Ontology Specification Document for the National Cybersecurity Strategy Development Guide (NCSDG) Ontology

1. Introduction

This document specifies an ontology for representing knowledge related to the development of a National Cybersecurity Strategy (NCS). The ontology aims to provide a structured and formal representation of key concepts, relationships, and actors involved in NCS development, facilitating, knowledge, sharing, reasoning, and data integration in this domain.

2. Purpose and Scope

The primary purpose of this ontology is to:

- Provide a common vocabulary and conceptual framework for describing NCS development elements.
- Enable the representation of relationships between different stakeholders, policies, and actions.
- Facilitate the development of knowledge-based systems for cybersecurity management.

The scope of the ontology includes:

- Key elements of a national cyber security strategy
- Stakeholders involved in NCS development (government, private sector, etc.).
- Structures and processes.
- Risk management concepts.
- Capacity and capability development.
- Critical infrastructure protection.
- Cyber threat.
- Technical structures.

3. Ontology Overview

The ontology is organised around the central concept of the National Cybersecurity Strategy (NCS) and its related components. The main classes and their relationships are as follows.

Key Classes

• NCS: represents the overall National Cybersecurity Strategy (NCS).
  – Governance: represents the governance aspect of NCS development.
    ∗ Legislation
    ∗ Policies
    ∗ Standards
    ∗ Strategies
    ∗ Coordination&MonitoringAssesmentMechanisms
      · Audit
      · KeyPerfomanceIndicators
  – RiskManagement: represents the risk management aspects of NCS development.
    ∗ ControlRisk
    ∗ ReviewControls
    ∗ RiskAssesment
    ∗ RiskIdentification

– Capacity&CapabilityDevelopment: represents the capacity and capability development aspects of NCS development.
    ∗ Training
    ∗ Education&Awareness
– Critical Infrastructure: represents the protection of critical infrastructures.
    ∗ Cyber
    ∗ Human
    ∗ Physical
– TechnicalStructures: represents the technical structures involved in NCS development and implementation.
    ∗ CSIRT/CERT
    ∗ DigitalForensicLab
    ∗ ReportingStructures
• Stakeholder: represents actors involved in NCS development.
– GovernmentStakeholders
– PrivateStakeholders
– SemiGovernmentStakeholders
• CyberThreats: represents various cyber threats.

Key Relationships (Object Properties)

- hasRole: relates a stakeholder to their role in NCS development.
- hasToAdhere, hasToComply, hasToCollaborate, hasToTrain, hasToRaiseAwareness, hasTo
- shareIntelligence, hasToReport, hasToResearch, hasToMeasure, hasToPromote, hasToProtect,
- hasToEnforce, hasToEstablish, hasToImplement, hasToDefineStandards, hasToDevelop,
- hasToEducate, hasToContribute, hasToCooperate, hasToCommunicate: represents
- various responsibilities and actions of stakeholders.
- isAPolicyElement: relates various classes to NCS.
- reportsTo: indicates a reporting structure, e.g., CSIRT reporting to another entity.

4. Intended End-Users

The intended end-users of this ontology include:

Policy makers and government officials involved in the developing and implementation of an NCS.

- Security professionals and researchers.
- Industry stakeholders responsible for protecting critical infrastructure.
- International organisations and agencies working on cyber security.
- Developers of cyber security tools and applications.

5. Intended Uses

The ontology is intended to be used for:

- Supporting the development and implementation of National Cybersecurity Strategies (NCS).
- Facilitating information sharing and collaboration amongst stakeholders.
- Enabling the assessment and evaluation of NCS effectiveness.

- Developing decision support systems for cybersecurity management.
- Enhance cybersecurity awareness, education and training.
- Improving risk management practices.

6. Non-Functional Requirements

- Clarity and consistency: the ontology should be clear, concise, and consistent in its representation of concepts and relationships.
- Accessibility: the ontology should be extensible to accommodate new concepts and relationships as the cyber security landscape evolves.
- Interoperability: the oncologist should be interoperable with other relevant ontologies and data standards.
- Maintainability: the ontology should be designed for ease of maintenance and updating.
- Reusability: the ontology should be reusable in different applications and contexts.

7. Functional Requirements (Competency Questions)

The ontology should be able to answer questions such as:

- Which mechanisms can be used for tracking and assessing the effectiveness of an NCS?
- What are the common cybersecurity threats?
- Who are the stakeholders with a role to research in NCS development?
- What is an NCS?
- Who are the stakeholders that have the role to cooperate?
- What are the key elements of an NCS?
- Which legislation supports cybersecurity?
- What are the major stages of NCS development?

8. Implementation Language

The ontology is implemented using the Web Ontology Language (OWL).

9. Future Extensions

Future extensions of the ontology may include:

- More detailed specification of specific cyber threats and vulnerabilities.
- Integration with other relevant ontologies such as those for cybercrime, critical infrastructure and data privacy.
- Support for multilingual representations.