Developing modelling and simulation standards for including the cyber domain in military training and exercises

Boltjes, Bert; Maathuis, Clara; van den Berg, Tom; Gouweleeuw, Rudi

Publication date
2019

Document Version
Final published version

Published in
2019 Simulation Innovation Workshop

Developing Modelling and Simulation Standards for Including the Cyber Domain in Military Training and Exercises

Bert Boltjes
bert.boltjes@tno.nl
TNO Defence Research, The Hague,
The Netherlands

Clara Maathuis
clara.maathuis@tudelft.nl
Delft University of Technology, TNO Defence Research, Netherlands Defence Academy
Delft, The Netherlands

Tom van den Berg
tom.vandenberg@tno.nl
TNO Defence Research, The Hague,
The Netherlands

Rudi Gouweleeuw
rudi.gouweleeuw@tno.nl
TNO Defence Research, The Hague,
The Netherlands

Keywords:
Cyber, Computational ontology, Cyber effects, Cyber domain engineering, Cyber reference FOM

ABSTRACT*: As cyber operations are evolving to become a major military enabler, cyber activities and their resulting effects should also be represented in simulation environments. Currently much effort is being put into creating simulation environments to enable the simulation of cyber operations at the technical (network) level. At this level the focus is on detection and exploitation of vulnerabilities on the offensive side and on prevention, detection and mitigation of malicious intrusions on the defensive side. Simulations at this level facilitate training of and competition between cyber technicians. Typical examples are so-called "Capture-the-flag" events. However, cyber operations also have an important impact at the tactical, operational and strategical level, but so far little effort has been put into integration of cyber operations and their effects at these levels. What there is, is mainly limited to degrading some of the tactical data communication or switching off C2 systems or simulators. A standard approach is required to integrate offensive and defensive cyber activities and their resulting effects in simulation environments in a timely, efficient, interoperable, and cost-effective manner.*

A first requirement for a standard approach is to describe the elements of systems that can be affected by cyber operations, their characteristics, the way they interact, offensive and defensive cyber activities and the effects they can have on operational capabilities. For this purpose, taxonomies and ontologies for cyber operations have been described in the literature, but they only cover elements of cyber operations (tailored to specific attacks, threats, vulnerabilities et cetera). All these attempts serve a specific research purpose and there is limited or no coherence between them. With only one exception that we know of, the research results have, beside papers, not been available for further development. Open sources and standards are lacking which hinders further development of interoperable products for introducing cyber operations in modelling and simulation for training and experimentation as they do exist for Land, Sea, Air, and Space. An ontology for the cyber domain is – however – important to the development of (re-usable) simulation conceptual models, simulation scenarios and simulation data exchange models. An ontology provides amongst others consistent naming, meaning, relations and interactions of the various elements used in the different models.

TNO Defence Research is strongly involved in many standardisation activities for modelling and simulation in the military domain. In addition, as part of a doctoral research project (Technical University Delft, TNO Defence Research, and Netherlands Defence Academy (NLDA)) aimed at assessing the effects of cyber operations in support of targeting decision making that avoids collateral damage. In this context computational ontologies have been developed

to describe cyber operations and to represent and reason around the necessary knowledge to assess the effects of cyber operations. These ontologies can be regarded as a (knowledge-based) simulation environment resulting from empirical research and design studies in the military cyber domain.

This paper describes a development method, focussed on the construction of a cyber operations ontology for training and exercises, and the initial steps toward a cyber simulation data exchange model.

1 Introduction

Cyberspace can be defined as the environment composed of means and services, in which digital data are stored, processed and/or transferred. Cyberspace has become a new dimension added to the traditional battlefield, in other words a real threat or a real option to be considered by military actors when trying to achieve their military goals and objectives by conducting cyber operations. To underline the importance, NATO has designated cyber space as the fifth domain of military operations, next to air, land, sea and space. cyber operations can have either a supportive or an amplifying role to other military operations, and are defined as parts of military operations (i.e. activities) or independent military operations [1] that produce effects on the targeted systems or actors, as well as on other collateral systems or actors [2], [3]. To be able to understand cyber operations and their effects (impact) properly, methods and models need to be proposed, created and validated.

The modelling and simulation of cyber operations is a relatively new domain where most effort is put in the simulation of cyber operations at the technical (network) level. There is not much literature available on modelling and simulation of cyber operations at the tactical level and what effects are most relevant in a tactical training environment. A recently started research project at TNO explores this new domain with the aim to better understand the cyber effects that are important in a tactical training environment, develop a domain model that can be used as authoritative reference for the simulation of cyber operations at the tactical level, and define building blocks and a simulation data exchange model [4] that can be used to develop simulation environments for cyber operations. Technical aspects on how cyberattacks are actually carried out, as they are in so-called cyber ranges, are beyond the scope of the research project. It is sufficient when the trainees can be exposed to the observable effects of cyberattacks, such as a manipulation of data or functionality (a violation of the integrity of data or applications) or a temporary or permanent denial of access to data or applications (violation of the availability of data or applications). It will force them to make tactical decisions, such as shutting down systems, use alternative systems or keep on using degraded systems. In tactical training environments it is generally not required that trainees will technically analyse a cyberattack or patch targeted systems. In this context it is for example not required to simulate vulnerabilities that can be exploited, nor the footprint malware leaves on targeted systems. It is not about the technical “how” of cyber operations. Although the scope of the research project is limited to cyber operations at the tactical level, the methods and structures used form a basis for application in cyber technical training environments in the future.

This paper describes a four-stepped development method to achieve the goals of the research project and presents the preliminary results of the first two steps, namely objectives of the cyber operations domain and a domain model in the form of a cyber ontology.

The remainder of this paper is structured as follows. Section 2 briefly discusses related work on M&S of cyber effects, taxonomies and ontologies. Section 3 discusses a four-stepped development method and how the results of this method relate to the engineering of individual simulation environments for the simulation of cyber operations. Section 4 discusses briefly the cyber operations domain objective of this research. In section 5 the computational ontology for cyber operations developed in our previous research is outlined. This section also provides an example in the form of a use case that uses a small part of the developed ontology. Section 6 concludes this paper with a summary of conclusions and the next steps in our research.

2 Related work

This section provides an overview of (known) related work in the field of cyber operations modelling and simulation at the tactical level.

2.1 M&S for Cyber Defence

The NATO Modelling and Simulation Group (MSG) 117 ("*Exploiting Modelling and Simulation to Support Cyber Defence*") has explored the field of M&S in support of cyber defence [6]. The purpose of that activity was to investigate and recommend what aspects of cyber defence can be supported with M&S. The activity focussed on education, training, exercise, evaluation, concept and CONOPS development and their validation, cyber threat assessment, enhancing cyber capabilities and technical solutions. Their report was submitted at the end of 2015. A follow-on activity was started July 2018 as Task Group MSG-170 ("*Top Ten Cyber Effects for Campaign and Mission Simulations*") [7]. This specialist team was tasked to answer the question, "*if one wants to simulate cyber effects in mission training and exercise, which effects should one start with?"*.

The focus of MSG-170 is on effects and not on operations that cause them nor the ways the attack is delivered. The key objectives and expected achievements of MSG-170 are:

- Development of a "top ten" list of cyber effects of attacks/countermeasures and counter effects that are most relevant for a mission training environment. Categorisation of these effects will be done at a technical, mission and campaign level. The study will address the required fidelity levels of the simulated effects;
- Evaluate and rank the credibility and likelihood of the effects in the "top ten" list;
- Gain insight on how simulation of the attacks/effects can support NATO cyber defence efforts;
- Collect and study reference examples and/or available implementations;
- Obtain insights from invited subject matter experts on the current status of research and best practice on how to achieve/implement effective representations in mission rehearsal and training.

Additionally this activity will also start to consider possible requirements for a NATO cyber HLA FOM Module. Their technical evaluation report, recommending work for future activities, and possibly the requirements for a cyber FOM are expected in August 2019.

Other related activities are NATO Task Group MSG-145 ("*Operationalization of Standardized C2-Simulation Interoperability*") [8] and the SISO "*C2SIM*" Product Development Group (PDG) [9] to standardise C2-Simulation interoperability. There is interest in introducing cyber effects in the interoperation between C2 systems and simulation, see for example [10]. Another initiative currently underway is the SISO "*Cyber M&S*" Study Group (SG) [11] which studies how to develop a widely accepted Cyber Reference Data Exchange Model (CyRDEM). Although these activities were started more or less separately, MSG-170, MSG-145, and the SISO Cyber M&S SG are sharing results, thus creating more synergy. Together these groups form a large community and give the research momentum in M&S for cyber.

2.2 Taxonomies and ontologies for the cyber domain

An introduction to taxonomies related to the cyber domain is given in the 2008 IEEE survey of Igure et al [12]. The report of Bernier [13] of the Defence R&D Canada describes in detail a taxonomy for military activities and cyber effects. According to Igure et al: *"A [cyber vulnerability] taxonomy classifies the large number of vulnerabilities into a few well defined and easily understood categories. … Such a classification can serve as a guiding framework for performing a systematic security assessment of a system. In fact, one of the goals of producing taxonomies of vulnerabilities has been to develop automated tools for performing security assessment."*

A Sandia labs report defines that a common language consists of terms and taxonomies (principles of classification) which enable the gathering, exchange and comparison of information [14]. The report states that categories in a taxonomy for computer security incidents exhibit the following characteristics: mutually exclusive, exhaustive, unambiguous, repeatable, accepted, and useful. These characteristics also hold for ontology classes.

The envisioned "automated tools" by Igure et al can be realised by creating an ontology in a relational database that can be queried. Such an ontology will build up on the classification of entities and their types of relationships. However, a very large number of papers on taxonomies related to Communication and Information Systems (CIS) and security/ cyber can be found in the literature [15]. However, as Igure et al states: "*Many taxonomies of attacks and vulnerabilities have been published over the years, but there is still no standard or universally accepted taxonomy. Several different taxonomies exist because each is mostly applicable only to a particular field of interest*."

The purpose and usefulness of an ontology for M&S of cyberattacks and their effects is discussed in the papers of Turnbull et al from 2015 [15], [17]. Their computational ontology and two use cases are open source and available on GitHub [18]. As stated in [15]: "*Public availability makes the ontology unique in that it is available for critique and analysis*". This is in stark contrast with the results of the many other research and development efforts in cyber ontologies [19] which unfortunately resulted in research papers with only description of the ontologies, each with their own terms, definitions and methodology.

The essential elements related to cyber operations were identified, defined and represented by Maathuis et al in [1] as a computational ontology for cyber operations. This work was continued in [2] and [3] where a knowledge-based model for assessing the effects of cyber operations and a supportive assessment methodology were proposed. The ontology introduced and described in [2] depicts and represents the knowledge around the intended and unintended effects of cyber operations, and is exemplified on three case studies of real cyber operations executed in Georgia and Ukraine in 2008, 2015 and 2017, respectively. One of the extensions considered in [2] is in the line of developing a FOM module for cyber that would facilitate the integration of cyber activities and their effects in distributed simulations of military operations. Accordingly, this model represents the starting point of this article and is elaborated in section 5.

Our research effort described in this paper is intended to take a step in the direction of creating a common understanding and an ontology that can serve as a basis for a future standard for further research and development. It is our intention that the computational ontology for cyber operations is made available for the research community in the nearby future.

3 Development method

This section describes the four-stepped development method in our research project (sub section 3.1), and how the results of this method relate to the engineering of individual simulation environments for the simulation of cyber operations (sub section 3.2).

3.1 Cyber simulation domain engineering

The development method used in our research project consists of the following four steps as described below and illustrated in Figure 1. Note that this paper focuses on steps 1 and 2. Steps 3 and 4 are beyond the scope of the current paper.

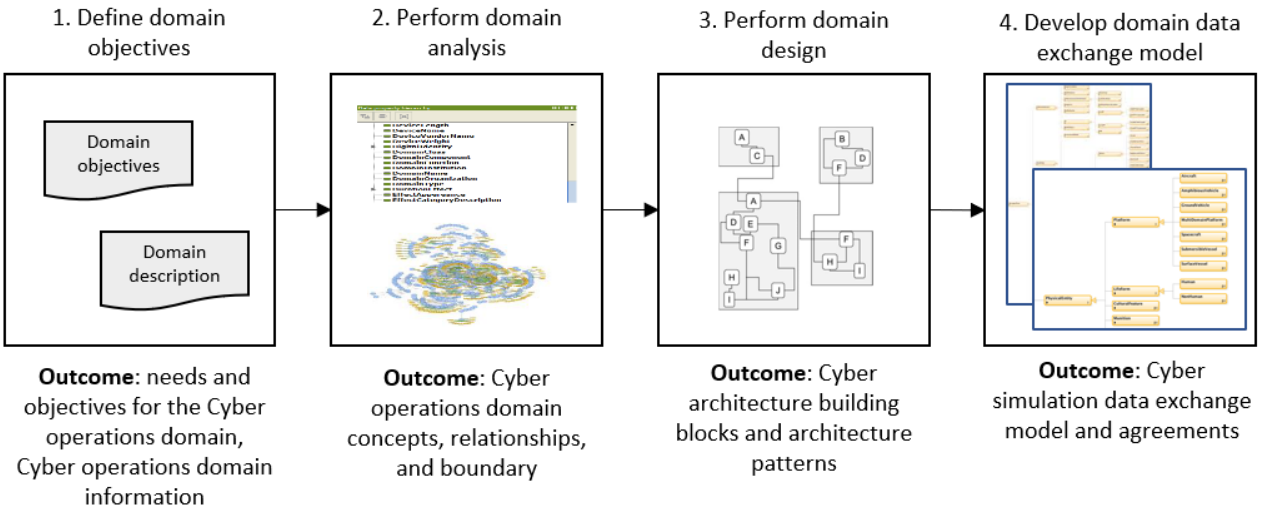

Figure 1: Stepped approach to develop a cyber Simulation Data Exchange Model (SDEM).

- Step 1: **Define domain objectives**: identify the needs and objectives for the cyber operations domain. In the research project we are interested in modelling the activities and resulting effects of cyber operations at the tactical level (see section 4).
- Step 2: **Perform domain analysis**: define the boundaries of the cyber operations domain, build domain models and construct a domain vocabulary. In this research project the domain models and vocabulary are captured in a knowledge model (ontology, see section 5). The knowledge model is built in four phases: Requirements and Knowledge acquisition (the necessary information and requirements for building the model are gathered), Design (the knowledge collected is prepared to describe and represent the effects), Implementation (the knowledge model is implemented in Protégé), and Validation (the knowledge model evaluated based on subject matter expertise (see [2]). A cyber glossary, that forms a foundation for a common understanding, can be found in the report of NATO MSG-117 [6].
- Step 3: **Perform domain design**: define the domain architecture and specify the cyber architecture building blocks and patterns that can be used to create the design, and to select or develop the software applications that will make up the cyber operations simulation environment. Architecture building blocks (ABBs) are the elements that constitute the domain architecture. Each ABB has attributes that specify its purpose and function using the vocabulary developed in the previous step. An Architecture Pattern (AP) is a high-level guideline for composing ABBs ([19],[27]). In this step use cases (including as far as available: simulation conceptual models, simulation scenarios and applications) for cyber operations simulation are studied to identify common cyber building blocks and patterns for the domain. This step and the next step are in line with the activities of the SISO Cyber M&S Study Group (see [21]) where a similar approach is followed for these two steps.
- Step 4: **Develop domain data exchange model**: identify the potential information that may be exchanged between cyber building blocks and develop the cyber simulation data exchange model (SDEM). The cyber SDEM serves as a reference for the simulation data exchange model of individual simulation environments in the cyber operations domain. The exact format of the cyber SDEM is to be determined later in the research project. E.g. the cyber SDEM may take the form of an HLA Federation Object Model (FOM) - i.e. cyber reference FOM for the simulation of cyber operations in an HLA federation - or may be described in a simulation architecture-neutral way.

The four steps in the development method are based on the Domain Engineering Process activities described in [22], [23], and [25]. In [23] domain engineering is defined as "*a reuse-based approach to defining the scope (i.e., domain definition), specifying the structure (i.e., domain architecture), and building the assets (e.g., requirements, designs, software code, documentation) for a class of systems, subsystems, or applications*." The building of assets is not

included in our four steps as we are in this research mainly interested in the activities that lead to the data exchange model.

It is interesting to look at the definitions for domain model and domain architecture used by these standards, since these definitions are important to the work that we perform in the research project. In these standards a *domain model* is defined as: "*A product of domain analysis that provides a representation of the requirements of the domain. The domain model identifies and describes the structure of data, flow of information, functions, constraints, and controls within the domain that are included in software systems in the domain. The domain model describes the commonalities and variabilities among requirements for software systems in the domain*."

In our research project we have opted to use a knowledge model (ontology) as domain model. The knowledge model describes the structure of data, relationships, constraints, as well as the vocabulary. Since the research project is ongoing, we have yet to find out if the information in the knowledge model is sufficient for the follow-on steps 3 and 4, and where more information may need to be added.

The standards define a *domain architecture* as: "*A generic, organisational structure or design for software systems in a domain. The domain architecture contains the designs that are intended to satisfy requirements specified in the domain model. The domain architecture documents design, whereas the domain model documents requirements. A domain architecture: 1) can be adapted to create designs for software systems within a domain, and 2) provides a framework for configuring assets within individual software systems*."

As mentioned earlier in this section, the domain architecture consists of cyber architecture building blocks and architecture patterns, stating the functions that implementations of these building blocks or patterns need to perform. Architecture patterns serve as implementation-independent references for designs at the application level, whereas design patterns provide more concrete information for refining the components of a software application [26]. The domain architecture in our research project will focus on architecture patterns for cyber applications rather than design patterns of cyber applications.

3.2 Cyber simulation application engineering

The four steps of the development method are defined such that they align with the first four steps of the Distributed Simulation Engineering and Execution Process (DSEEP) [4]. The DSEEP is a recommended practice for the development and execution of a simulation environment. The DSEEP is independent of a particular simulation environment architecture and provides a consistent approach for objectives definition, conceptual analysis, design and development, integration and test, simulation execution, and finally data analysis. The DSEEP identifies a sequence of seven basic steps as illustrated in Figure 2; note that by no means these steps are intended to be performed strictly sequentially. The same DSEEP steps should be applied to the engineering of a simulation environment for the simulation of cyber operations.

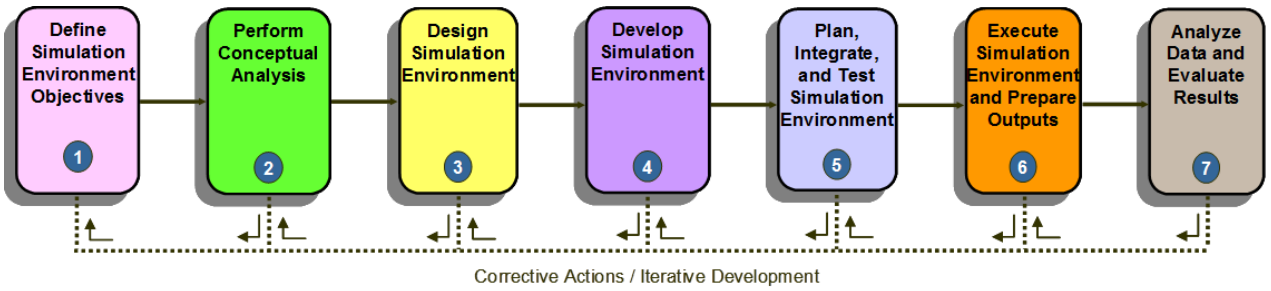

Figure 2: DSEEP steps.

So, where the DSEEP in our context is focussed on the engineering of a simulation environment for cyber operations, i.e. *cyber simulation application engineering*, the four steps of the development method in our research are focussed on *cyber simulation domain engineering*. The relationship between the two engineering processes is shown in Figure 3, where we only look at the first four steps of the DSEEP. In these four steps the simulation environment architecture development takes place, which is of interest to both processes. For the DSEEP more information on architecture development can be found in [28].

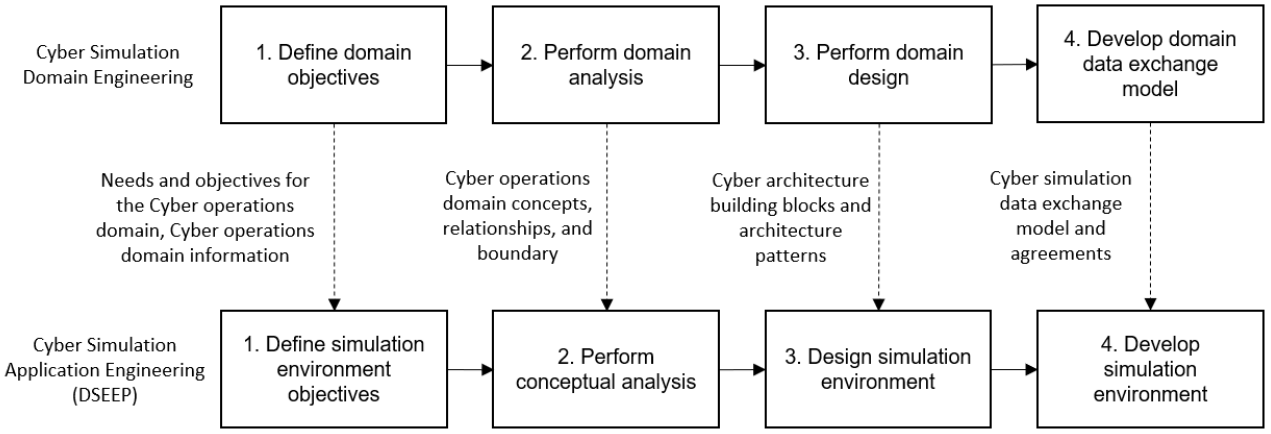

Figure 3: Cyber simulation domain engineering (top) and cyber simulation application engineering (bottom).

Figure 3 illustrates the information flow from the cyber simulation domain engineering process to the cyber simulation application engineering process. The domain engineering process is generally invoked just a few times for the domain, but the application engineering process (i.e. the DSEEP) is invoked for the engineering of each individual simulation environment within the domain. Fortunately, the DSEEP already provides several "hooks" for receiving domain related information, which makes it easy to connect the two processes as illustrated in the figure:

- In step 1 the cyber application engineer uses the cyber operations domain information and the objectives for the domain in the needs and objectives settings for his simulation environment.
- In step 2 the cyber application engineer uses the language and concepts of the cyber operations domain models as authoritative domain information to develop the simulation conceptual model and simulation scenario for his simulation environment.
- In step 3 the cyber application engineer uses the cyber architecture building blocks and patterns for the design of the simulation environment and for the selection and development of software applications. The engineer also uses M&S repositories for retrieval of existing cyber simulation assets for the domain.
- In step 4 the cyber application engineer uses the cyber simulation data exchange model as a reference for the development of the data exchange model for his simulation environment.

Following this approach, the architecture artefacts from the cyber simulation domain engineering process also facilitate a higher level of interoperability between models developed in the cyber simulation application engineering process, i.e. by using a common domain model (ontology in our case), building blocks, data exchange model, etc.

In summary, the development method used in our research project concerns the cyber simulation domain engineering process as described in this section. We follow these steps to develop a cyber SDEM and other architecture artefacts that support the development of individual simulation environments in the cyber operations domain. In the remainder of this paper we will present the preliminary results of step 1 and step 2 of the domain engineering process: objectives and analysis of the cyber operation domain.

4 Cyber operations domain objective

The domain objective of this research runs in parallel to those of MSG-170, which focusses on cyber operations at the tactical level. As stated by MSG-117: "*There is currently little representation of cyber in campaign and mission level exercises, what there is being mainly limited to degrading or switching off C2. Whilst this can be a quick and effective way of creating a basic representation of the impact on a mission of a cyberattack, it does not cover the full range of potential impacts. A better understanding is needed of effects that should be represented.*" One of the tasks of MSG-170 is to investigate how to create effective and credible representations of cyber effects and countermeasures for simulation in campaign and mission level exercises. Another task of MSG-170 is to investigate and document the requirements for a cyber HLA FOM module for the simulation of cyber effects.

Cyber effects can be defined at several levels of (technical) detail. For training and exercises a first categorisation can be made based on the three main concepts of information assurance: confidentiality, integrity and availability. Offensive cyber operations can violate each of these properties of data, applications or (physical) systems:

- A violation of confidentiality means that information is made available or disclosed to unauthorised individuals, entities or processes. An applicable cyber effect could be named "disclose".
- A violation of integrity means that information is altered in an unauthorised or undetected manner. An applicable cyber effect could be named "manipulate". Changing the locations of entities displayed on an electronic map or changing the content of an observation report are examples of such manipulation.
- A violation of availability means that information is made unavailable (inaccessible or unusable) when required by authorised individuals, entities or processes. An applicable cyber effect could be named "deny". Not being able to log in anymore on a system or a computer program that does not start anymore are typical examples of such denial. This cyber effect can be further broken down into subcategories, for example into:
    - Degrade: temporarily or permanently deny access to, or deny use of a part of data, applications or (physical) systems. This also includes a degradation of performance, where data becomes available after a certain delay.
    - Disrupt: completely but temporarily deny access to, or deny use of data, applications or (physical) systems.
    - Destroy: completely, permanently and irreparably deny access to, or deny use of data, applications or (physical) systems.

      These effects can be applied to for example:
        - Strategic Communications and Information Systems (CIS).
        - Tactical communications (i.e. disruption of the UAV video downstream or its control upstream).
        - Position Navigation and Timing services (i.e. GPS spoofing).

Although cyber effects are commonly associated with cyberattacks, also defensive cyber operations can result in relevant effects in cyberspace, such as "secure" (to protect the confidentiality, integrity and availability of designated (parts of) systems against cyberattacks), "contain" (to render a cyberattack incapable of further spreading in a system), "neutralise" (to render a cyberattack incapable of further affecting the confidentiality, integrity and availability of (parts of) systems) and "recover" (to remove inflicted effects resulting from a cyberattack). Further levels of detail can be specified, see for example [2].

MSG-170 is currently working on a method to rank these effects. The focus of MSG-170 is on effects and not on operations that cause these effects, nor the ways a cyberattack is delivered. The scope of the research described in this paper is broader, however. It includes a knowledge-based model that describes the actors and their relations through a computational ontology. The ranked list of cyber effects as well as the ontology serve as basis for the creation of a cyber DEM and associated agreements on its use.

5 Cyber operations domain analysis

This section introduces an ontology for cyber operations and provides an example in the form of a use case.

5.1 An ontology for effects of cyber operations

Section 3 has proposed a way for domain analysis. This was done by designing, developing and validating an ontology for cyber operations embedded in a knowledge-based model aiming at assessing the intended and unintended effects of cyber operations [2]. This research was presented at the 12th NATO OR&A Conference in 2018, and the embedded ontology is further elaborated. The development of an ontology represents a standard and optimal approach in Computer Science and Artificial Intelligence fields and is intensively applied in other domains such as biology and medicine. The reasoning behind the choice to develop an ontology rests on considering the fact that ontologies allow knowledge to be defined, (re)used, and shared between different domains, communities and/or actors. Additionally, they are useful to facilitate or strengthen situational awareness and decision making in different domain applications. Furthermore, the proposed ontology was born from the necessity of defining, classifying, and assessing the effects of cyber operations for targeting purposes relying on two main fundamental causes: i) the fact that cyber operations became a real option to achieve military objectives, and ii) the lack of understanding, expertise, and transparency reflected in the limited amount of existing (open) data, frameworks, methodologies, and models that could be used. To reach out to this knowledge model (proposed ontology), a Design Science Research [23] approach was considered using Knowledge Engineering and Ontology Engineering methodologies [24]. The ontology was developed using OWL (Web Ontology Language) due to its higher level of expressivity and machine interpretability when compared with other languages such as UML (Unified Modelling Language). This model is based on extensive technical – military empirical and design research founded on data and requirements collected and analysed from seven case studies of cyber operations (five real incidents and two simulated incidents), scientific literature and military doctrine, field work in joint military exercises, and three rounds of interviews with forty military Commanders [2]. Furthermore, the proposed ontology was validated from a dual perspective (technical and tactical/operational) and reached its final form as a medium – large ontology (i.e. 400+ classes and 400+ properties) structured in four levels. The levels are defined in Table 1 and are described below:

Table 1: Cyber operations effects ontology levels.

Level number	Level name
1	Upper Class Level
2	Child Class Level
3	Individual Level
4	Property Level

The *Upper Class Level* (level 1) contains the upper classes that are depicted in Figure 4. These upper classes are connected by relationships between them illustrated as coloured arrows. For instance, the relation marked with red in Figure 4 is named *hasImpactMeaningOn* and connects an individual of the class *EffectOn* with one of the class *TargetOrAsset*. It is important to stress that the more in depth these classes are represented together with their child classes, the more relationships will exist. Furthermore, the upper classes are defined as follows:

- Class *Actor* comprises all the participants involved intentionally or not in a cyber operation, starting from the ones that are responsible for the planning, design or execution of a cyber operation, and ending with the ones who, or whose systems, are affected by a cyber operation, such as opponents, allies, friendly and neutral actors.
- Class *CyberWeapon* consists the cyber capacities or means deployed in a cyber operation to engage targets [5].
- Class *TargetOrAsset* embodies the entities (human or object, both civilian or military) that are being (un)intentionally and (in)directly impacted by a cyber operation.
- Class *EffectType* contains the type of effects that impact targets in a cyber operation, for instance *Degradation* and *Injury*.
- Class *EffectCategory* incorporates useful information for classifying these effects as Collateral Damage (i.e. unintended effects appearing (mainly) on civilians and civilian systems) and Military Advantage (i.e. intended effects contributing to achieving the military mission, appearing generally on military actors and systems) in a cyber operation [3].
- Class *EffectOn* holds information regarding aspects and qualities (e.g. software or data) of entities (targets or collateral assets that are affected by the effects of cyber operations, such as *Confidentiality*, *Functionality* and *Stability*).
- Class *EffectRole* refers to the contributing character of an effect in a cyber operation and even broader than that in the sense of supporting or amplifying the effects of a military operation that embeds the current cyber operation or a different military operation.
- Class *Metric* contains a series of metrics defined at hardware, software and military levels in order to facilitate measuring the effects of a cyber operation.

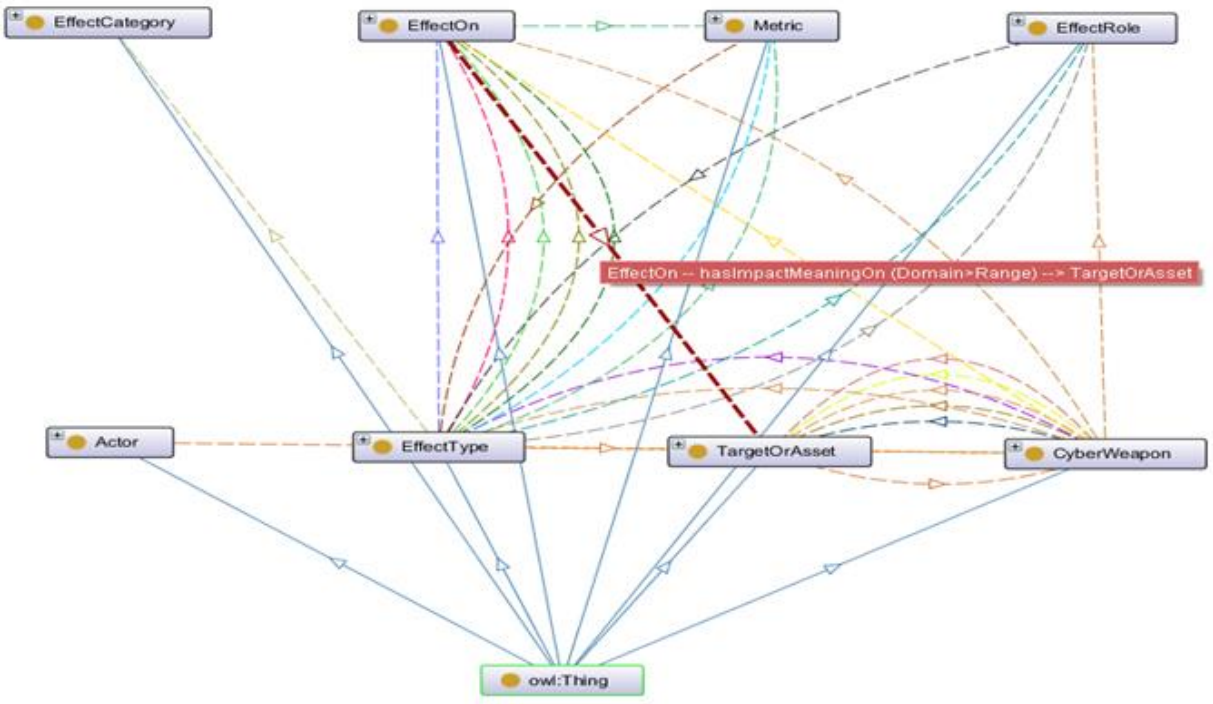

Figure 4: Cyber operations effects upper classes represented using OntoGraph.

The C*hild Class Level* (level 2) is composed by the child classes of the already defined upper classes. Figure 5 illustrates the upper class *CyberWeapon* [2] with its direct child classes: *CyberWeaponCheck, CyberWeaponReport, CyberWeaponStructure, and CyberWeaponType*, where the coloured arrows describe the subclass relationship.

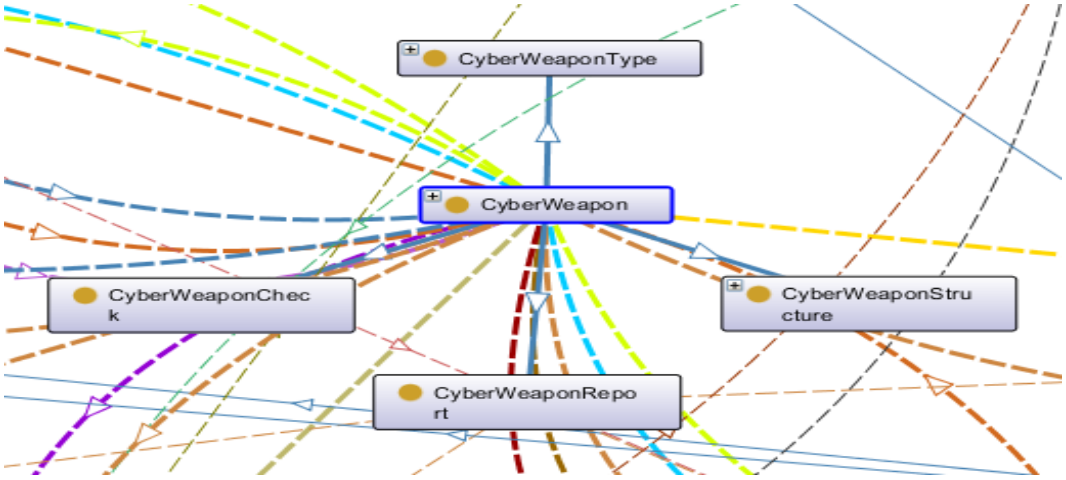

Figure 5: CyberWeapon upper-class with its direct child classes represented using OntoGraph.

Other examples of relevant child classes are:

- Class *ResponsibleActor (*subclass of *Actor* class*)* represents the actor which is responsible for planning, designing and/or employing a cyber weapon on a target in a cyber operation.
- Class *CyberWeaponType (*subclass of *CyberWeapon* class*)* illustrates different categories and types of cyber weapons such as Malware and (D)DoS.
- Class *Disturb (*subclass of *EffectType* class*)* refers to a specific type of effect that interferes or perturbs an entity.
- Class *ExploitCodeMaturity (*subclass of *Software->Metric* class*)* holds information about the likelihood of a vulnerability to be exploited.

The *Individual Level* (level 3) contains the individuals (objects or instances) of all defined classes specific for each considered use case. For illustration purposes, in Figure 6 the individuals of the class *SoftwareVulnerability* are depicted as they have been used for the cyber operations case studies conducted on Georgia and Ukraine.

Figure 6: Individuals of SoftwareVulnerability class for cyber operations conducted on Georgia and Ukraine.

The *Property Level* (level 4) embodies data properties that represent relationships between individuals and literals/data types (e.g. float or string types) and object properties that represent relationships between individuals. A selection of data properties and object properties is depicted in Figure 7 (respectively left and right). Moreover, a few properties are explained:

- Data property *EffectDiscoveryTime* reflects the moment when a specific effect is discovered and is of type (range) dateTimeStamp.
- Data property *EffectIntensity* captures the intensity of a specific effect and is represented using predefined string values such as Moderate and Severe.
- Data property *MediumTermEffect* characterises the duration of a specific effect which is considered to be in a predefined range of double values between 24 (hours) and 730.484 (hours – around one month).
- Data property *TargetOrAssetCheckMilitaryStatus* denotes whether a real world entity (human, software, physical object, et cetera) is a military target or a civilian asset.

- Object property *isExecuting* illustrates the fact that a *ResponsibleActor* individual (object) is the one which employs a *CyberWeapon* individual.
- Object property *hasEffectRole* shows that a specific effect with an *EffectType* individual has a role depicted by an *EffectRole* individual.
- Object property *isMeasuredByMetric* reflects the fact that a specific type of *EffectType* (individual) is measured by an explicit *Metric* (i.e. software, hardware or military – as individual).
- Object property *isReportingOver* shows that a *CyberWeapon* individual is reporting about different facts such as achieving an explicit *EffectType* individual on a specific aspect of a system characterised by an *EffectOn* individual.

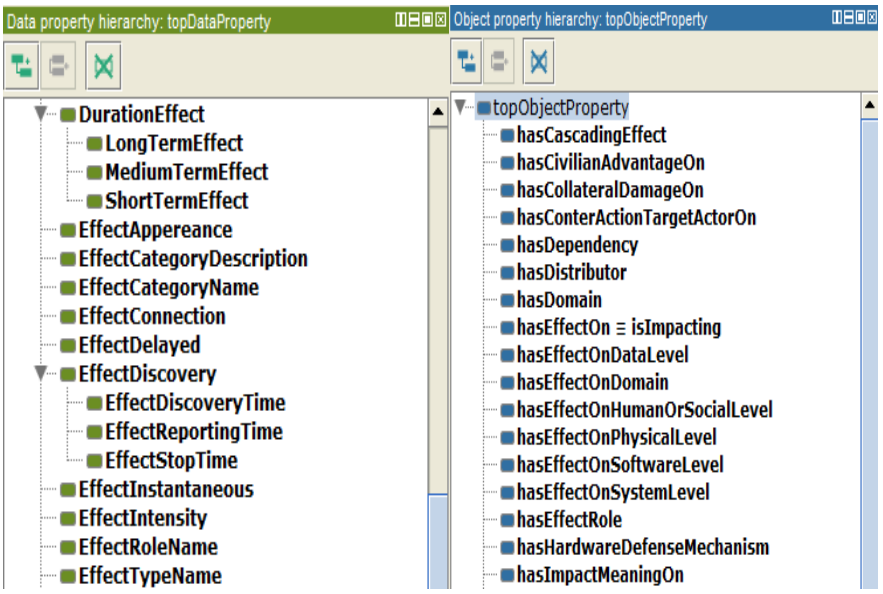

Figure 7: Cyber operations effects ontology data properties (left) and object properties (right).

5.2 Ballistic Missile Defence System (BMDS) use case

The proposed ontology is aimed at assessing the effects of cyber operations and used in conjunction with the effects assessment methodology proposed by [3]. To exemplify this model, a use case / case scenario based on the dataset and case scenario used in [3] is further presented. This use case is based on technical – military research conducted between January – May 2017, and represents a fictitious cyber operation virtually conducted for validation purposes in two steps: firstly, with nine military experts from TNO and the Netherlands MoD at TNO in June 2018, and secondly, with four military experts with international experience from and at the Netherlands MoD between June – October 2017. It is important to mention that this use case was designed taking into consideration the advice provided by the international military experts that we have consulted together with the current global security issues in which case cyber operations play a significant role (e.g. cyber operation on the Ukraine power grid, counter-terrorism, U.S. elections). In this fictitious cyber operation the country Amdasia wants to destroy the military land HQ of the country Risian by a ballistic missile. With its Ballistic Missile Defence System (BMDS) Risian has the capability to neutralise the Amdasian ballistic missile. In order to prevent Risian to defend against the attack with its anti-ballistic missiles, Amdasia conducts a cyber operation aimed to disrupt the functionality of the Risian BMDS Command and Control (C2) using a cyber weapon that exploits an existing unknown vulnerability.

The use case considers the upper classes depicted in Figure 4 without the classes *EffectCategory* and *Metric*. The following list describes the individuals (ontology level 3, see Table 1) and is illustrated in Figure 9:

- *Actor: Amdasia* (individual of *ResponsibleActor* subclass), *Risian* (individual of *TargetActor* subclass) and *Limia* (individual of *AllyActor* subclass). On the ground of an international armed conflict ongoing in Risian, Amdasia

decides to launch a ballistic missile attack on the military land HQ located in the capital of Risian. However, Risian has a BMDS procured from Limia which is a neutral country in this conflict, but ally to Amdasia.

- *TargetOrAsset*: *AntiBMOfRisian* (individual of *TargetOrAsset* class via BMDSC2) represents the anti-ballistic missile that Risian intends to launch in response to Amdasia's missile attack.
- *CyberWeapon*: *CWPOnBMDSC2* (individual of *CyberWeapon* class) disrupts the functionality of the Risian Ballistic Missile Defence System C2 software based on exploiting an existing unknown vulnerability implanted during the design phase by an insider. In this way, when the Risian anti-ballistic missile is launched, a destruction message from the BMDSC2 initiates the self-destruction in the boost phase. Consequently, the Risian anti-ballistic missile will not reach its target – the ballistic missile launched by Amdasia.
- *EffectType*: individuals such as *AlterRisianCivilianData, InfluenceRisianFutureMO* (MO stands for Military Operation), *and InfluenceRisianDefence* (individuals of *AlterOrManipulate* subclass); *DisruptionBMDSC2* (individual of *Disrupt* subclass); *InjuryRissianCapitalPopulation* and *InjuryRisianCapitalSurroundingsPopulation* (individuals of *MentalInjury* and *PhysicalInjury* subclasses); *DeathRisianCapitalPopulation* and *DeathRisianCapitalSurroundingsPopulation* (individuals of *KillOrLossOfLife* subclass). These effects are aligned with the ones already introduced in Section 4 of this article.
- *EffectOn*: individuals like *FunctionalityOfAntiBMOfRisian, FunctionalityOfBMDSC2, FunctionalityOfBMDSC2Plans,* and *FunctionalityOfBMDSC2Systems* (individuals of *Functionality* subclass); *IntegrityOfBMDSC2, IntegrityOfBMDSC2Data, IntegrityOfBMDSC2Plans,* and *IntegrityOfBMDSC2Systems* (individuals of *Integrity* subclass).
- *EffectRole: SupportingMOOfAmdasia* (individual of *EffectRole* class). The role of this cyber operation is to support the current military operation conducted by Amdasia on Risian.

Figure 8: A selection of individuals from the cyber operation Use Case Simulation conducted on a BMDS.

For this use case 98 individuals were created considering the data collected and the results presented in [3], and a selection of them is illustrated in Figure 8. Moreover, a caption of some of the important results of this simulation are presented in Figure 9.

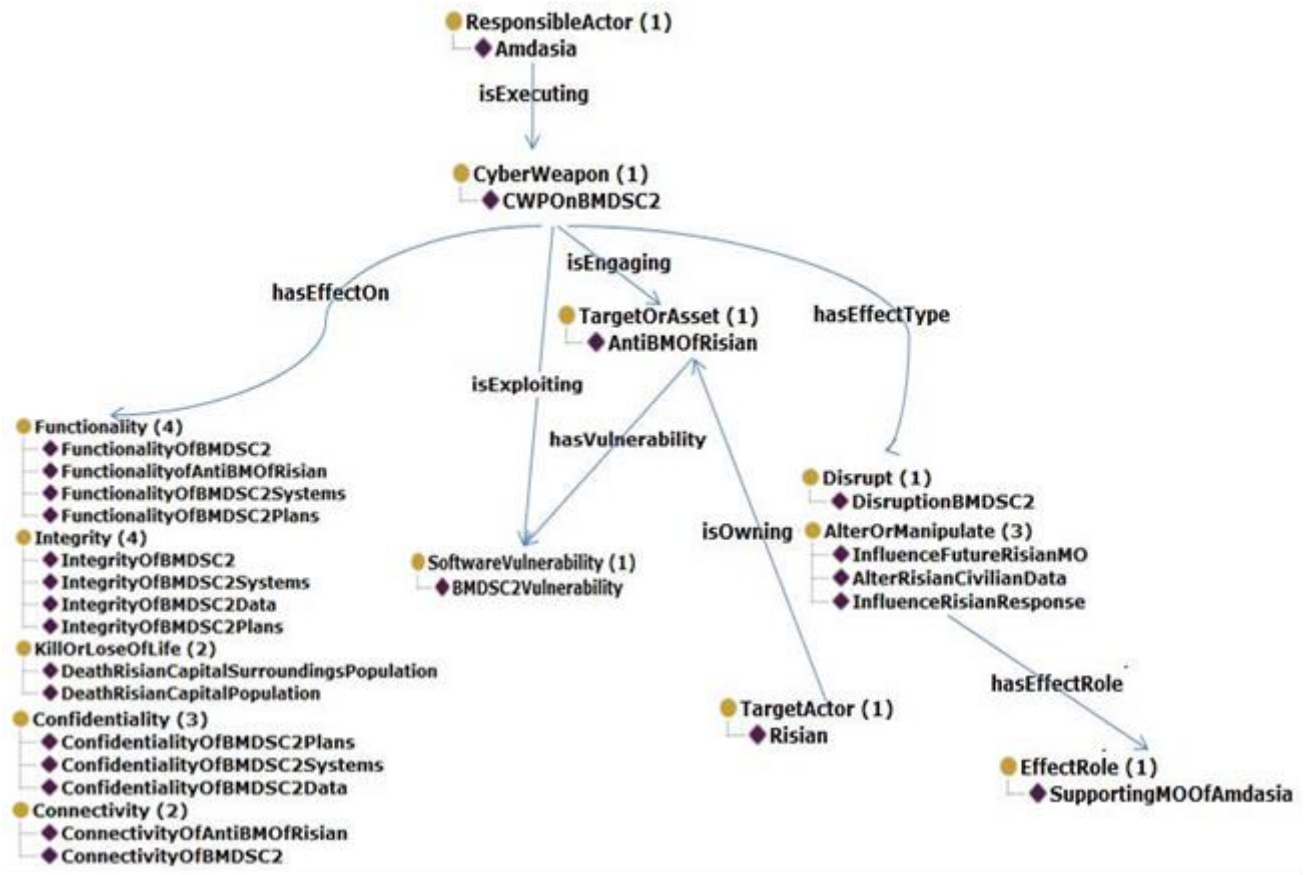

Figure 9: A selection of classes, individuals and relationships from the fictitious cyber operation conducted on a BMDS.

The selected results presented in Figure 9 reflect the effectiveness of the proposed ontology to be applied on both real cyber operations incidents (e.g. conducted in Georgia and Ukraine), as well as on simulated incidents, such as the one presented in this section. Moreover, [3] considers a more detailed description of the intended and unintended effects produced by this fictitious cyber operation. Although the approach that was followed in designing and implementing this model was multidisciplinary or better said, transdisciplinary (technical - military), this model has a high degree of granularity from a technical point of view. However, the proposed ontology can easily be reduced and used from a tactical perspective by using entities such as the classes located at upper class level or the first generation of child classes of the upper classes. Moreover, taking into consideration the flexibility that such a model embeds, operations such as alteration, addition and extraction of entities are always possible.

6 Summary, conclusions, and next steps

6.1 Summary and conclusions

The research project described in this paper explores the new domain of M&S of cyber operations for training and exercises with the aim to better understand the cyber effects that are important in a tactical training environment, develop a domain model that can be used as authoritative reference for cyber operations simulation at the tactical level, and provide cyber building blocks and a simulation data exchange model that can be used to develop cyber simulation environments. The research project defined a four-stepped approach to achieve these goals and the preliminary results of the first two steps are described in this paper. The results are in summary:

Step 1 - domain objectives: the purpose of this step is to provide a list of cyber effects that is important for a tactical training environment. An important source of definition of cyber effects consists of national and international doctrinal publications on cyber operations. Especially relevant might be the NATO Standard AJP 3-20 (Allied Joint Doctrine for Cyberspace Operations) which is currently in development. Work in this step is thus ongoing and is performed in parallel to NATO MSG-170, which focusses on cyber operations at the tactical level. Several potential examples for cyber effects are listed.

Step 2 – domain analysis: the purpose of this step is to define a domain model and construct a vocabulary for the modelling of cyber operations. Similar to step 1, this step is an ongoing multidisciplinary/transdisciplinary research. Knowledge models for cyber operations and their effects represented in the form of computational ontologies have been designed, developed, validated, and presented in several publications by Maathuis et al. in [1] and [2], respectively. The cyber operations ontology [2] provides a set of concepts and definitions (vocabulary) together with relationships between them by modelling cyber operations at all warfare levels: strategic, operational and tactical. It aims at assessing the intended and unintended effects (e.g. Collateral Damage) in order to support targeting in cyber operations. As exemplification, this paper contains a description of its application in a typical use case of a fictitious cyber operation. Furthermore, the ontology will evolve as more use cases are conducted and represented.

Preliminary conclusions from our research are:

- The computational ontology developed for operations in the cyber domain is a valuable base for describing building blocks and developing a cyber Simulation Data Exchange Model (SDEM).
- The ontology is also valuable to individual simulation environments, providing a common authoritative reference for concepts and relationships in simulation conceptual models and simulation scenarios for cyber operations. The ontology has been validated, is extendable, and can be used to instantiate specific use cases and scenarios.
- Although a few use cases are available, a larger set of use cases will obviously be helpful to support the work in steps 3 and 4.
- So far the development method has helped us structuring our research activities quite well. It is expected that this applies also to the follow-on steps 3 and 4.

6.2 Next steps

Our work will continue in steps 1 (domain objective) and 2 (domain analysis): description of relevant cyber effects and further improvements and additions to the domain model (ontology). At the same time steps 3 (domain design) and 4 (develop a cyber SDEM) will start with the preliminary results of steps 1 and 2, and using any additional information still becoming available from steps 1 and 2. Tasks in step 3 include: analysis of the ontology and available use cases (for a tactical training environment), identification of building blocks, identification and allocation of functionalities and modelling responsibilities to building blocks, and transformation of functionalities to requirements. Relationships in the ontology may potentially result in required interactions between building blocks. Using the fictitious use case in this paper as a simple example, building blocks might be cyber weapon simulation and cyber damage effect simulation for the execution phase of the cyber operation. An interaction between these building blocks is for example the employment of the cyber weapon and the resulting cyber damage assessment. In this example there is a strong resemblance with the modelling in the physical domain [3].

Throughout these steps the research project will actively engage within NATO MSG-170 and the SISO Cyber M&S SG. It is the intention that the computational ontology for cyber operations is made available for the research community in the nearby future. This will be the baseline for development of cyber SDEM, which should be a joint effort of the NMSG and the SISO community.

7 References

[1] C. Maathuis, W. Pieters, and J. van den Berg, "A Computational Ontology for Cyber Operations", Proceedings of the 17th European Conference on Cyber Warfare and Security, p. 278-288, 2018a.

[2] C. Maathuis, W. Pieters, and J. van den Berg, "A Knowledge-Based Model for Assessing the Effects of Cyber Warfare", Proceedings of the 12th NATO Conference on Operations Research and Analysis, 2018b.

[3] C. Maathuis, W. Pieters, and J. van den Berg, "Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations", In *MILCOM 2018, IEEE Military Communications Conference (MILCOM)*. IEEE, 2018c.

[4] IEEE 1730-2010, "Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP)", IEEE Standard 1730-2010.

[5] C. Maathuis, W. Pieters, and J. van den Berg, "Cyber Weapons: a Profiling Framework", In *Cyber Conflict (CyCon US), International Conference on*. IEEE, p. 1-8, 2016.

[6] NATO Study Group MSG-117 for "Exploiting Modelling and Simulation to support Cyber Defence", https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16280

[7] NATO Study Group MSG-170 for "Top Ten Cyber Effects for Campaign and Mission Simulations", https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16589

[8] NATO Study Group MSG-145 for "Operationalization of Standardized C2-Simulation Interoperability", https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16062

[9] SISO Product Development Group for "Command and Control Systems - Simulation Systems Interoperation (C2SIM)" https://www.sisostds.org/StandardsActivities/DevelopmentGroups/C2SIMPDGPSG-CommandandControlSystems.aspx

[10] J. M. Pullen and J. Ruth, "Military Training in a Cyber active Environment Exploiting C2-Simulation Interoperation", SISO SIW 18F-SIW-02

[11] SISO Study Group for "Cyber Modelling & Simulation", https://www.sisostds.org/StandardsActivities/StudyGroups/CyberModelingSimulationSG.aspx

[12] Igure, Vinay M., and Ronald D. Williams. "Taxonomies of attacks and vulnerabilities in computer systems." IEEE Communications Surveys & Tutorials 10.1 (2008).

[13] M. Bernier, "Military Activities and Cyber Effects (MACE) Taxonomy," Defence R&D Canada, Centre for Operational Research and Analysis, 2013.

[14] Howard, J.D., Longstaff, T.A., A Common Language for Computer Security Incidents, SANDIA REPORT SAND2012-2427, Sandia National Laboratories, October 1998.

[15] Google Scholar returned 49,300 results on the phrase "Cyber taxonomy" (November 2018).

[16] O'Sullivan, Kent, and Benjamin Turnbull. "The Cyber simulation terrain: Towards an open source Cyber effects simulation ontology." (2015).

[17] Ormrod, David, Benjamin Turnbull, and Kent O'Sullivan. "System of systems Cyber effects simulation ontology." Winter Simulation Conference (WSC), 2015. IEEE, 2015.

[18] https://github.com/AustralianCentreforCyberSecurity/Cyber-Simulation-Terrain

[19] Google Scholar returned 32,200 results hits on the phrase "Cyber ontology" (November 30 2018)

[20] MSG-149, The NATO MSG-136 Reference Architecture for M&S as a Service, Jo Erskine Hannay, Tom van den Berg, 2017.

[21] https://www.sisostds.org/StandardsActivities/StudyGroups/CyberModelingSimulationSG.aspx

[22] Software Reuse, A Standards-Based Guide, Carma McClure, IEEE Computer Society, 2001.

[23] K. Peffers, T.Tuunanen, M. A. Rothenberger and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research", Journal of Management Information Systems, 24(3), p.45-77, 2007.

[24] A.T. Schreiber, G. Schreiber, H. Akkermans, A. Anjewierden, N. Shadbolt, R. de Hoog and B. Wielinga, "Knowledge Engineering and Management: the CommonKADS Methodology", MIT press, 2000.

[25] IEEE 12207-2008, Systems and software engineering - Software life cycle processes

[26] Pattern-Oriented Software Architecture, A System of Patterns, Volume 1, Buschmann, 1996

[27] SISO SIW 17F-SIW-018, Modelling and Simulation as a Service: Rapid deployment of interoperable and credible simulation environments – an overview of NATO MSG-136, T. van den Berg et al, 2017.
[28] SISO SIW 15F-SIW-019, Simulation environment architecture development using the DoDAF, T. van den Berg, Bob Lutz, 2015.

Author Biographies

Bert Boltjes is a specialist in modelling and simulation with a background in physics, quantum molecular dynamics and computer tomography. For TNO in the Netherlands he has worked for EU (project Driver), NATO (MSG-117 and MSG-170, co-chair), the Dutch DoD, and Defence industry on performance analysis and prediction of fixed and wireless defence communication networks. He has designed, implemented, and validated high fidelity network and radio propagation models. He is a skilled in implementing technologies to couple network simulators to other simulators, hardware and live networks. Dr. Boltjes is currently performing research in M&S for cyber, and distributed mission training with multiple levels of security.

Clara Maathuis is a PhD Researcher at Delft University of Technology, TNO, and the Netherlands Defence Academy in Cyber operations using Cyber Security, Artificial Intelligence, and Military operations/Defence Studies methods and techniques. Her background is in Computer Science and Automatic Control (BSc), Artificial Intelligence (MSc), and is specialised from an early stage in Information/Cyber Security. In the industry, she worked as a Senior Software Engineer in telecommunications (on data and voice solutions) and control systems (on automation solutions) industries.

Tom van den Berg is a senior scientist in the Modelling, Simulation and Gaming department at TNO, The Netherlands. He holds an M.Sc. degree in Mathematics and Computing Science from Delft Technical University and has a long working background in distributed operating systems, database systems, and simulation systems. His research area includes simulation systems engineering, distributed simulation architectures, systems of systems, and concept development & experimentation. Tom is a member of several SISO Product Development / Support Groups, participates in a number NATO MSG activities, and is co-chair of NATO MSG-164 (Modelling and Simulation as a Service).

Rudi Gouweleeuw has a scientific background in computer science (artificial intelligence) and is project manager at TNO, first for projects in the field of military tactical training and simulation. Later he broadened his scope towards operational analysis, aimed at measuring the effectiveness of military operations in a complex environment. Application of this knowledge is in support of policy studies, doctrine development, materiel procurement and mission evaluations. Currently he leads projects to develop scientific knowledge and expertise in order to enable the Netherlands Armed Forces to create and employ their aspired cyber capabilities.