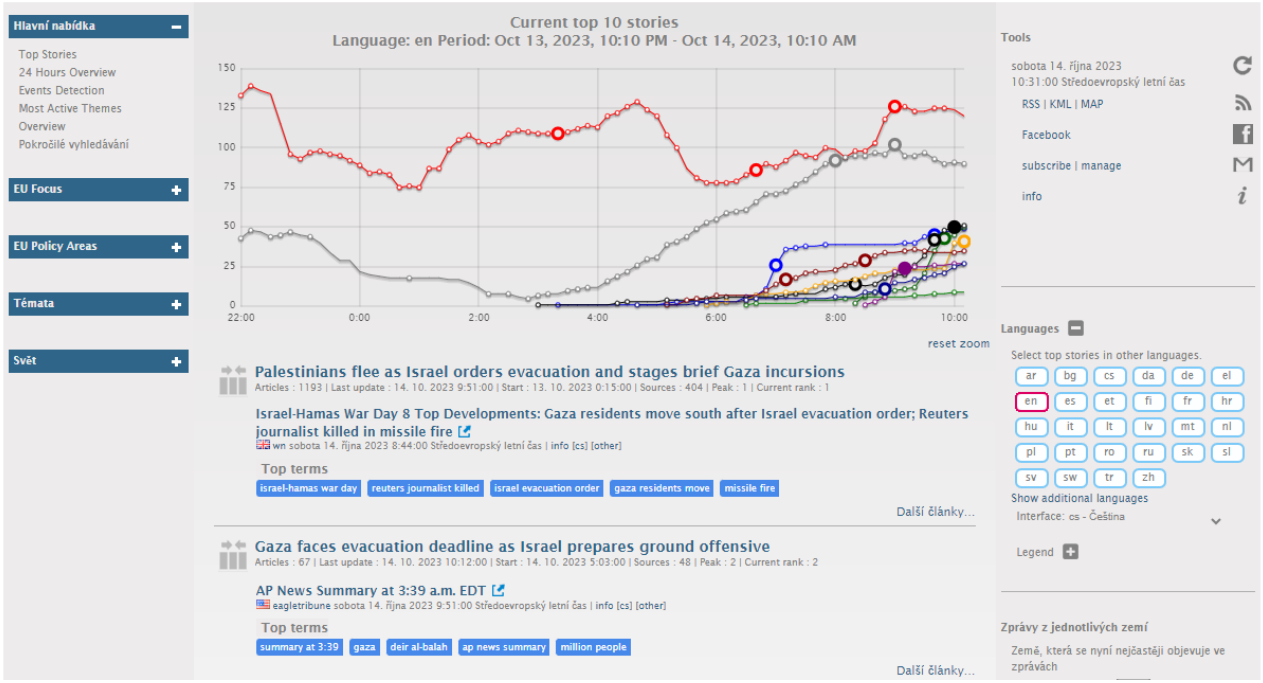
Tools



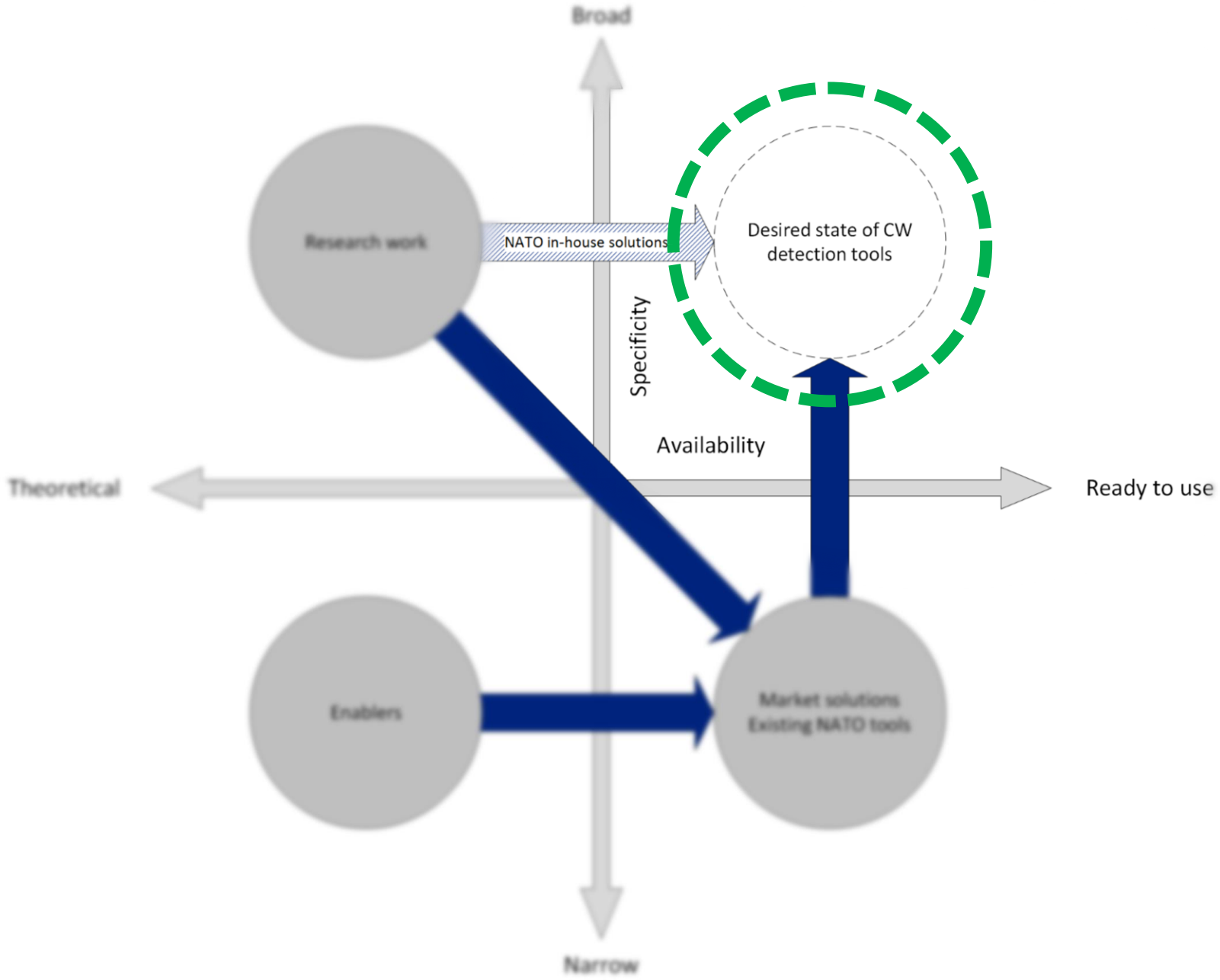

Broad
Research work
NATO in-house solutions
Desired state of CW detection tools
Specificity
Availability
Theoretical
Ready to use
Enablers
Market solutions
Existing NATO tools
Narrow

Tools

- National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena (NAAS)
- The Europe Media Monitor
- Commercially available tools:
  - Belief3
  - ThreatMetrix
  - Cisco Secure Network Analytics
  - …



MUNI FSS


Broad
Research work
NATO in-house solutions
Desired state of CW detection tools
Specificity
Availability
Theoretical
Ready to use
Enablers
Market solutions
Existing NATO tools
Narrow

MUNI
FSS

Thank you!

Contact information:

robin.burda@fss.muni.cz

Sources

Claverie, Bernard, and François Du Cluzel. 2022. "'Cognitive Warfare': The Advent of the Concept of 'Cognitics' in the Field of Warfare." NATO Collaboration Support Office. https://hal.science/hal-03635889/document.

Ellul, Jacques. 1973. *Propaganda: The Formation of Men's Attitudes*. Vintage.

Images

Slide 12

- https://commons.wikimedia.org/wiki/File:Decision_Tree_vs._Random_Forest.png
- https://www.tensorflow.org/tutorials/generative/dcgan

Slide 15

- https://emm.newsbrief.eu/NewsBrief/clusteredition/cs/latest_en.html

MUNI FSS