NIAG SG 279

How to certify AI applications according NATO PRUs

Mirek Necas, SG 279 Chair

Context of the NIAG SG 279

NATO Artificial Intelligence Strategy

- Principles of AI responsible use within NATO (NATO PRUs)
- NIAG SG 252: Emerging and Disruptive Technologies in the context of Emerging Powers

DARB: Data and AI Review Board

- NIAG SG 279: Protocols and Standards to Certify Applications using AI within NATO

NATO PRUs

Lawfulness: AI is developed and used in accordance with national and international law, including international humanitarian law and human rights law.

Responsibility and Accountability: AI is developed and used with appropriate levels of judgment and care; clear human responsibility shall apply.

Explainability and Traceability: AI is appropriately understandable and transparent, including through the use of review methodologies, sources, and procedures.

Reliability: AI has explicit, well-defined use cases. The safety, security, and robustness of such capabilities are subject to testing and assurance within those use cases across their entire life cycle.

Governability: AI is developed and used according to it‘s intended functions; allows appropriate human-machine interaction; the ability to detect and avoid unintended consequences; and the ability to take steps, when AI demonstrate unintended behaviour.

Bias Mitigation: Proactive steps will be taken to minimize any unintended bias in the development and use of AI.

Methodology of the study

Based on the Risk Management approach:

1: Describe role of AI in the defined Use Cases

2: Map relevant civilian AI standards and identify gaps

3: Identify risks of using civilian standards / no standards

4: Propose steps necessary to build trusted environment

Teams arranged according Use Cases

1. Military Mobility
2. Imagery Analysis
3. Information Environment Assessment
4. Cyber Threat Analysis
5. Assisted Decision Making
6. Climate Analysis

Key Findings and Recommendations

Principles relate each another

Role of AI is different in various Use Cases

More than 30 relevant industry standards

Recommended certification approach

Importance of common understanding

Principles relate each another

Different Role of AI in various Use Cases

	Military Mobility	Imagery Analysis	Cyber Threat Analysis	Information Environment Assessment	Assisted Decision Making	Climate Analysis
Natural Language Processing			X	**XX**	**XX**	X
Computer Vision	X	XX		X	X	
Speech Recognition				**XX**	**XX**	
Anomaly Detection	X	X	**XX**	X	X	X
Graph-based Algorithms	**XX**		**XX**	X	**XX**	
Time Series Analysis & Forecasting	X		X	**XX**	X	**XX**
Optimization Algorithms	**XX**				**XX**	**XX**
Generative Algorithms				**XX**	**XX**	
Intelligent Agents	**XX**		X	X	X	
Data mining	X	X	X	X	X	X

Relevant industry standards

60 standards analysed (IEEE, ISO/IEC, BSI, SAE, CAN/CIOSC)

- 23 Published
- 12 Proposal in approval process
- 25 Draft / Preparatory

More than 30 was found relevant to AI certification

Most weak areas: Lawfulness, Responsibility and Accountability

Recommended certification approach

Certification shall be an enabler to AI implementation, industry standards shall be used when possible.

AI application shall be certified in a context of the whole system, Risk Management approach shall apply.

Common PRUs understanding

USA DoD 5 principles of ethical AI use: Responsibility, Equitability, Traceability, Reliability and Governability;

European Commission proposes Artificial Intelligence Act (AIA) based on similar principles;

United Kingdom introduced vision of AI implementation in Defence. AI implementation shall be Efficient, Effective, Trusted and Influential;

OECD introduced 5 principles Human-centred values and fairness; Transparency and explainability; Robustness, security and safety; Accountability;

Questions?

Principles relate each another

Role of AI is different in various Use Cases

More than 30 relevant industry standards

Recommended certification approach

Importance of common understanding

Thank you for your attention!

Mirek Necas

NIAG SG 279 Chair

www.tovek.com

necas@tovek.cz