Towards a Scenario Ontology for the Norwegian Cyber Range

John André Seem

14-12.2020 2019/07/18

Abstract

The Norwegian Cyber Range (NCR) is a security training platform, which aims to conduct full-scale exercises across three layers: strategical, tactical and technical. In NCR, most domain experts from different layers work primarily in their own fields and are not familiar with the workings of the others perspective. This results in the main challenge in NCR exercises, that is the ambiguity of the used terminology and vocabulary among the security experts in these layers. To mitigate this problem, this thesis suggests a solution by developing a scenario ontology for NCR. An ontology can solve this problem as it is an knowledge management center. A place like that would make it easier to understand each other use of these concepts. This thesis employs different research methods to designing and developing the ontology, including: literature review, ontology development, and a 2-phase evaluation of the ontology. The ontology created serves as a backbone for further studies and usage for the NCR further down the line. It shows positive results in evaluation, but still needs development when their still are limitation to the ontology. It is still a start and a viable product.

Sammendrag

Norwegian Cyber Range (NCR) er en treningsplattform for sikkerhet, som har et mål å produsere full skala øvelser over tre lag: strategisk, taktisk og teknisk. I NCR jobber de fleste domene eksperter primært til sitt eget felt og er lite kjent med perspektivene til de andres arbeid. Dette har resultert til en utfording for NCR øvelser, i at det er en tvetydighet i bruken av terimonologier og ord blant sikkerhetsekpertene i disse lagene. For å minske dette problemet, har denne avhandlingen foreslått en løsning med å lage en scenario ontologi for NCR. En ontologi kan løse disse problemene siden det er en kunskapsforvaltning senter. En ting som det vil gjøre det lettere å forstå hverandres bruk av konseptene. Denne avhandlingen anvender forskjellige forsknings metoder for å designe og utvikle ontologien, dette inkluderer: litteraturanmeldelse, ontologi utvikling og to faset evaluering av ontologien. Ontologien somer laget kan brukes som en ryggrad for videre studier og bruk for NCR. Ontologien har vist positive resultater under evaluering, men det trengs videreutvikling når det er fremdeles begrensninger i den. Det er fremdeles en god start og et levedyktig produkt.

Contents

Figures

Tables

Code Listings

Acknowledgement

I would like to give a huge thank you to my supervisors Basel Katt and Shao-Fang Wen .They where always there if needed help and even more if I tried to do more without contact. As both experts in different aspects of the thesis they always knew how to improve stuff or could discuss that with me. Though the thesis is my work it couldn't have been done without their guidance, direction or status update.
I would also like to thank core personnel in the NCR. Primarily Vasileios Gkioulos, Espen Torseth, Grethe Østby, Benjamin Knox, Stewart Kowalski and Jannis Schaefer. Their insights in the work inside the cyber range and willingness to discuss their specific layer whenever they where available helped a lot. Both in understanding their was a big difference between the personnel understanding of vital terms, but also being quite positive and interested in my thesis. Without them other perspectives or layers would been incomplete in understanding.
A final thanks to my family and my closest friends. My family for understanding that I needed the time for myself and focus on this task. To my closets friends to make sure I wasn't always doing work, but sometimes said hi to people and grow my understanding by explaining my work to them. The more they let me talk freely on this topic the more I gained ideas and understanding what I needed to do myself.

Keywords

Scenario, Ontology, development, cyber range, exercise, NCR, concepts, layers, perspective

Abbreviation

In this thesis there exits some abbreviations. Here is a list of with their full word in place 1.

Table 1: The list of abbreviations.

Word	Full word
NCR	Norwegian Cyber Range.
CQ	Competency Question.
Sparql	Protocol and RDF Query Language.
CIA	Confidentiality, Integrity, Availability
UML	Unified Model Language.
NATO	North Atlantic Treaty Organization
EU	European Union

Chapter 1

Introduction

Cyber Ranges are complex infrastructures or platforms for conducting experiments, research and exercises [1]. This is done in a closed environment where people can safely learn, try and explore their skills in cyber security. Those exercises simulate real life scenarios [2]. he Norwegian cyber range abbreviated NCR is a platform developed by NTNU. " to "The Norwegian Cyber Range(NCR) is a security training platform developed by NTNU. The NCR works on multiple levels of abstraction, called layers, as shown in figure 1.1.

These layers are the societal, digital value chains and digital infrastructure/design layers [3]. The societal layers considers the human, social, and organizational decision making. The digital value chain layer considers the tactical decision level and the relationships among various systems, and finally, the infrastructure layer deals with the technical infrastructure and design decision level. Besides NTNU, the Norwegian Center for Information Security (NORSIS) and the military are partners and essential stakeholders in the NCR project and work closely with NTNU in research and development. Below is a figure on how the NCR is divided in layers. [1]

In order to save time and resource one will reuse as much of the artifacts from previous exercises as possible, details about the execution of an exercise, topology and storyline, are stored in an object that is called a *scenario* [2].
A scenario works as an initial storyline, with foreseeable interactions of actors in a system, as well as the infrastructure design of the exercise. Designing a high quality scenarios is a costly and essential elements in an exercise preparation and correct execution [2], as well as it helps assigning initial resources required in an exercise [4]. These examples show why a scenario plays an important role in cyber ranges. On the other hand, there also needs to be a range of diversity of these scenarios, each of which touches upon different training aspects, otherwise, the training benefits of them reduces drastically [1]. However, if they are used

[1] NCR layer extraction

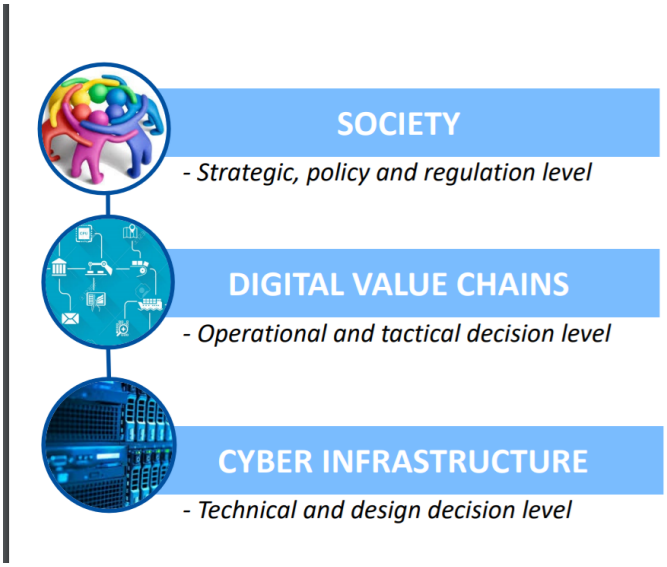

Figure 1.1: NCR layers

correctly and efficiently, they cut tremendously in preparation time and makes it possible to simulate or train more complex exercise with a complex scenario. That is something the NCR looks at it as an important area of research. And to make the NCR even more unique, they have an ambitious goal to create configurable scenarios that can work in more difficult situation over multiple layers. This can be done as NCR exercises already span across within multiple layers [3].

1.1 Problem description

The problem so far to realising that goal is that these terminologies and concepts used by these layers are either different or have different meanings. A vulnerability can mean all from a computer bug to structural problem in an organization. Is the consequences of such an attack just some networks down or the the power relay system or a NATO summit? Those are example of things that comes up in a scenario from different layers. Mostly domain expert works primarily in their fields and isn't familiar with the workings of the others perspective. And if people cant agree on vital terms it is hard to make multilayered scenarios. At least correctly formed one. And the use of one wouldn't give any more benefits than having one scenario from each layer. This also leads to the potential that scenarios build from different layers follows different standards and cant be beneficial for much than a specific problem.

If they started making these scenarios without solving this it would create at best scenarios and exercises being vague and ambiguous. At worst quite wrong scen-

arios. And with a platform to educate people in cyber range scenarios that cant happen. And a purpose of education is to gain or share knowledge of the world. And the training often happens of personnel to become cyber experts or people that doesn't know about cyber security.

A scenario like this could happen if they don't solve their problems: If NCR train personnel in these scenarios that doesn't know about cyber security from before it could make them take the wrong decisions in a real life situation. That could lead to the cyber attacks these exercises where meant to prevent. If the NCR trains up students that will become security experts in these wrong scenarios it could lead them be trained wrongly in cyber security. That could lead them to spread these wrong ideas into cyber domain and can worsen an already advanced cyber attack. All of this would be looked back at NCR and their reputation would be tarnished. It could also affect NTNU as a research institution for security. It could in worst case make the idea of cyber ranges be seen as a bad thing. And without these training platforms it wont remove the cyber attacks and maybe increase the number of successful attacks. That would lead to more work for the cyber security workforce which has a lack of personnel already.

To overcome these problems this thesis is addressing in this solution to create an ontology to expose and solve these problems. An ontology can solve this problem as it is an knowledge management center. An ontology goal is to clear up ambiguity and make clear concepts. A place like that would make it easier to understand each other use of these concepts. It could also make a framework for this concepts to be understood to mean exactly what it should mean in a scenario. As this ontology will be for making scenarios it also has a place where one can add in or create a scenario fitting to these standards solving the problem of creating scenario that isn't following the same clear structure. It would also serve as a knowledge center to find easy use certain scenario to an exercise that could be used. It would also reduce the risk for the things happening in the scenario above to happen. This is why this thesis propose the creation an ontology to solve these problems.

This research and thesis will be covering the development and production of this ontology for the NCR. Data was gathered by abstracting it from related literature and key personnel working in the NCR.

1.2 Research objective

Research objectives are concise expectations of what to achieve through the research. This research will have this objectives

Objective 1: Understand the problems NCR has for achieving their goals of multilayered scenarios.

Objective 2: Learn about ontology and be able to create a working ontology.

Objective 3: Create an ontology that can be the first step and can be developed in further steps to eliminate NCR's problem for creating multilayered scenarios.

1.3 Research question

Research questions is a vital part of research work. They help the readers understand what is this project about into simple questions. Those questions has to be a red hearing in the thesis and answered by the project to serve its real purpose.

RQ 1: What are the main challenges identified in creating scenarios in the NCR?

The NCR has a problem creating scenarios for their exercises. It will be even more important in the future to look at because they plan to create scenarios in multiple layers and not just for one that is usually the case.

RQ 2: What is an ontology that can help solving the challenges for these stakeholders when working on different layers?

Creating a ontology for cyber security scenarios is the suggestive solution this would be the natural point for a second research question. It would need to look into what an ontology is and how that could be modified to help the NCR to achieve their overall goal.

RQ 3: How can the ontology be applied in real case scenarios to solve the identified challenges?

When an ontology is created one will have to apply it to its field of research. Otherwise the ontology wouldn't have any use and a waste to be made. This ontology has to be applied to scenarios and see if it targets the original challenges the stakeholders faced.

RQ 4: How can the ontology be verified for completeness and correctness?

For an ontology to have a value for use by others it needs to be verified. As if it can be applied to a case, but not produce a result in other cases the ontology is limited and needs modifying. Good validation criteria for ontology would be looking at correctness and completeness. Correctness to see if the ontology is correct in a certain extent and completeness to see it can cover more areas and have a complete holistic build up. That would make it validated and viable for more use than is limited by this research.

All these research questions has a vital part in this research, but also shows the timeline of this research. As one start with a challenge. With a challenge one suggest a solution that would need to be researched on. When explored it can be developed and then applied and verified for use. All of this pointing back to the original goal set by the NCR and scenarios being in focus. This structure will be used in this thesis as well to show and explain better how this project and thesis beginning, development and end.

Chapter 2

Technical Background

Background materials covers previous established knowledge in the field working on. That will be any work that isn't covered in a research paper directly to the research. That would be in a related work. Here established knowledge on cyber range, ontology and scenario will be explored.

2.1 Cyber Range

This thesis is creating an ontology scenario for the Norwegian Cyber Range. One thing one would need to explore is the cyber ranges itself and the concept of layers so that everyone is on the same page.

As stated in the introduction a cyber range is an arena or a platform for doing experiments, research an training. This is done in a closed environments where people can easier learn, try and explore their skills in cyber security. A cyber range can be fully virtual or a physical environment. It can also be a hybrid environment. It also needs a set of hardware and software for it to work on.

Depending on what the goal of a cyber range that will be influencing how stakeholders would build a cyber range. Etc if they want to train the users of the cyber range in cyber physical systems like industrial or embedded systems they would make a hybrid environment mentioned in [5]. While a more virtual cyber range would benefits capture the flag or technical exercises.

A cyber range is used by many different parties or users and having different objectives using it. From [5] here are a description of them:

- Students. They can use the cyber range to apply their knowledge, increase their knowledge in cyber security. Depending on the exercises it can be done in a group or alone. It can also be used to preparing them for cyber security certifications.

- Educators. Educators use the cyber range as a platform like a classroom to teach, train and evaluate students or other groups in an exercise.
- Researchers. For them the cyber range is a research tool that they can use to apply or experiment their research in a safe environment. Can also be educators that train others as they are often the cyber experts.
- Professionals. From different groups in society that uses the cyber range to improve their knowledge and skill.
- Organization. Specific organization can use it for evaluating their own skills and train their skills in cyber security. They can also invest in improving certain aspects of the cyber range for their good

These groups organize themselves in certain teams when doing an exercise. They can be unique or overlapping roles. From [5] here is a rendering of that in a classical exercise that is very technical:

- Red Team. This is the team responsible for the attack on a system. They will have to penetrate the security of the exercise infrastructure to obtain their goal. They can be played by the user or be organized directly as a part of the exercise.
- Blue team. Has the defending role and will need to resolve an attack. Often the group that is trained in a cyber range.
- Green team. Is the infrastructure team. They are the ones keeping the infrastructure up and running.
- Yellow team. Is the situational team. Can either be generated or played. They are their to improve realism and provide update to the story running in the exercise.
- White team. Prepares the exercise and leads the overall exercise forward.

Most of these teams have specific tool used to reach their objectives. Red teams have many forms of attack tools, blue analysing tools and green tools for monitoring infrastructure etc.

Before an exercise one would need the environment and a story ready for a practice sessions. These are scenarios and are one of the main background components in a cyber range. That is to generate scenarios that meet the requirements for training and exercise use in the cyber range. As stated scenario is the central element of a traning session. [5]

2.2 Layers in the Cyber Range

An important part of exercises in cyber rangers are layers. Layers are a division of any kind with multiple components. It can be multilayered defence of a system or a multi layered alarm system of a building. In this research layers are different stages a cyber security scenario can be operated in. In cyber security one operate with three layers. NCR layered it a specific way and can be found in the figure in

chapter 1.

At bottom level, it is the technical level. Here a scenario focus on the users technical skill and work in a fully technical environment and components. It is also called the digital infrastructure layer where the infrastructure is running [3]. A typical technical scenario would be a capture the flag and those scenarios would work more closely with concepts network, server and configuration.

The mid-level of this stack is tactical layer. It models networks of producers and consumers of digital services [3]. The consequences of an incident and immediate response is simulated here[3]. A scenario will focus here on the critical infrastructure components or digital value chains. [1] is an example of a scenario with tactical components .

At the top you have the strategical or socio-technical level. It focuses on the social technical and management perspective when a scenario looks at that. It also reflects on societal structures and simulates impact of cyber events with chain reactions and consequences on different levels for society [3]. It also explores how to solve things for the organization as a whole or discovering consequences over multiple states or systems depending on the scope of the scenario. [3]. The Cyber 9/12 scenarios are a common example of a strategical layered scenario.

2.3 Scenario

Scenario has been used for a time in cyber ranges. It is one of the main purposes of a cyber range. There are many things important to make a scenario as good as possible.

One of them is that scenarios aren't static[7]. This makes it easier to use and one need the scenario to be able to be changed later when information comes in and change the situation or the goal of a scenario.

A scenario also needs to have information of the execution. This is because a scenario needs to be self aware where it can go to. Either because the more explained the less planning one need to do when the exercise is being done. Or in case one need multiple scenarios that is a consequence of this scenario.

Each step in a scenario contains a detailed action on how to be used [8]. This can be expanded if explained in a scenario. That will increase how important a scenario can be. Then a scenario can be used to the fullest extent. That eliminates planning time in exercise when more can be explained in a scenario.

[1] [6]

With the initial storyline, and the decision maker process a scenario is shown with these over included to be a powerful to explain an event inside a cyber range. When that is explained clearly that would also make it easier to perform exercises and educate people in what the scenario is set up to teach the users of the cyber range.

And with that less time would be used in planning and performing these exercises. That would make it even easier to perform one or even more exercises in a set amount of time. And time is essential in categories like cyber security. As in best case that time spent would give the users more training time to be ready for the next cyber incident that covers the scenario they have been trained. At worst case what they have learned can still be relevant with the less time spend on preparing.

As security and breaches are quite dynamic and changes quickly with zero day attacks and zero days patches one would need to be sure what the educators train them in are still relevant. This is also helpful if the scenario designers did make it possible to change scenario after creations so that even less time is needed as then one can update a scenario instead of replacing it.

Scenario can be further explained or divide into concepts. This will help when creating an ontology as one will need to make this as clear as possible. And dividing up that to concepts is one way to do it if they are clearly explained. Some of these will be presented here:

- Storyline: the plot of the scenario used. It tells us what has happen and the current situation that is under way when the scenario is going on.
- Goal: Represents the objective at the end of a scenario by those performing it [2].
- Type: Indicates what type of a scenario it is. It is determined on what the scenario explores. A type could be network defence scenario.
- Artifact: What will this scenario create. An artifact is the end product that a scenario will create.
- Challenge: indicates what in the scenario that one needs to overcome. This could be an unresponsive system or lost data.
- Policy: A set of principles in the scenario. It helps guide what the users can do and achieve in the scenario.
- Rules: Specific set of instructions. This needs to be followed for the scenario to work.
- Assumption: Things in the scenario that isn't directly written. These are things one would know based on previous knowledge on similar scenarios or expected by the scope given. Like if a scenario is under the jurisdiction of EU then one would assume that EU law and regulation needs to be follow if stated to make this scenario realistic. Source: Who created the scenario. This will affect the scenario as those will have a certain pattern in their

scenario buildings.
- Arena: where is the scenario being done under. Explored further in perspectives like environment.
- Domain: A distinct place in the scenario where a certain agent or organization has control or can issue power over. Can be a strategical one like a region. A tactical one like control data in infrastructure. Or a technical one like a network. It can be real or an abstract place.

More concepts used in this ontology will be explored that are part of other perspectives in the chapter final product.

2.4 Ontology

Ontology has a fair set of usage and has a theoretical development from past use to now. To further understand Ontology's that needs to be address.

An ontology has different meanings or usage from different fields. As a concept ontology stretch back to the ancient Greece as the studies of beings [9]. In a pure form, Ontology is a philosophical discipline is characterized by being independent of singular, perspectives and domains and as a consequence oriented towards making claims about the world [9]. It was then a part of philosophy and metaphysics. It was further developed as a term in the 17th centuries Enlightenment. In this era ontology was seen as creation of true statements. Those true statements to the study the structure of reality. It has also been looked as a systematic account of existence [10]

These historical studies and usage has had its part when it was considered being used in computer science. Some of the history in philosophy has its part as in a systematic account one will need a dividing into some form of concepts to describe. Though the idea of true statement has been played down in usage.

In computer science it used as formal representation of knowledge inside a domain. It is also seen a information practice characterized by fragmented pieces of knowledge, that depends on the use of domain and perspective, and a fact, makes mostly local claims, and it is also intended as an information strategy [9]. Ontology can also act as as a concept requirement list whether things are met or not through analysis [11] . This step to step is needed to understand when creating an ontology [12]:

- Determine the domain and scope of the ontology
- Consider reusing existing ontologies
- Enumerate important terms in the ontology
- Define the classes and the class hierarchy
- Define the properties of the classes slots

- Define the facets of the slots
- Create instances

They also created a set of rules to easier understand ontologies [12]):

- There is no one correct way to model a domain— there are always viable alternatives. The best solution almost always depends on the application that you have in mind and the extensions that you anticipate.
- Ontology development is necessarily an iterative process.
- Concepts in the ontology should be close to objects (physical or logical)and relationships in your domain of interest. These are most likely to be nouns (objects) or verbs (relationships) in sentences that describe your domain.

This is done by having a set of concepts within the domain and looking at the relationships between them. That for description or modeling of a domain will clear up and give a shared idea of what the domain is. Its end goal is to make a clear insight into a domain that has ambiguity or different view on from the expert in the fields. These aspects is why ontology can help with the research the thesis has explored.

Chapter 3

Related Work

Research in this area isn't the biggest focus area in research. But what is has contributed to this research. The requirements for the related work that was used when screening was if the paper told of all or some of these topics: Ontologies or Modeling of Cyber range, Exercise or Scenario

[2] introduced a framework for automating the process around scenario. That includes designing, validations and testing of scenarios. In that work they introduced a scenario design language. That is a framework used for testing scenarios in cyber ranges. It primary works on scenarios in the technical level.. Scenarios and cyber ranges are huge elements in this paper and the paper states that: "All the training operations carried out in a Cyber Range revolve around the concept of scenario." It states also that a scenario needs to include the digital infrastructure where the activities are staged in. It also describes interesting concepts. Some where used like goal while others gave a point of view of some concepts that can be used or worth noticing like rules and invariant. Note that all concepts introduced would be refined as stated they are used in a technical sense only. That tells also how the broader research in this area is often working in their own layer. All their exercise work where developed for the KYPO cyber range. And all testing product is used for a cyber range. Their information on scenario, concepts and a little on it being used in a cyber range was helpful in this research.

[13] has a systematic literature review on Cyber ranges and security testbeds. It studies the concept in cyber ranges and concludes that scenarios are a vital part of a cyber range. They also developed a taxonomy of current cyber range systems. That taxonomy is explaining many concepts that could be used in an ontology. A figure with their module is find under here. Many concepts ended up in the final ontology like team, domain, tool and storyline. While some concepts like lifecycle management where considered and was in earlier draft of the ontology. It also has a dedicated scenario part and explain that a scenario has to define the execution of environment. Results of this study can be used as a framework for further development and evaluation of cyber ranges. Their studies on cyber range,

scenarios and the taxonomy as framework for continuous research helped much in evaluating good concepts to the research and earlier design of the ontology.

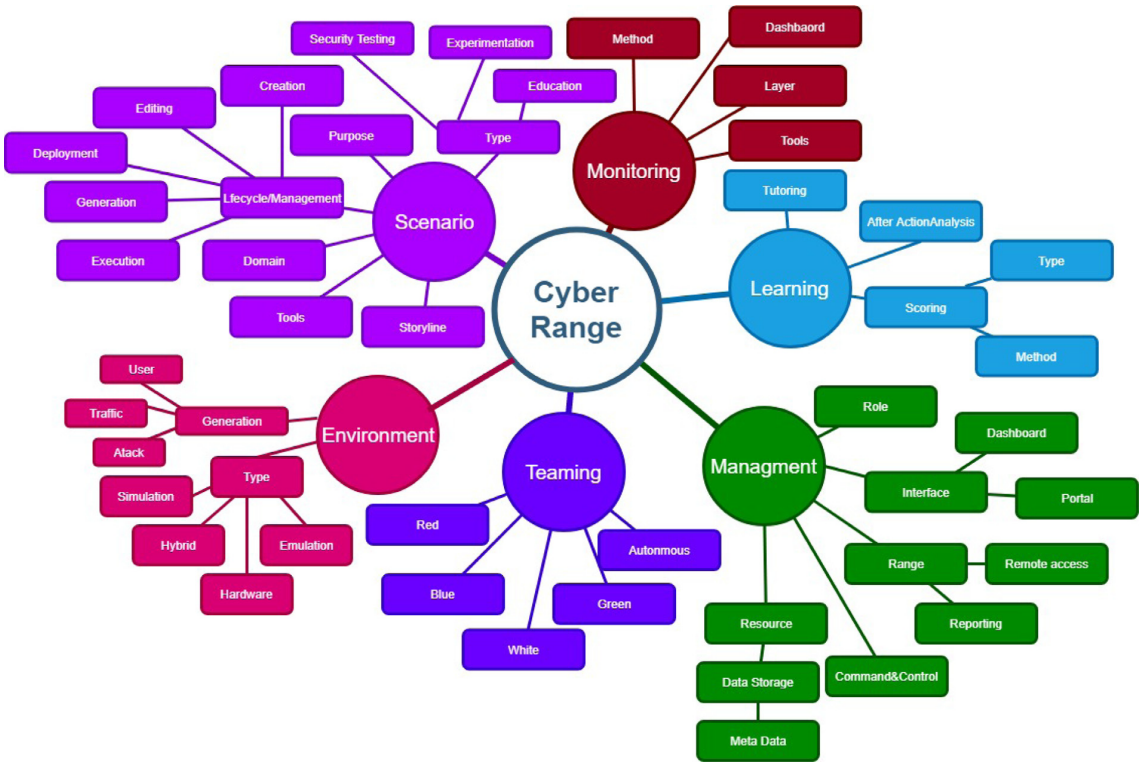

Figure 3.1: A taxonomy of cyber ranges [13]

[14] introduces a approach that is model-driven for the cyber range. The model-driven approach is based on the Security Assurance model. From there they proposes a security assurance model for training scenarios in a cyber range. For now it is only tested on basic scenarios, but they want to expand it to more advanced scenarios at a later date. Their aim is to highlight cyber range training. They also divide the cyber range into sub models for better representation of the cyber range and helping their approach. Their approach leds ways for automation of cyber range training programs that aligns with certain requirements and alignments. Their research on modelling of cyber ranges and scenarios where quite helpful in this research. Even though it works leads to another set of products than an ontology.

[3] proposes a framework for designing Serious Games to raise security awareness. This would be used in a cyber range. Specifically the NCR is mentioned in details. They also tell much on the social-technical layer as the framework is produced with that layer in hand. It mentions what the model in a is focused on depends on the scenario in play. They have a dedicated chapter for the NCR. In

it it briefs short on a cyber range, explain the interdisciplinary and multilayered focus of the NCR. That multidisciplinary focus is crucial for their research. Their research gave a solid background into the NCR and the layers it works under. It also mentioned the importance of scenario briefly as a deciding factor that points out scenarios importance even in papers not dedicating much to scenario.

[15] talks about scenario building in a cyber range is Here they build an quantitative risk approach to estimate risk of compromising. Technical and organizational difficulties has held this approach back from much use before. In the set up of the methodology a scenario plays an important component and is also measured and simulated. It also mentioned definition of score is dependent on the scenario. That played a factor as scoring was considered a concept for a time. With this it tells the concept is clear enough to be used as a concept which made the decision of not having it as a concept in the final ontology. It also describes ctf as use of scenario and exercise for testing the cyber range. This research helped in understanding what could and shouldn't be concepts to be used in own research. Also the methodology they propose is used to monitor outcomes of ctf exercise and scenarios which could help modelling and evolving certain scenarios.

[16] discusses the concept of cyber defence exercises. Their aim is to reveal the process through an exercise. Scenario plays a vital function in the exercises they discuss. Scenario has its own subsection telling a lot what a scenario needs to have in a storyline and its effect on the team being trained. It also has a planning section of the exercise that can be also be used to see what a scenario needs to consider. A defined purpose, identifying impacts and information on the environment are some of these areas that needs to be covered. It also is giving example on how injections can be used which ended up being a concept in the ontology. This research helped in the understanding of scenarios,its vital link to exercises and what some of the concepts needs to cover like impact and storyline.

[17] proposes a modeling language to analyze the problem of security. In this paper societal and organizational level is the main focus. They also proposed an ontology to model security at an organizational level. This is done through the answer set programming. They used a bank scenario for testing it out. The ontology is structured to fit in answer set programming, but to explain the important of agents and organizational structure. Below is a figure to see some concepts in this format. This research helped in looking how to model an ontology on security and having a scenario/use case to test it. Even though they programmed it in a different syntax than this research will. It is also designed to work in societal layer, but it has still usable concepts and the building blocks.

[18] designed an exercise to focused on situational awareness. It was a capture the flag exercise. It also has a scenario section called story and part of the pre competition setup. It goes into subsections on important concepts for this scen-

Type Predicates
service(Service:s)
goal(Goal:g)
task(Task:t)
resource(Resource:r)
actor(Actor:x)
agent(Agent:a)
role(Role:p)

Figure 3.2: Concepts showed in answer set programming [17]

ario. Some of them being storyline and challenge. Without the set up done before the exercise it would not be clear to read the exercise in this paper. This paper helped in the research to show not tell that scenario needed to be explain properly. Especially concepts a part of it.

[8] presents a design and implementation of progression management module. That module is also tested with its interactions with an overall training framework. The progression management is build on a scenario processes. They also use multiple cyber security scenarios to test out the scenario process from competition in Japan. One capture the flag, one forensic and one attack scenario. The scenario is also run in a cyber range. And the management system can be used to describe a cyber range. The research helped this project to show a scenario and how to run it through a module running in cyber range. It basically shows the importance of scenario and the interconnection between scenario and cyber range. And when focusing of different kind of scenarios it can be used in this research how to work in multiple layers and that the product can be used in more than one type of layer or scenarios.

[4] proposes a game for development of cyber security scenario exercise. That game will provide a platform for these scenarios. That is then transformed into a environment through a domain specific language. This game was proven to be useful in these security scenario exercise. Its main focus is in the technical layer. For this research the most applicable part to this project is that it has a dedicated chapter on domain specific language. The DSL chapter looks into step by step on how to create an ontology for a scenario exercise and put scenario in the center of the process. A figure of the ontology is shown below. Some of these concepts could be reused in this thesis as they explained well some concepts and was part of an ontology. Although their focus was exercise scenario and this will be scenario their will be overlaps.

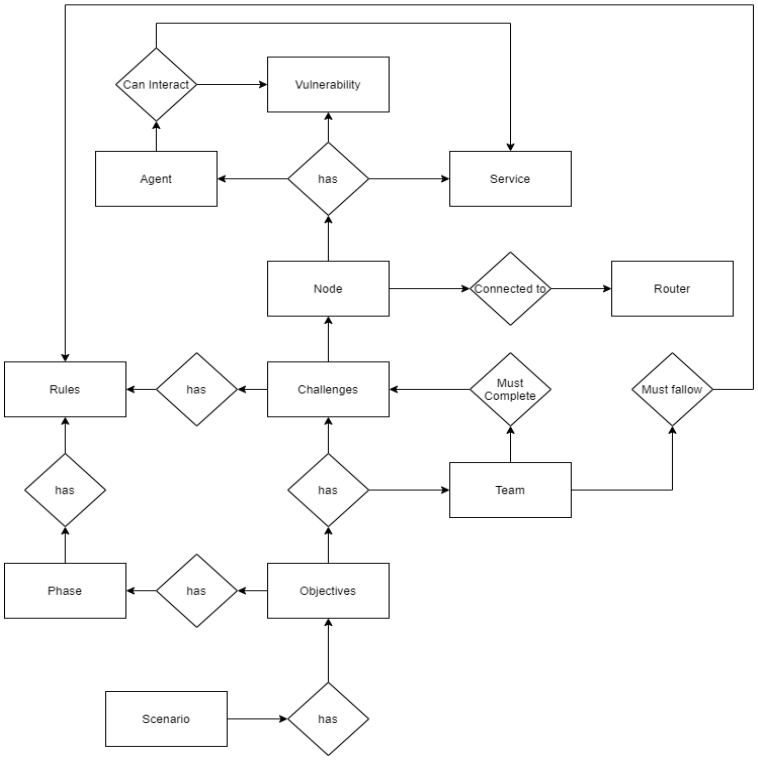

Figure 3.3: Ontology for cyber security exercise scenario in Serious Game paper [4]

[19] made an ontology based on a iso standard. This was based on the iso27005:2011 risk management standard. It stresses out that it only makes the onotlogy of key concepts in the standards. Those concepts are described very well and was used explanation of relevant concepts in this ontology. Threat, CIA and vulnerability are example of these concepts. It also stood as an inspiration of how to make an cyber security ontology for critical concepts only. A figure of this is below.

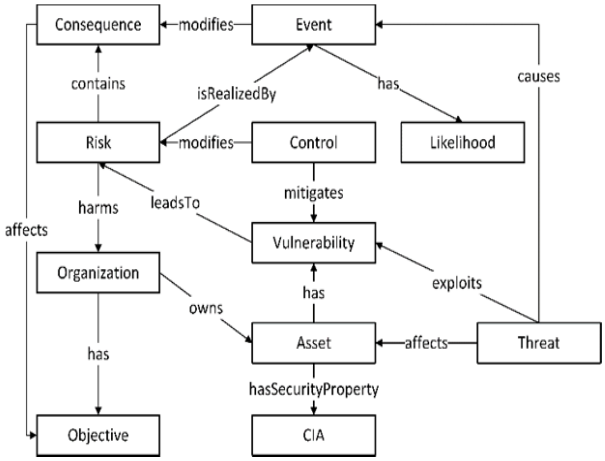

Figure 3.4: Ontology for concepts in Iso 27005:2011 standard [19]

Chapter 4

Research Methods

This chapter will be looking at the method used. It will also describe the development, designing and empirical studies done in this thesis. All to make a clear idea of the product and its story. Because a clearer story makes the ontology clearer which is a goal with an ontology to do. A figure of some research methods is included below[1]:

Figure 4.1: Some Research methods that can be used from Liu Post. Some of them are used in this research. From Sage research.

4.1 Literature Review

Literature review is an essential research method for most research projects. Finding out what has been done will help in what the current research is and where the development to the field is. Here, the main task was to find data done before

[1] Research method

on either ontologies or modeling of scenarios or exercises in cyber range.

This was done through searching these criteria on academical journal sites or ask researcher. The main finding was that there existed some scenarios-related research work to use. Furthermore, background information on cyber ranges and ontologies were studied and has supported this research. A detailed description can be found in the related work chapter.

Simultaneously, when doing literature review was being an initial development of the ontology was done. This was mostly to get a practical grip and understanding of how to make an ontology. The first prototype was created in draw.io. That helped the research since it gave a piratical understanding of what was needed to be created.

The first set of data to build an ontology on was gathered from the literature review. Those versions were made through visio by suggestions from the supervisors. Most of these steps where qualitative researches method as collecting data is exploratory activities and by that factor qualitative. That is also counted in the fact that the research time was limited and interviews where semi structured focusing on a few core personnel that had relevant data compared to reaching out to as many as possible.

Even though a lot of valuable data where collected it still wasn't enough to create a viable ontology. So a second literature review was done. As there where already done much in background it was easier to find relevant literature even though it still wasn't much. And often it was only a section of a paper that could be relevant for the research.

4.2 Development

Now that multiple rounds of literature reviews had been done it was enough data to make a fitting ontology. The work was divided into multiple parts. As it was easier to start with a scenario in one layer and complete one layer at time. From then one could go over the scenarios in the other layers to fill up lacking concepts to cover multiple layers. The first modelling was done here as well in visio. But at a point their became to many concepts to understand the ontology in one drawing. So the ontology was divided into multiple drawing divided into main perspectives of the ontology. It was still a bit unclear so it needed a more firm application to represent things clearer. The application chosen to do this was protege.

This ontology was build by abstracting concepts from many sources. Some related literature review either being existing ontologies or concepts from scenario modelling and some from ncr core personnel. But scenarios that would be targeted by

such ontology where abstracted concepts form as well. Two real created scenarios was selected. The scenarios used are a Locked shield scenario from 2013 [2] and a Cyber 9/12 scenario from 2020 [3]. *Locked shield* is a yearly NATO cyber defence exercise that has a scenario component . It covers tactical and technical concepts. While Cyber 9/12 is a yearly cyber competitions for students. Here there is a more focus on the social technical aspect and is in the strategical layer.

The ontology was made by following the guide on making ontologies [12]. Note that these steps uses the terms in Protégé. So classes is concepts, hierarchy includes perspectives, Here are the steps followed:

- Step 1: Determine the domain and scope of the ontology
  First the ontology needed a domain and cope. The domain was cyber security and scope scenarios within the cyber security domain.

- Step 2: Consider reusing existing ontologies
  The project looked at existing ontologies in this domain and scope. They weren't anyone at the level of complexity?(please suggest me a word) created that would satisfy the research questions. Ontologies I looked at that had reusable material where the ones cited in these papers: [4], [19] and[4].

- Step 3: Enumerate important terms in the ontology
  Before classes was created the research also looked at scenarios and abstracted concepts from there. With that and the reuse of previous ontologies the classes could be created. There where also classes inheriting from others and the hierarchy had the perspectives at the top.

- Step 4: Define the classes and the class hierarchy
  In this step, each class/entity was defined through a combination development process, which combines the top-down and bottom-up approaches. The more salient concepts were defined first and were generalized and specialized appropriately.

- Step 5: Define the properties of the classes slots
  After that some properties for these classes were made. Those could be used for linking relationships under object properties or describing a certain class when linked to an instance under data properties.

- Step 6: Define the facets of the slots
  The facets were not explored and if suggested the suggestive insertion protege had as default where chosen. Domains and ranges where added to most properties. Characteristics and constraints in protege were not explored.

[2] [6]
[3] [20]

- Step 7: Create instances
  At the end some instances where created from individual and type them to their class. Later the ontology was modified, but it could from there be used for simple testing for trial and error evaluation.

In Protégé, one could easier read what was of the ontology and what needed to change to make it more clearer to others. With some reworking a final stable version was made which signalized the endgame of the story.

After that a more stable ontology was made. That ontology went through several versions. That is usually normal with ontologies as one expand it with new knowledge in the domain. But developed understanding of what an ontology is also played a factor in the changes. Earlier version worked similar to a taxonomy. The data was collected from interviews, literature review and abstraction of scenarios. From there it was modeled and visualized in competent applications. This was done first through visio and later in protege.

By abstracting these scenarios one found out what concepts where needed to explain these scenarios in these ontologies. And choosing from all the layers one would get a complete view. And with the already use of domain expert opinions and literature review an ontology was created. An ontology that can be used in all three layers for scenarios and could give NCR some answers.

4.3 Evaluation

The developed ontology was evaluated with a 2-phase scheme: A competency question evaluation followed by a domain-expert review.

In the first phase, the ontology was validate whether it could resolve the prepared competency questions (CQ). This is done by using SPARQL (SPARQL Protocol and RDF Query Language), a semantic query language for retrieve and manipulate data stored in Resource Description Framework format (RDF). These CQs and results are presented in Chapter 6. The results showed that the ontology had a usage even if not completed yet. It also shows how powerful an ontology can be if correctly modelled in protege.

In the second phase, the ontology was further evaluated through a domain expert review, where a semi-structure interview method was adopted to validate whether the ontology could be use in the real-world situation. The interviews was done on a handful of key personnel working in different layers in the NCR. Most of them researchers, but some of them were engineers as well. There where

planned some questions to the interviews. Those were used in case those being interviewed didn't have much to say and needed some help in what to evaluate. Most personnel had much to evaluate the product without use of question. These procedures showed that the ontology had reached some maturity and potential for use by the domain experts based on what one could get by the limitations of a master thesis. However there where many suggestions of improvement or what needed to be done to make it usable. All of these comments will be discussed in the domain expert review chapter.

Chapter 5

Development of the Ontology

The ontology made has a lot of data to cover. All from its development to its final version. These events and data will be covered here.

5.1 Design concept

Some mentioned would be needed to be said about the design. As the applications already chosen had pre-made models or syntax the only choices to make was to decide what fitted best with the proposed product. For visio modelling UML classes was the best tool for concepts and a collapsed package for its perspectives. For protege all was given by the syntax which was learned through the tutorial given to protege.

There where 5 perspectives chosen as the main groupings of the concepts. Those being scenario, security, operation, environment and stakeholders. All of them and the concepts will be explained in section 5.4, but here is a figure to show it all and that their is a link between these perspectives:

The ontology was designed through visio. Visio is a diagram and vector graphics application. It was made by Shapeware in 1992 and acquired by Microsoft in 2000. It has many visual drawing capabilities. It begins with having a lot of templates, diagrams, flowcharts and stencils. As most of it is already in ready to use one would only need to add ones ideas into the right template. Visio 2016 version was used in this thesis to graphically represent the ontology and develop it through the phases to a final product. For the perspectives package (expanded) template was used under UML class. This was to differentiate from concept with a over-category and package worked for that purpose in this case.

For the concepts a standard UML Class where used. That is because it is the most natural way to show a concept off.. Especially if wanting to model it with a scenario then one could show the instances of the concept in the membername tabs

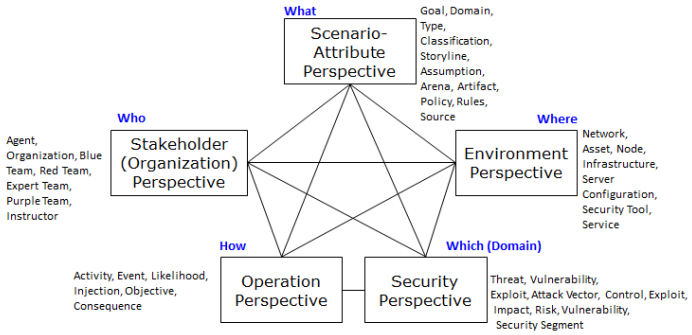

Figure 5.1: Perspectives in this ontology with their concepts a part of it

under.

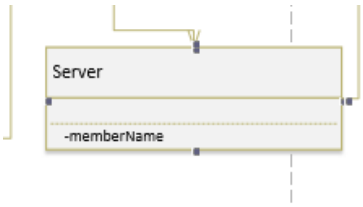

Figure 5.2: Example of UMLclass in Visio

For connecting the concepts an arrow is used and a description of the connections between the concepts. For the arrow directed association was used. It will generate a pregenerated arrow and then one can edit it by moving it around for connecting it to the concepts wished to bed related to each other. For the description a package (collapsed) where used. This can hold small sets of words perfect for this. And if this is put it inside a directed association between two UML classes visio will automatically make another directed association arrow. This finish up the use of visio.

Originally the ontology was designed as one big class. From there going from version 1.0 to 3.0*. Through the updates the ontology expanded and it would be difficult to read clearly the ontology. So it was in visio divided into their perspectives to increase readability. That also came with some edits internally in each perspective creating some versions to be 3.1 or 3.2.

Scenario is a perspective that was divided in visio. Here is the visualization of it:
The next perspectives modelled is security. This is the visualization of it:
Operation was the next perspectives to be divided and modelled. Here is the visualization of it:

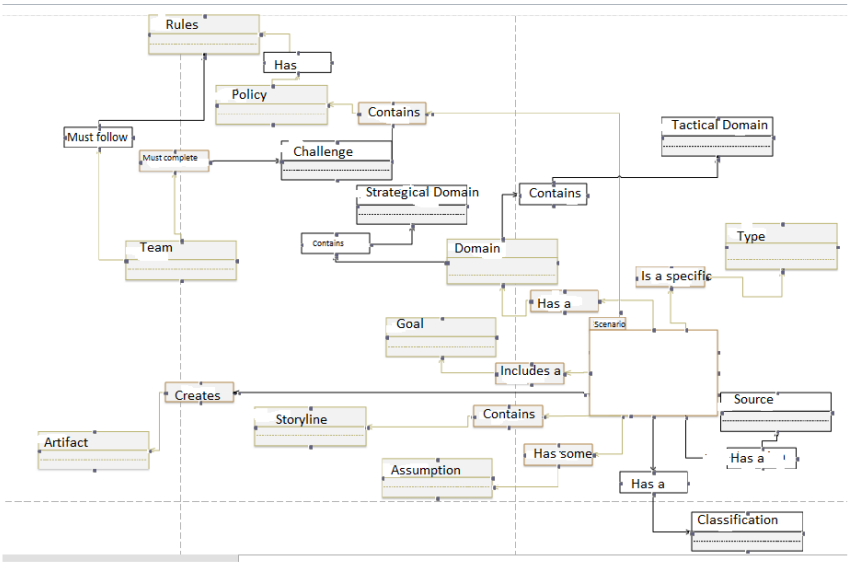

Figure 5.3: Modelling of the perspective scenario

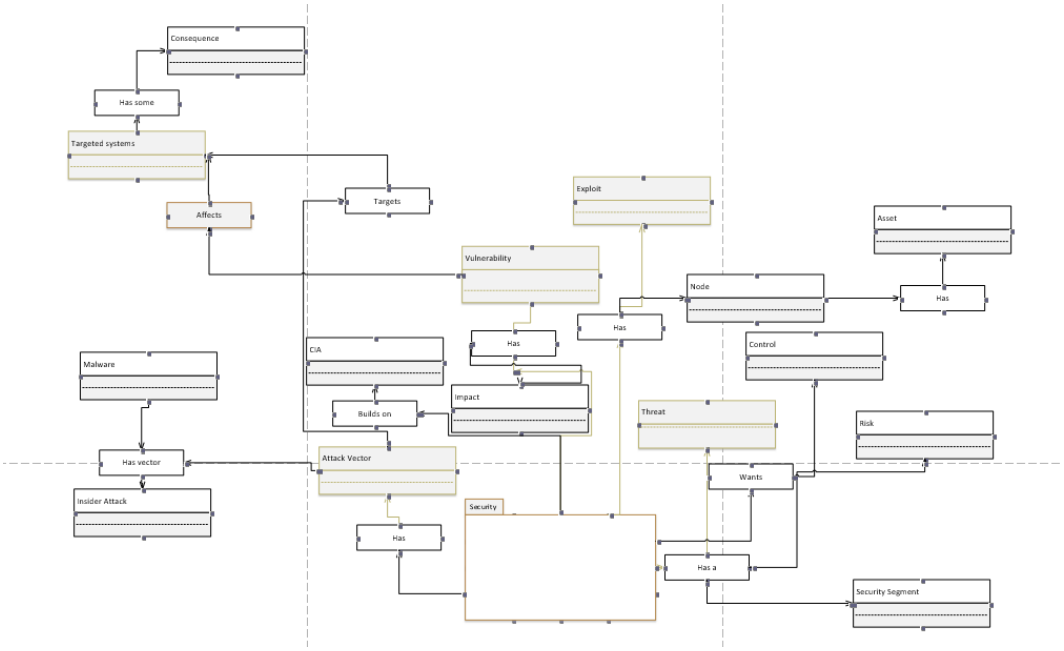

Figure 5.4: Modelling of the perspective security

Environment was also divided into its own model. That visualization is showed here:
The final perspective is stakeholders. And this is how its modelled in visio:

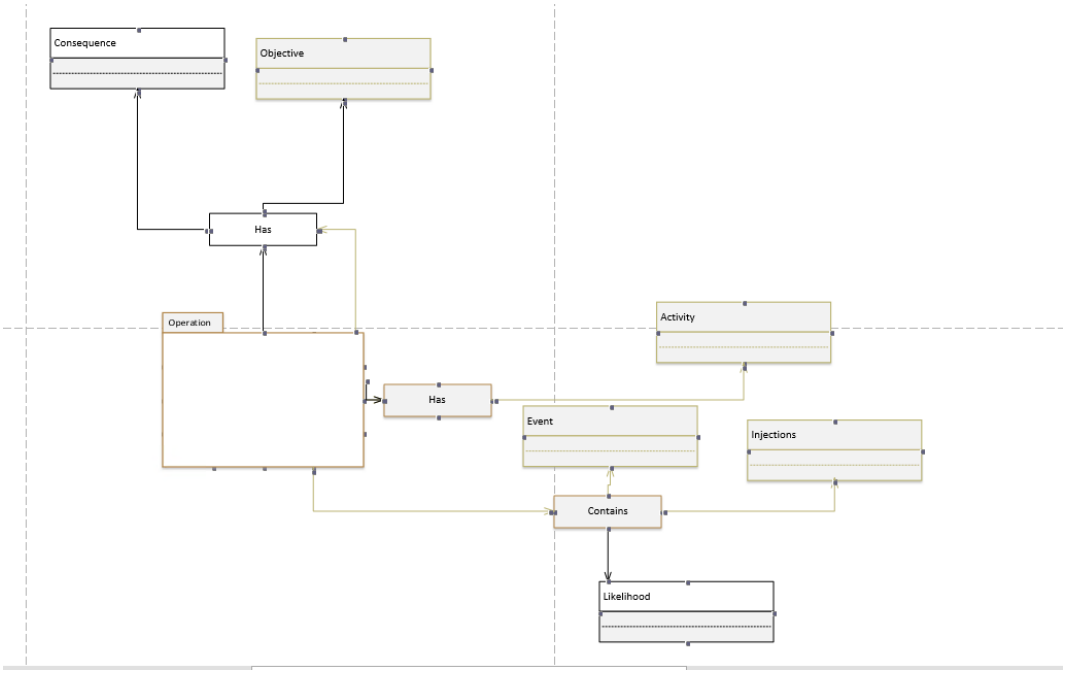

Figure 5.5: Modelling of the perspective operation

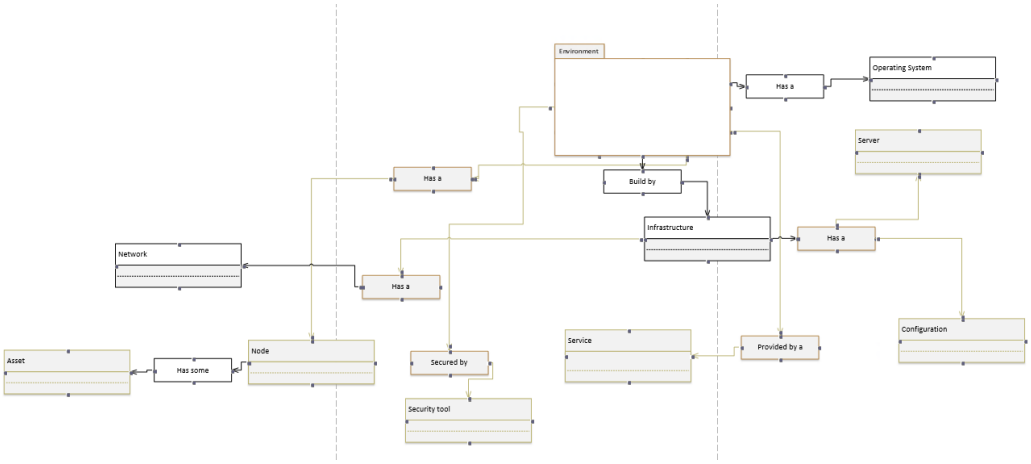

Figure 5.6: Modelling of the perspective environment

5.2 Development

The final product is an ontology for scenarios in cyber security. It is for now called Scenario Ontology. It is modelled in Protege. It consists of 5 perspectives and 44 concepts. The main perspectives is scenario, security, stakeholder, operation and environment. A brief description of these and a explanation of each concepts a part of them will be covered in this section. It will also look at the ontology with the final edits. Concepts added from evaluation will be explained in evaluation.

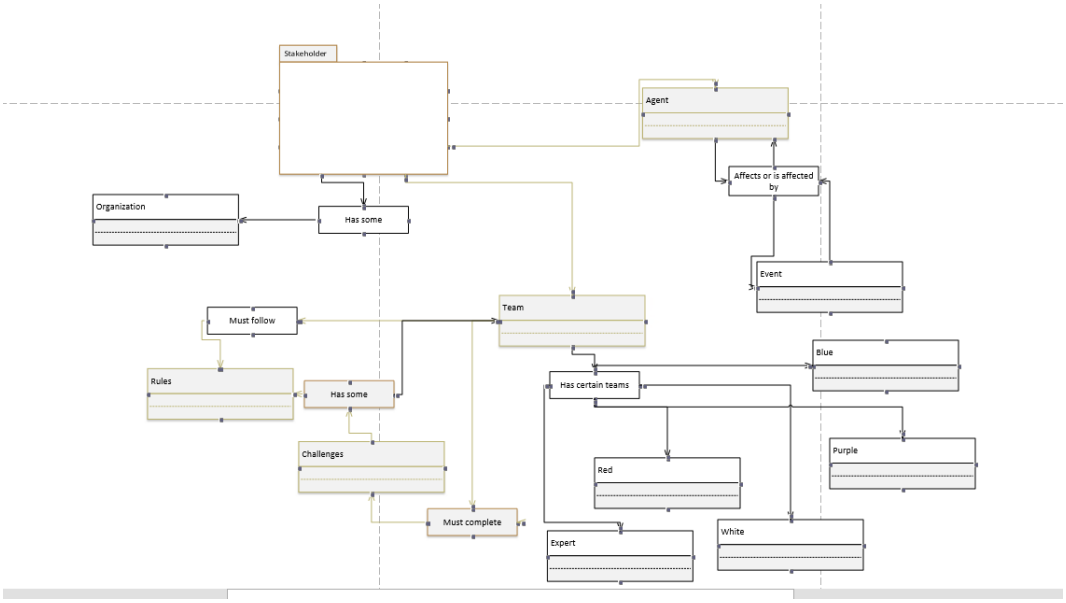

Figure 5.7: Modelling of the perspective stakeholder

Protege was first created in 1999 and is distributed free by Stanford University. It requires java runtime environment to run properly. Protege is an application for for ontology environment especially for creation and editing of ontologies. It is also an knowledge management system. It also feature a lot of tools for navigating through the relationships within an ontology. There is an convention on how each value should be added. Here is how protege looks like:

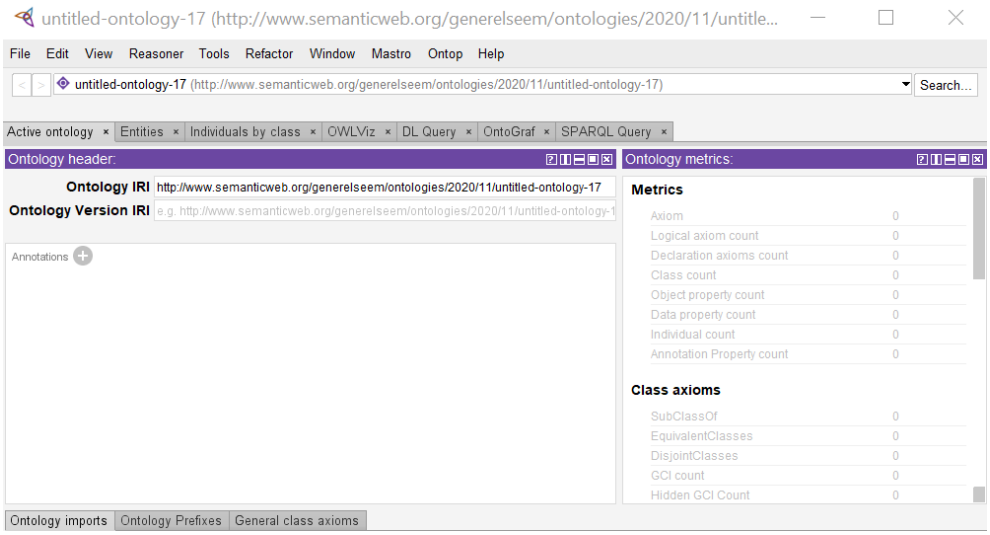

Figure 5.8: First view when entering Protege

For the creation of an ontology the most important tab to start working is the entities tab. One can use it to work on multiple aspects with an ontology. The most common is to start with classes. Perspectives and concepts can be added from here. In this thesis as the this was created before it only needed to add it in classes. Classes are named in the syntax capital letter on first word. If multiple words are needed one would need to add an underscore and then all in small letters. Here is an example:

Figure 5.9: Example of syntax in protege

For using the ontology or creating specific usage of a class one will need to use the individual tab. Here an instance of a perspective or concept can be added. To add detailed data or relations between classes or individuals one would use properties. Their exists object and data properties. Object properties is used when dealing with instance of a concept that can be used in multiples scenarios that have some sense. While data is used on concepts that cant be generalized and still have relevant information to give. A concept like storyline can only be viably used in one scenario so it goes under data properties and have a description inside the instance. Individual has the same syntax as classes, but properties has small letter, underscore and then capital letter on the next words:

Figure 5.10: Example of property syntax in Protege

5.3 The Ontology

Here follows the description of the ontology. Here includes the perspectives, concepts and how its represented in protege.

5.3.1 Scenario Perspective

Scenario is the first perspective under the loop. This cover normal concepts that are common to make a scenario. Things like storyline and goal comes under this category. Without them one cant make a basic scenario at all. Scenario covers 11 concepts and make sure the fundamentals is in place. Here is how the relationships between them are modelled and how it looks it in protege.

- Storyline: the plot of the scenario used. It tells us what has happen and the current situation that is under way when the scenario is going on.
- Goal: Represents the objective at the end of a scenario by those performing it.
- Type: Indicates what type of a scenario it is. It is determined on what the scenario explores. A type could be network defence scenario.
- Artifact: What will this scenario create. An artifact is the end product made through a scenario create.
- Challenge: indicates what in the scenario that one needs to overcome. This could be an unresponsive system or lost data.
- Policy: A set of principles in the scenario. It helps guide what the users can do and achieve in the scenario.
- Rules: Specific set of instructions. This needs to be followed for the scenario to work.
- Assumption: Things in the scenario that isn't directly written. These are things to know based on previous knowledge on similar scenarios or expected by the scope given. For example if a scenario is under the jurisdiction of EU then would assume that EU law and regulation needs to be follow if stated to make this scenario realistic.
- Source: Who created the scenario. This will affect the scenario as those will have a certain pattern in their scenario buildings.
- Arena: where is the scenario being done under. Explored further in perspectives like environment.
- Domain: A distinct place in the scenario where a certain agent or organization has control or can issue power over. Can be a strategical one like a region. A tactical one like control data in infrastructure. Or a technical one like a network. It can be a real or an abstract place.

Below is the scenario modelled in protege.

5.3.2 Security Perspective

Security is the second perspective. Security covers perspectives that are related to cyber security. Things like vulnerability and threat comes under this category. Without them it would be hard making a scenario inside the security domain. Security covers 18 concepts and make sure security the critical concepts of security are covered. This is a perspective with potential to increase in scale quickly as

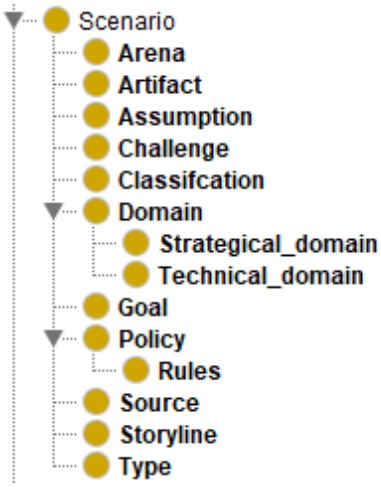

Figure 5.11: Representation of scenario in protege

security is a vital part of the cyber range and things security can and will cover is easily increasing. Here is how the relationships between them are modelled and how it looks it in protege.

- Attack Vector: Ways or means one can be able as an attacker to attack the system. Inside attack and malware are examples of attack vector.
- CIA: The three pillars in information security. Represents the confidentiality, integrity and availability of data.
- Control: A class that tell us what is being done to mitigate risks in a system.
- Exploit: A class that looks at systems or resources that can be used for the benefits of the attacker..
- Impact: Representing the marked effect of an attack. This indicates those that happens on the primary system attacked.
- Node: Devices of data that needs to be protected.
- Asset: Data with a set of value that needs to be protected.
- Risk: Representation of an effect from unsecured devices
- Threat: Potential cause of an unwanted situation that can result in harm in either systems or organization.
- Vulnerability: A weakness in a program or a system that can be used by a threat. For data that can be a bug and for company a structural weakness in a company.

Below is the security perspective modelled in protege.

5.3.3 Operation Perspective

Operation is the third perspective. This cover concepts that are used to make thing happen or describes things that happen in a scenario. Things like event and activ-

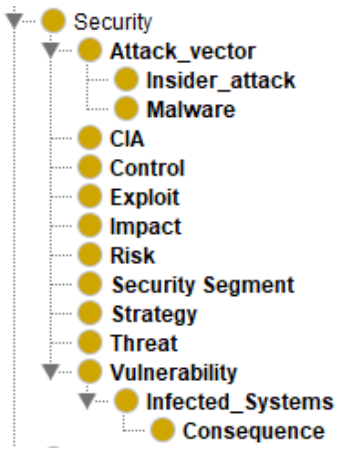

Figure 5.12: Representation of security in protege

ities comes under this category. Without them cant events in the scenario cant be described properly. Operation covers 7 concepts. Here is how the relationships between them are modelled and how it looks it in protege.

- Activity: A thing that the team doing the scenario has done.
- Consequence: The outcome of an event. Not the same as impact since these are outcomes further down the line like outcome on systems not targeted in the event or the outcome on the companies or organizations reliant on systems being affected by the outcome of an event.
- Likelihood: Tells us how likely an attack or situation can happen.
- Objective: Plans or steps on the way achieving the goal of a scenario.

Below is the operation modelled in protege:

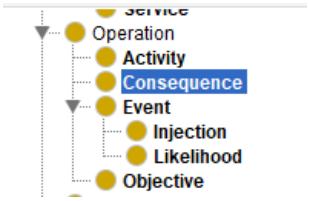

Figure 5.13: Representation of operation in protege

5.3.4 Environment Perspective

Environment is the fourth perspective under the loop. This cover concepts that are described within the systems the scenario is working in. In security and IT scenarios that would be the computational environment. Things like network and asset comes under this category. Without them data or systems cant be described in a scenario. Environment covers 9 concepts. Here is how the relationships between

them are modelled and how it looks it in protege.

- Asset: Data that has been labeled or inserted a form of value to someone in the scenario
- Infrastructure: The basic structures to, facilities or code needed for the organization int the scenario to function.
- Server: A machine that operates and provides services to other systems. Often described with operating system.
- Configuration: Build up of the server room
- Network: A collection of computers, servers and devices in a system inside an organization
- Node: Devices of data able to communicate with other devices.
- Security Tool: Software or data used to secure the environment
- Service: Those systems that supplies a need to someone in the scenario not part of the original environment.

Below is the environment visualised in protege:

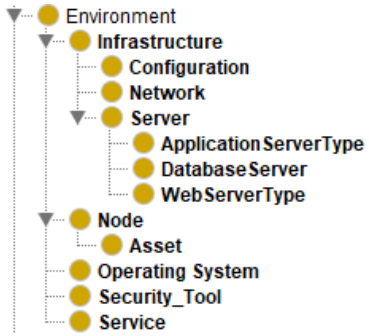

Figure 5.14: Representation of environment in protege

5.3.5 Stakeholder Perspective

Stakeholder is the final perspective under the loop. This perspective covers concepts that are personnel doing or affected by a scenario. Things like agent and team comes under this category. Stakeholder is needed so can describe the different teams or agent in the scenario. It also explains which of those agents and teams are controlled or just used by the scenario. Stakeholder covers 7 concepts. Here is how the relationships between them are modelled and how it looks it in protege.

- Agent: A person or a thing that affects the scenario by doing the specific events. Can be played or automated by the scenario
- Organization: Organized group of people that is affected by the scenario.
- Team: Groups of player performing a scenario.

- Configuration: Plans or steps on the way achieving the goal of a scenario.
- Red Team. This is the team responsible for the attack on a system. They will have to penetrate the security of the exercise infrastructure to obtain their goal. They can be played by the user or be organized directly as a part of the exercise.
- Blue team: One of the teams used in a scenario Has the defending role and will need to resolve an attack. Often the group that is trained in a cyber range.
- Purple team: The leading responsible for the scenario. The
- Expert team: A possible team in the scenario. In a scenarios where protecting an environment isnt the main goal, but gather information or brief on a environment this will be the group trained. Quite often used in the strategical layer.
- White team: One of the teams in a scenario. Prepares the exercise and leads the overall exercise forward. Can also be called an instructor

Below is the stakeholder modelled in protege.

Figure 5.15: Representation of stakeholder in protege

Chapter 6

Evaluation of Ontology

Making a product solid from these sources is a good start, but it needs more than just being. Otherwise it would just be a concept that has interesting, but not proven. To make it viable or a proof of concept one would need validate it. There are many ways to validate a product. An image of some evaluation methods are on the next page [1]:
For this ontology it was the most logical approach to validate correctness and completeness based on those visualised above. As the ontology needs to be correct as possible to be viable for usage. Completeness can check if the ontology covers all the concepts that comes up in a normal scenario. Then a complete ontology would be expected to cover the common critical concepts of scenarios it faces.

The approaches used for evaluating it was these. First a test by choosing a scenario and add it in to the ontology. Then if one could describe all concepts in the scenario chosen the concepts where critical and correct. The results of that are in section above.

Another approach was to use the tools in protege. SPARQL was used to answer some question that could the ontology answer these questions for us. If the ontology could answer some questions in the range from easy to medium it would show that the ontology had achieve some form of completeness. The results of that can be found in section of competency questions.

The third approach where domain expert reviews. Here the NCR personnel got a first hand view of the taxonomy and the Scenario Ontology to review its status. Both correctness and completeness can be tested then as if they could see the use and agree to these concepts being vital then it was correct. If they didn't have many more critical concepts to add that also means it had received some form of completeness. Domain expert review where also used to see if they had ant other things worth discussion or ideas for future work not already been discussed.

[1] Validation figure

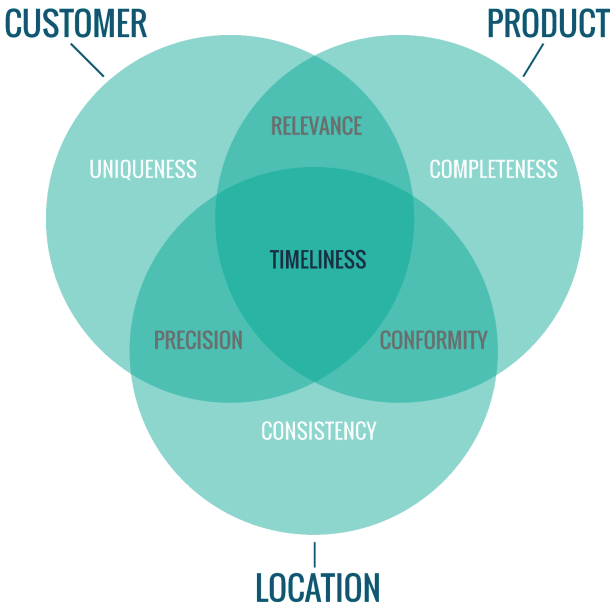

Figure 6.1: Validation options

6.1 Use Case

The ontology can also be described by adding a scenario and using its data to explain each concepts. That would be called a use case. Here is the ontology used to describe the first scenario in Cyber 9/12 in Geneva of 2020.

Perspective:Class	Instance on a scenario
Environment: Asset	Control data, personnel data, Power distribution data,
Environment:Configuration	Windows legacy setups.
Environment: Operating systems.	Most likely Windows 2000 or XP.
Environment: Node	Pc, telephone, control systems,
Environment: Security Tool	SCADA security mechanism didn't respond under the attack
Environment: Server	Windows legacy systems on 32 bits
Environment: Infrastructure	power distribution system, , pipelines, telephone lines,
Environment: Network	SCADA is one of the networks used in this scenario
Operation: Activity	Forensic analysis, meetings, decision brief
Operation: Consequence	EU lost most sources of energy and power.
Operation: Event	Situational meeting, upgrade of systems, committee hearings
Operation: Injection	alarm rise, additional situational updates
Operation: Objective	Collect knowledge to asses what is going on.
Scenario: Source	Cyber 9/12 atlantic council
Scenario: Arena	Cyber 9/12
Scenario: Artifact	policy statement/document
Scenario: Assumption	Work under EU and direct cases to right committee
Scenario: Challenge	Unresponsive System. Unknown threat actor. Can strike again
Scenario: Rules	Realistic, multi-dimensional, creative, analyze.
Scenario: Domain	NisPower/EU
Scenario: Goal	Solve the security problems in NISPower and EU.
Scenario: Impact	NisPower systems unresponsive. Not able to access their assess.
Scenario: Policy	EU monitored principles used by the memberstates.
Scenario: Storyline	NisPower executed a planned upgrade of SCADA unsuccessfully.
Scenario: Attack Vector	Friendlie Pixie, malware
Security: CIA	data leaked, datasystem cant be trusted, systems not available.
Security: Control	Not using legacy systems, Not one source of power for EU.
Security: Exploit	Legacy SCADA systems, VOD telephone lines, bad routines
Security: Risk	Denial of service, unresponsive systems,
Security: Vulnerability	Old SCADA systems, old windows system, old telephone lines.
Security: Infected Systems	NisPower systems, power plants in France
Security: Threat	Insider attack, legacy attacks, denial of service.
Stakeholder: Agent	EU, Nistria, NATO etc.
Stakeholder: Organization	NisPower
Stakeholder:Team	Cybersecurity expert team.
Stakeholder: User	Specific team member in the taskforce with dedicated tasks.
Stakeholder: White Team/Instructor	The organization team that sends out intelligence brief.
Stakeholder: Service	These systems supplies transportation of gas in pipelines

Table 6.1: Description of ontology by use of concepts from the scenario

Relation	Class Involved	Instances based on a scenario
exploits	Threat,Vulnerability	There are multiple threats like insider attack, malware injection etc that can exploit the vulnerability of the systems.
causes	Event, Threat	An event from harmful agents or technical programs causes threats in a system.
is realized by	Event, Risk	An event from harmful agents or technical programs is realized by the risk how things like DOS
modifies	Event, consequence	An event that is made from the the team modifies the consequences of the attack,
leads to	Vulnerability, risk	The vulnerability of the systems leads to those systems having risk.
mitigates	Control,Technical vulnerability,	Control mechanisms mitigates System vulnerabilities.
affects	Threat, assets	A threat like insider attack affects the data or assets to NisPower
has security properties	asset, CIA	Those data that has an asset/value has a security property that correspond with the CIA model
belongs to arena	Scenario, Arena	This scenario belongs to the arena cyber 9/12 which has multiple scenarios made in it
contains	Scenario, storyline	The scenario contains a rich storyline that gives the scenario meaning for the users.
has	Policy, objective	Every policy made has an objective to solve a part of the scenario.
has goal	Scenario, goal	Any scenario has a goal. Here the goal is to solve situation without escalating it if possible.
includes	Scenario, goal	Any scenario like includes a goal to work for by the user.
interact with	Infrastructure, agent	A infrastructure system like the power distribution system interacts with an agent like NisPower or EU .
makes	Threat, risk	A threat from insiders or malware etc makes a risk like DOS.
has	Team, challenge	The expert teams has some challenges to deal with in the scenario
must follow	Team, rule	Any team doing this scenario must follow the rules of the scenario to do the scenario.
targeted by	Risk, Actors	The risk to a system is targeted by foreign actors presumed to be affiliated with Mustelus
owns	Organization, asset	NisPower owns it valuable data/asset.
harms	Risk, organization	Insider attack or dos harms NisPower day to day operation and their reputation.
modifies	control, risk	Control mechanisms modifies the extent a risk can have to NisPower.
affects	activity,event	Forensic analysis is an activity that affects an hearing or other events.
affects	infected systems, infrastructure	Scada systems affects the infrastructure like the systems inside of pipelines or electricity in Nistria.
leads to	Events,injection	Meetings leads to discussion and update of information like forcefully change of severity in the situation.
has	system, exploit	The SCADA central system is old and contains many exploit Mustelus can take advantage of.
contains	risk,consequence	Any risk like dos contains consequences like EU loosing most of their sources to energy.
has	Scenario, team	Cyber 9/12 scenario has a team of cyber security experts that works with the sceanrio.
affects	event, team	A meeting can affect the next cause of action to this expert team
affects	event, user	Those same meetings can affect what the individual user of a team does or say
affects	activity, actors	A forensic analysis affects the next course of action to EU and Nistria
affects	consequence, objectives	EU loosing their source of power affects the objective as that is information they need to collect on what happen.
has	team, user	The cyber expert group has user or individual group members having their expert field
has	vulnerability, exploit	Those old SCADA systems also have known exploits that Friendly Pixie can use
has	organization, objectives	NisPower want power restored and their day to day operation go back to normal
has	asset, vulnerability	Valuable datasystem in NisPower has vulnerabilities by the nature of being old systems not updated for a while.
has	event, activity	An committee meeting has a decision brief as an activity
was the trigger	event, network	An upgrade of the scada system was the trigger for the SCADA system becoming unresponsive
has	event,likelihood	Upgrade of the system has a likelihood to help or make things worse if already compromised
has	scenario, artifact	In this scenario the team creates a policy brief that includes the teams suggested solution
has	Scenario, storyline	This scenario has a storyline of the events leading up to current situation.
must complete	user,challenge	Those individuals user expert must complete or solve the challenge of unresponsive systems
must follow	user,rule	Those same user must follow the rules of Cyber 9/12 challenge
makes	threat, risk	A threat of an insider attack to NisPower makes a risk of unresponsive systems
uses	threat, attack vector	An insider uses friendly pixie to affect NisPower systems.
works on	team,artifact	A team creates a policy brief in the scenario
is affected by	server, attack vector	The windows servers in this scenario is affected by the friendlie pixe attack as its targets legacy windows systems.
has a	scenario, source	This scenario has a source of where it was created. This was created by the Cyber 9/12 atlantic council.

Table 6.2: Description of ontology relations between concepts

6.2 Competency question evaluation

For testing of the ontology, five CQs were created to see if the ontology could be used to abstract knowledge from it. This was done by making some questions that would answer something a person would like to know of the scenario of to one or multiple scenarios and then query it in SPARQL. The five CQs are:

CQ1: Which scenarios are network defense scenarios? Below is the syntax and then result of the competence question.
CQ2: Which systems are infected in Scenario 1?
CQ3: Is the assets protected by someone in scenario 2 and what asset is protected?
CQ4: What layer are each scenario in?
CQ5:What are the scenarios dealing with "Privileged Access" in Apache web servers, and what are the embedded vulnerabilities?
The SPARQL statement for each CQ and the corresponding results were given in the following.

CQ1: Which scenarios are network defense scenarios? Below is the syntax and then result of the competence question.

```
SELECT *
Where {
        ?Scenario m:typeofScenariols ?Type.
        FILTER regex(str(?Type), "Network")
}
```

Figure 6.2: SPARQL of CQ1

Scenario	Type
Scenario_2	Network_defence
Scenario_4	Network_defence

Figure 6.3: Output of CQ1

CQ2: Which systems are infected in Scenario 1?

```
SELECT *
WHERE
        { ?Scenario m:infrastructureAffectedIs ?Targeted_Systems.
        FILTER regex(str(?Scenario), "Scenario_1")


}
```

Figure 6.4: SPARQL of CQ2

Scenario	Targeted_Systems
Scenario_1	Power_distribution_system
Scenario_1	Phone

Figure 6.5: Output of CQ2

CQ3: Is the assets protected by someone in scenario 2 and what asset is protected?

```
SELECT *
WHERE
        { ?Scenario m:infrastructureAffectedIs ?Targeted_Systems.
        FILTER regex(str(?Scenario), "Scenario_1")


}
```

Figure 6.6: SPARQL of CQ3

Scenario	Blue_Team	Asset
Scenario_2	Karl	PC

Figure 6.7: Output of CQ3

CQ4: What layer are each scenario in?

```
SELECT *
WHERE
        { ?Scenario m:layer ?layer.

        FILTER regex(str(?Scenario), "Scenario_")

}
```

Figure 6.8: SPARQL of CQ4

Scenario	layer
Scenario_4	"Tactical"
Scenario_1	"Strategical"
Scenario_3	"Technical"
Scenario_2	"Technical"

Figure 6.9: Output of CQ4

CQ5:What are the scenarios dealing with "Privileged Access" in Apache web servers, and what are the embedded vulnerabilities?

```
SELECT ?Scenario ?Vulnerability ?Segment ?Server ?ServerType ?Version ?OperatingSystem
  WHERE {
  ?Scenario onto:relatesToVulnerability ?Vulnerability.
  ?Vulnerability onto:inTheSegmentOf ?Segment.
  ?Scenario onto:hasEnvironmentalComponent ?Server.
  ?Server rdf:type onto:Server.
  ?Server onto:isTypeOf ?ServerType.
  ?Server onto:Version ?Version.
  ?Server onto:usesOperatingSystem  ?OperatingSystem.
  FILTER regex(str(?Segment), "PrivilegedAccessManagement").
  FILTER regex(str(?ServerType), "ApacheWebServer").
  }
```

Figure 6.10: SPARQL of CQ5

Scenario	Vulnerability	Segment	Server	ServerType	Version	OperatingSystem
Scenario_5	Improper configuration fo	Privileged Access Manag	Server1	ApacheWebServer	"2.2.46"	Ubutu Linux 20.10

Figure 6.11: Output of CQ5

This of course can be expanded, but this was just a proof of concept which can abstract information from the ontology. That gives it a strong usability which is a part of what the ontology needs to have. The only limits for question to use is to have time making them and the persons imagination. Then the scenario would need to be configured with the right syntax with that information. But this is a beginning and a showing what it can do.

6.3 Domain expert review

The domain expert where introduced to the taxonomy to have a view of the concepts and the ontology to see what it could do at this point in time. From that they had certain comment or wishes for what it could do for them. Some where as simple they wanted a simple concept. And some had further comments on what they wanted to see that the ontology could show them or not. And some of them had thoughts for the future. Each valuable comment to the review will be added here with a comment section to see if I agree, dont agree or cant take a stand in this comment.

Concepts	Meaning	Decision
Confidentiality	Is this scenario accessible or only accused with security clearance	Easy understandable concept and some scenarios will be classified. Added
Media/Purple Team	A team generated responsible for dealing with the media in the scenario	Easy understandable concept and some scenarios feature that. Added
Initial Situation	A concept under operation to deal with what is the starting point.	This could be explained by the storyline in the scenario or not clear.
Situational Actors	Actors that only appears if the correct event happens in a scenario	To vague and unclear term. Better as an annotation if needed.
Information Team	A team responsible for bringing updates on the information in the scenario	Can be the white team in some scenarios so no.
Observers	A team watching others doing the scenario	Not critical concept as they don't affect the scenario.
Standardization	Process of implementing standards in the scenario	Not critical enough at this stage. Can be added later or used by other.
Risk Analysis	examining project outcomes and changed due to the impact of the risk	Can be added later if needed. Not critical enough in this stage.
Management Tool	Tools managing data.	Just another category under security tool. Not critical enough at this time.
Surveillance tool	Tools looking over data.	Just another category under security tool. Not critical enough at this time.
Education	What to learn the teams in scenario	There was multiple discussion on what it should be, future work
Exercise	Tabletop, discussion	There was multiple discussion on what it should be, future work
Security Segment	A component that creates a specific security for a product like privileged access management	Yes as it takes up critical instances not addressed elsewhere.

Table 6.3: Table on feedback concerning concepts and perspective changes

First there where some concepts they wished to be added. For simplicity this was made into a table with the concept, what it means and then decision as of now on it.
One feedback was if operation and environment should be own perspectives or under scenario. As those perspectives could be vague was argued.

Those perspectives are clearly explained and makes scenario a more clearer perspective. Most domain expert didn't find it to be an issue. Not added.

Another feedback was having education and exercise as own perspectives or concepts. Here education is what one will get out of it in education of scenario. For exercise it is type of exercise like game, tabletop, discussion and such.

As this was considered to be multiple things in the ontology made it not something that could not be decided at this point in time. So this is a discussion for future work. Although a clear way to deal with education is to make a concept combining type and goal. Or just make a competence question, but syntax ask for type and goal.

A big feedback put on the table was that could this ontology be realistically used in real life and not be a form of database manager.

This is not the scope of the thesis, but a decision on that should be made at a later point. What that is will be relived in future work.

One domain expert commented that military had goals for the cyber range and the ontology had potential to help in that. One of them was representing infrastructure in a large scale. Another was how can the ontology and cyber range scenario help in execute power, educate personnel and improve skills.

The ontology addresses infrastructure and how much data needed in that is decided by the user. For the other section that can also be answered by the ontology. Improving skills would make one find out what is needed to improve and ask

from these scenarios as shown in competency question one. Educate personnel goes hand in hand with improving skills, but can also be a goal of the scenario. For executing power a concept could be made in either scenario or operation explaining power level or potential power gain. But that is a complicated concept to make in this short of time clear so that should be in the future work. Nevertheless many of these goals also depends on what then cyber range decides and how the ontology should be used and will be a future work section.

Operation can mean differently if a person have worked in specific locations and thus can experienced the perspective differently than intended.

What operation means in this context is clearly defined in the thesis if another concept or explanation of different kinds of operation is needed should be future work goal.

A feedback was tho rework some of the node-asset relationship and adding characteristics in properties was suggested. This was argued with that although the ontology is a powerful tool, but if not all these are proper in place the ontology can be broken in expansions later and proven useless.

This is a clear and reasonable feedback of the long term viability of the ontology. As this is not that something that can be fixed in this short amount of time and outside of the competence of what can be done on protege it can make things worse if changing it at this time. This will be covered both in future work and limitation of the ontology

A final feedback was that it is needed a rational for why the ontology. As using ontologies is really necessary if the product doesn't use Reasoner. Then it can just be used a taxonomy.

This feedback can be tackle in multiple ways. But use of Reasoner is a part of the rework that will be done with the previous comment that fits in future work and limitations. But the use of ontology is still needed. And if we are removing the reason that is the goal of thesis there are still some arguments. The main reason is that an ontology answer more what the NCR situation than a taxonomy. And even though Reasoner isn't used at this time the ontology can still be used to abstract knowledge. And with competence question it shows that the ontology can be used at this point in time and answer some questions domain expert can wonder about. And the options with an ontology makes it more likely to be used and developed than a taxonomy. And that potential with future work makes it a good enough rational to develop the first step of an ontology and not just a taxonomy.

6.4 Correctness

For correctness it showed form validation of scenario promising it showed that the critical concept used where correctly used and explained. This is showed in describing ontology chapter.

From the domain experts had some comment. The comments related to correctness if asset where under node or its own concept where also suggested. Also in security perspective it was suggested a missing link to make it more correct, but it wasn't anything suggested in that point.

For the asset it can in the suggestive ontology be correct as it is described and with a scenario it works. For the security comment that cant be really addressed if no one know what it actually is.

The concepts that was tested in the competence questions shows that those concepts where correct. Based on all this tested point the concepts used can be validated fairly in correctness.

6.5 Completeness

For completeness with the used scenario couldn't point at any thing as it was a similar scenario to those used creating the ontology. That will be put in limitation

From interviews they where suggested multiple concepts. All covered in the table above. Some where added and some where not based on decision showed above.

The competence questions didn't help much in completeness. As their is a limit in the competence question and variedness it cant really test completeness at this stage.

With the concepts added from the evaluation and the arguments to those not added their is an argument to be made that is has some completeness. At least when it comes to critical concepts at this point in time. But that is as very vague definition of completeness. As the nature of ontologies makes it always expandable to create new concepts. Depending on that these concepts are clearly defined. And with domain this ontology is under cyber security it also is an expansive domain. A domain that in this point in time looks ever expansive. But when used some criterion and limitations on the scope completeness has been achieved in some sense at this point in time.

Chapter 7

Discussion

This chapter will discuss the research project and see if the thesis was overall successful. The most common and fitting way to do that is looking back at the research questions. As they was build at the beginning of the project it is a sign of progression if those can be answered.

RQ1: What are the main challenges identified in creating scenarios in the NCR?

This was known partially beforehand, but with exploring and discussion with NCR it has been highlighted even more. The NCR main challenges was that there was a lack of cohesion between the personnel working in the different layers. This came from a lack of unified terminology. That led to researchers talking about the same concepts in different ways or using concepts in different ways. So words like vulnerability became for some people a computer bug while other saw it as a structural weakness in an organization.

This is just one example of concepts with different meaning, and that shows the problem of not having a unified terminology. This makes it almost impossible to create multilayered scenarios which the NCR wish to do. Because if the scenario isn't clear and concise enough it will need to cover a lot more data to be useful. Which will takes time to create. And will that even be used by groups. Unnecessary complicated scenarios will not be used and will have very little learning effect. This thesis has answered the first research question of the project.

RQ2: What is an ontology that can help solving the challenges for these stakeholders when working on different layers?

This is what some of the literature review where tasked to find. An ontology is a knowledge management system. Its goal it to be as clear as possible and cover as much of the terminology inside its domain area. That will remove ambiguity and make it as usable as possible. It shares similarity with a taxonomy. But an ontology has a lot more use cases than a taxonomy. Data can extracted from it

and constraints can be used. This will make a system for handling concepts and individuals/instances.

That helps the NCR stakeholders as with the correct labels and constraint one can easily set which layer a concept or an instance is a part of. Then different vulnerabilities in a scenario can be explained without confusing what layer this vulnerability is describing. It will also give a clear knowledge base they can use as a basis for a unified terminology. Gathering the most critical concepts and explain in which setting used it can help in the research working on different layers at the same time. That shows the second research question has been answered by the thesis.

RQ3: How can the ontology be applied in real case scenarios to solve the identified challenges?

This is a part of the evaluation process and needs to be solved. As there is no point creating a product cant be used at all. That would be a waste of time that no one can gain by.

The first way looking at it is to look at what the ontology can do by itself. This is a Scenario Ontology which means one should be able to add a scenario into the ontology. Then the ontology can be described through the scenario. And the scenario has been used in a clear system. And that system consisting of knowledge and concepts can be used as a system for terminology. Meaning when the scenario is used through the ontology it can be given a "stamp" that follows a set of standards agreed upon that is also unified in terms. That means when the ontology is further developed it can be used to solve their challenge as a terminology checker and standardization clearer.

At this point in time it is not fully there. But through future work and mentioning of the limitations it has the potential to be there. For now it can by this be used as can this scenario be explained through this and can critical concepts be added from it if it can fully explain the scenario. But it is a start and a concept on how it can do it. So the research question has been answered based on that it has established a way to do it, even though the ontology isn't fully developed yet to give ideal answers following those steps.

RQ4: How can the ontology be verified for completeness and correctness?

Verifying of the ontology where showed in the evaluation chapter and can fully explored there so only a brief dip will be given here.

Correctness is validation of the concepts is used in correct and correctly explain the scenarios that are using the ontology. This is mainly done by using scenarios

in the ontology and when tested with competence question on the ontology that gives the correct or the expected answer when queried into sparql. When adding scenarios to the ontology showed the concepts in a correct manner. And when using the competence questions it also gave the expected answers. So a level of correctness has been achieved and how to do it has been explained.

For completeness it's can the ontology fully explain its content with the critical concepts chosen. For that one will have to look at using it for scenarios again and comments from domain expert reviews. When used on a scenario it is showed that the concepts chosen could completely explain the scenarios in question if one would only look at the critical concepts. For the domain reviews there where some comments on concepts that could be added for completeness, but overall the ontology served fine in this regard. Those concepts and evaluation of those can be found in domain expert review section. But again it shows that there is a method to validate for completeness and for limit scope of critical concept the completeness has been partly satisfied.

Based on that the final research question has also been answered by the thesis. Which means all research questions has been accounted and answered by this research. This is a sign of a research that has been developed and usable based on the limits of the research questions

Chapter 8

Conclusion

A conclusion summarize the work done in the thesis and makes a conclusion. But before one can conclude on will need to explore what didn't the ontology cover in. That is taken up either in the limitation or in the future work section.

8.1 Limitations of the Research

Of course one would like to pick a topic that will change the world and has no setback when it is done. But, like many other things, there are limitations to this work that need to be addressed. This section will explore those limitations.

The first limitations is in the issue of time. Usually an ontology is created within the scope of a year for proper evaluations and expansions of it. This thesis was done in a period of three months. That will limit what the ontology can achieve or do. And as ontology and protege were new concepts, time was also used in understanding and learning how to use those tools. That limits the possibility of getting a complete ontology. That made into the factor why some concepts wasn't explored or perspectives wasn't considered. So with a time restraint of a more normal thesis length one would see even more results and more thorough work on the ontology.

Another limitation is things the ontology don't use as a constraint to time. There are not many constraints used and no use of characteristics in the properties. These are things| that if not use properly can cripple an ontology if not developed when processing it further. With further time and training in the tool that would be something that would have been implemented.

Another limitation is not using reasoner. Reasoner is one of the key things to use if making an ontology. But at this stage in time it wasn't the most critical for this project to be implemented. The first step is to create an ontology that works and be further developed. Reasoner will have to come later.

Another limitation is the lack of testing with full scenarios. Although a lot of scenarios were collected. Some were fully used for abstraction to create the ontology and some only had bits of information added. And fewer where either used for full scale testing or partial testing. With more time there would have been dedicated more time in using more full scenarios to describe and test the ontology. As it is a vital component in testing an using the ontology that it can be used properly by actually putting it to the test against scenarios that is what its made for.

A final limitation lies is not a way to use it outside of protege and another ontology application for full usage. Protege is a powerful tool, but its syntax needs to be learned and it is not realistic that all stakeholders will learn or should learn for applying it to realistic use. Either finding or creating a scenario. This is not in the scope of the thesis, but a suggestion to that problem has been suggested in the future work section.

8.2 Future work

This chapter will be revolving on thing that can or needs to be worked at further with the ontology in the future. That is to strengthen the ontology and make it even more usable to be used for the NCR.

Firstly, one would be expanding the ontology. That would come naturally by no ontology is completed fully and will be developed further. This can be in adding concepts or perspectives. Some of them where suggested in the domain expert review. Some of them can be things not considered and some things might not be existing yet. But if things will be added there must be a discussion around it to make sure all new entries are clearly and completes the ontology more.

Secondly, the application as well as the the usability of the ontology can be achieved through creating a web application that works with the ontology. That web application should provide facilities in manipulating the ontology, including creating/querying/managing scenarios. This will help improve the usability of the ontology, which was suggested by the NCR experts. That will help with the usability and how many potential will be able to use the ontology. NCR has some internal solutions for web applications so it should be not a problem expanding its usage with a web application.

Thirdly, further development with the ontology would also see a quantitative testing where time can allow for testing and bigger multiple situations outside the scope of this thesis. That is something that will be worked on to prove further the usage of the ontology. As the ontology wont be able to expand without using more scenarios to test it. Especially varied scenarios so one can test the endpoints of the

ontology. That would make it possible to expand the ontology.

Fourthly, more enhancement would be using more of the features of the ontology to strengthen its potential. That would be adding restrictions in the properties itself, adding characteristics to them, make a revamp of used properties and start using reasoner. From there one can eliminate possible setbacks with the ontology in the future and using all the strength of the ontology. That would only be beneficial for quicker achieving the NCR goal for creating such a product.

Finally, a further research work could see the scenario ontology be adapted to simple exercises in the NCR. Although it is far from making multilayered scenarios or exercises it would be needed at a point to test if the ontology can go the leap from stamping a scenario and then used as a simple exercise in the NCR. That would also help validating weak points if at that time there are still noticeable limitation in the ontology.

Ultimately the final future work would be achieving ncr goal that they can develop complex and multiple layered scenarios. An ontology is just a start for clearing up and making a stage ground possible for creating them.

8.3 Concluding Remark

By the scope of this an ontology was made. Although it has it limitations needed to be addressed in future. So not a complete ontology, but a beginning and a workable ontology that can developed further.

Though the project also answered the research questions that suggest a completed project. Overall an ontology has been crated and it is up to NCR to take it to use and develop it for further use. But what they have got is still a powerful that can help them starting that work. And that tells the power of a viable ontology.

Chapter 9

Appendix

Here will data, extra text code and documentation be added in full unlike a snip where it is described in the thesis itself.

9.1 Scenarios Used

Here will the links to the scenarios used in the creation or use of the ontology be added. Those scenario being Atlantic council cyber 9/20 Geneva scenario 1 [20] and Locked Shield 2013 [6]

9.2 Ontology Dataset

Here is the dataset of the ontology in xml:
<?xml version="1.0"?> <rdf:RDF xmlns="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenario" xml:base="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenario" xmlns:owl="http://www.w3.org/2002/07/owl" xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns" xmlns:xml="http://www.w3.org/XML/1998 xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema"> <owl:Ontology rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology Scenario"> <owl:versionIRI rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ont Scenario/3.0"/> </owl:Ontology>
<!– // // // Annotation properties // // –>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLayer –>
<owl:AnnotationProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology ScenarioLayer"> <rdfs:subPropertyOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategical$_layer$"/ >< $/owl : AnnotationProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPerspective

–>
<owl:AnnotationProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology
ScenarioPerspective"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategical$_layer$–
– >
<owl:AnnotationProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology
ScenarioStrategical$_layer$" >< $rdfs : subPropertyOf rdf : resource = "http :$
$//www.w3.org/2000/01/rdf-schemalabel$"/ >< $/owl : AnnotationProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTactical$_layer$–
– >
<owl:AnnotationProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology
ScenarioTactical$_layer$" >< $rdfs : subPropertyOf rdf : resource = "http :$
$//www.w3.org/2000/01/rdf-schemalabel$"/ >< $/owl : AnnotationProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTechnical$_layer$–
– >
<owl:AnnotationProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology
ScenarioTechnical$_layer$" >< $rdfs : subPropertyOf rdf : resource = "http :$
$//www.w3.org/2000/01/rdf-schemalabel$"/ >< $/owl : AnnotationProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariolayer
–>
<owl:AnnotationProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology
Scenariolayer"/>
<!– ///
// // Object Properties // ///
–>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAssetProtectedBy
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioAssetProtectedBy"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioaChallengeIs
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioaChallengeIs"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioaTemdontwantto
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioaTemdontwantto"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioTeam"/> <rdfs:range rdf:resource="http://www.semanticweb.o
/ontologies/2020/10/Ontology-ScenarioTeam"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioaffects
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
Scenarioaffects"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioActivity"/> <rdfs:domain rdf:resource="http://www.semanticw

/ontologies/2020/10/Ontology-ScenarioInfected$_S ystems$"/ >< $rdfs : domainrdf$: $resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioThreat$"/ >< $rdfs : rangerdf : resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology - ScenarioAgent$"/ >< $rdfs : rangerdf$: $resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioAsset$"/ >< $rdfs : rangerdf : resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioInfrastructure$"/ >< $rdfs : rangerdf$: $resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioTeam$"/ >< $/owl : ObjectProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioassetProtectedIs –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioassetProtectedIs"> <rdfs:subPropertyOf rdf:resource="http://www.w3.org/2002/07/owltopObje
</owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioattackerAttacks –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioattackerAttacks"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariobased$_O n$– – >
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariobased$_O n$" >< $rdfs : domainrdf : resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology–ScenarioGoal$"/ >< $/owl : ObjectProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariobelongsToArena –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariobelongsToArena"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <rdfs:range rdf:resource="http://www.semanticwe
/ontologies/2020/10/Ontology-ScenarioArena"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioblueTeamsProtectsFrom –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioblueTeamsProtectsFrom"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioBlue$_T eam$"/ >< $rdfs : rangerdf : resource =$ $"http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology–ScenarioAsset$"/ >< $/owl : ObjectProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariocauses –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariocauses"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEvent"/> <rdfs:range rdf:resource="http://www.semanticweb.o
/ontologies/2020/10/Ontology-ScenarioThreat"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariocontains –>

<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariocontains"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEvent"/> <rdfs:domain rdf:resource="http://www.semanticweb /ontologies/2020/10/Ontology-ScenarioOperation"/> <rdfs:domain rdf:resource="http://www.semantic /ontologies/2020/10/Ontology-ScenarioRisk"/> <rdfs:range rdf:resource="http://www.semanticweb.org /ontologies/2020/10/Ontology-ScenarioActivity"/> <rdfs:range rdf:resource="http://www.semanticweb /ontologies/2020/10/Ontology-ScenarioConsequence"/> <rdfs:range rdf:resource="http://www.semant /ontologies/2020/10/Ontology-ScenarioEvent"/> <rdfs:range rdf:resource="http://www.semanticweb.o /ontologies/2020/10/Ontology-ScenarioInjection"/> <rdfs:range rdf:resource="http://www.semanticwe /ontologies/2020/10/Ontology-ScenarioObjective"/> <rdfs:range rdf:resource="http://www.semanticwe /ontologies/2020/10/Ontology-ScenarioStoryline"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioexpertTeamInvestigate –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioexpertTeamInvestigate"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioexploits –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioexploits"> <rdfs:subPropertyOf rdf:resource="http://www.w3.org/2002/07/owltopObjectPrope <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioThreat"/> <rdfs:range rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioVulnerability"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioharms –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioharms"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRisk"/> <rdfs:range rdf:resource="http://www.semanticweb.org /ontologies/2020/10/Ontology-ScenarioOrganization"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariohas –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariohas"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAsset"/> <rdfs:domain rdf:resource="http://www.semanticweb /ontologies/2020/10/Ontology-ScenarioEnvironment"/> <rdfs:domain rdf:resource="http://www.sema /ontologies/2020/10/Ontology-ScenarioEvent"/> <rdfs:domain rdf:resource="http://www.semanticweb /ontologies/2020/10/Ontology-ScenarioInfected$_S ystems$"/ >< $rdfs : domainrdf$: $resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioNode$"/ >< $rdfs : domainrdf : resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioObjective$"/ >< $rdfs : domainrdf$: $resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioOperation$"/ >< $rdfs : domainrdf : resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioOrganization$"/ >< $rdfs : domainrdf$: $resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioSecurity$"/ >< $rdfs : domainrdf : resource = "http : //www.semanticweb.org/john-$

/ontologies/2020/10/Ontology − ScenarioTeam”/ >< rdfs : domainrdf :
resource = ”http : //www.semanticweb.org/john−/ontologies/2020/10/Ontology−
ScenarioVulnerability”/ >< rdfs : rangerdf : resource = ”http : //www.semanticweb.org/john−
/ontologies/2020/10/Ontology − ScenarioActivity”/ >< rdfs : rangerdf :
resource = ”http : //www.semanticweb.org/john−/ontologies/2020/10/Ontology−
ScenarioAgent”/ >< rdfs : rangerdf : resource = ”http : //www.semanticweb.org/john−
/ontologies/2020/10/Ontology − ScenarioArtifact”/ >< rdfs : rangerdf :
resource = ”http : //www.semanticweb.org/john−/ontologies/2020/10/Ontology−
ScenarioAssumption”/ >< rdfs : rangerdf : resource = ”http : //www.semanticweb.org/john−
/ontologies/2020/10/Ontology−ScenarioAttack$_v$ector”/ >< rdfs : rangerdf :
resource = ”http : //www.semanticweb.org/john−/ontologies/2020/10/Ontology−
ScenarioConfiguration”/ >< rdfs : rangerdf : resource = ”http : //www.semanticweb.org/john−
/ontologies/2020/10/Ontology − ScenarioExploit”/ >< rdfs : rangerdf :
resource = ”http : //www.semanticweb.org/john−/ontologies/2020/10/Ontology−
ScenarioInfrastructure”/ >< rdfs : rangerdf : resource = ”http : //www.semanticweb.org/john−
/ontologies/2020/10/Ontology−ScenarioLikelihood”/ >< rdfs : rangerdf :
resource = ”http : //www.semanticweb.org/john−/ontologies/2020/10/Ontology−
ScenarioNode”/ >< rdfs : rangerdf : resource = ”http : //www.semanticweb.org/john−
/ontologies/2020/10/Ontology−ScenarioObjective”/ >< rdfs : rangerdf :
resource = ”http : //www.semanticweb.org/john−/ontologies/2020/10/Ontology−
ScenarioPolicy”/ >< rdfs : rangerdf : resource = ”http : //www.semanticweb.org/john−
/ontologies/2020/10/Ontology−ScenarioRisk”/ >< rdfs : rangerdf : resource =
”http : //www.semanticweb.org/john−/ontologies/2020/10/Ontology−ScenarioSecurity$_T$ool”/ >
rdfs : rangerdf : resource = ”http : //www.semanticweb.org/john−/ontologies/2020/10/Ontolog
ScenarioServer”/ >< rdfs : rangerdf : resource = ”http : //www.semanticweb.org/john−
/ontologies/2020/10/Ontology−ScenarioStoryline”/ >< rdfs : rangerdf :
resource = ”http : //www.semanticweb.org/john−/ontologies/2020/10/Ontology−
ScenarioTeam”/ >< rdfs : rangerdf : resource = ”http : //www.semanticweb.org/john−
/ontologies/2020/10/Ontology−ScenarioVulnerability”/ >< /owl : ObjectProperty >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasEnvironmentalComp
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenariohasEnvironmentalComponent"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john
/ontologies/2020/10/Ontology-ScenarioScenario"/> <rdfs:range rdf:resource="http://www.semanticwe
/ontologies/2020/10/Ontology-ScenarioEnvironment"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasEvent
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenariohasEvent"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasGoal
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenariohasGoal"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> <rdfs:range rdf:resource="http://www.semanticwe

/ontologies/2020/10/Ontology-ScenarioGoal"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasMalware
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasMalware"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasSecurityProperty
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasSecurityProperty"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAsset"/> <rdfs:range rdf:resource="http://www.semanticweb.o/ontologies/2020/10/Ontology-ScenarioCIA"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasSeverity
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasSeverity"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasVulnerability
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariohasVulnerability"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironment"/> <rdfs:range rdf:resource="http://www.semant/ontologies/2020/10/Ontology-ScenarioVulnerability"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariohas$_O bjective$–
– >
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariohas$_O bjective$”/ >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioinTheSegmentOf
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioinTheSegmentOf"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioVulnerability"/> <rdfs:range rdf:resource="http://www.semanti/ontologies/2020/10/Ontology-ScenarioSecuritySegment"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioincludes
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioincludes"> <rdfs:range rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioGoal"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioincludesStrategy
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioincludesStrategy"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecuritySegment"/> <rdfs:range rdf:resource="http://www.sem/ontologies/2020/10/Ontology-ScenarioStrategy"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioinfrastructureAffectedIs
–>

<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioinfrastructureAffectedIs"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioinfrastructure$_A ttacked_b$
– >
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioinfrastructure$_A ttacked_b y$"/ >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariointeract$_W ith$–
– >
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariointeract$_W ith$" >< $rdfs : domain rdf : resource =$ "$http : //www.semanticweb.org/john$–
$/ontologies$/2020/10/$Ontology – ScenarioService$"/ >< $/owl : ObjectProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioisRealizedBy
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioisRealizedBy"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEvent"/> <rdfs:range rdf:resource="http://www.semanticweb.o/ontologies/2020/10/Ontology-ScenarioRisk"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioisSecretLevel
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioisSecretLevel"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioisTypeOf
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioisTypeOf"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioServer"/> <rdfs:range rdf:resource="http://www.semanticweb./ontologies/2020/10/Ontology-ScenarioApplicationServerType"/> <rdfs:range rdf:resource="http://ww/ontologies/2020/10/Ontology-ScenarioDatabaseServer"/> <rdfs:range rdf:resource="http://www.sema/ontologies/2020/10/Ontology-ScenarioWebServerType"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioleadsTo
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioleadsTo"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioVulnerability"/> <rdfs:range rdf:resource="http://www.semanti/ontologies/2020/10/Ontology-ScenarioRisk"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariomakes
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariomakes"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioThreat"/> <rdfs:domain rdf:resource="http://www.semanticwe/ontologies/2020/10/Ontology-ScenarioVulnerability"/> <rdfs:range rdf:resource="http://www.semanti/ontologies/2020/10/Ontology-ScenarioRisk"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariomitigates
–>

<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariomitigates"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioVulnerability"/> <rdfs:range rdf:resource="http://www.semanti/ontologies/2020/10/Ontology-ScenarioControl"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariomodifies –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariomodifies"> <rdfs:subPropertyOf rdf:resource="http://www.w3.org/2002/07/owltopObjectPrope
<rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioControl"/> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEvent"/> <rdfs:range rdf:resource="http://www.semanticweb.o/ontologies/2020/10/Ontology-ScenarioConsequence"/> <rdfs:range rdf:resource="http://www.semant/ontologies/2020/10/Ontology-ScenarioRisk"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariomust$_C$omplete– –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariomust$_C$omplete" >< $rdfs : domainrdf : resource = "http : //www.semanticweb.org/john–$ $/ontologies/2020/10/Ontology - ScenarioTeam"/ >< rdfs : rangerdf :$ $resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–$ $ScenarioChallenge"/ >< /owl : ObjectProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariomust$_F$ollow– –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariomust$_F$ollow" >< $rdfs : domainrdf : resource = "http : //www.semanticweb.org/john–$ $/ontologies/2020/10/Ontology - ScenarioTeam"/ >< rdfs : rangerdf :$ $resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–$ $ScenarioRules"/ >< /owl : ObjectProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioowns –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioowns"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOrganization"/> <rdfs:range rdf:resource="http://www.semant/ontologies/2020/10/Ontology-ScenarioAsset"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariopcProtecteBy –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariopcProtecteBy"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAsset"/> <rdfs:range rdf:resource="http://www.semanticweb.o/ontologies/2020/10/Ontology-ScenarioBlue$_T$eam"/ >< $/owl : ObjectProperty >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioprotectsAsset –>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioprotectsAsset"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioBlue$_T$eam"/ >< $rdfs : rangerdf : resource =$

”$http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAsset$”/ >< /owl : $ObjectProperty$ >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariorelatesToSecurityConcep
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariorelatesToSecurityConcept"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <rdfs:range rdf:resource="http://www.semanticwe/ontologies/2020/10/Ontology-ScenarioSecurity"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariorelatesToSecuritySegmer
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariorelatesToSecuritySegment"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <rdfs:range rdf:resource="http://www.semanticwe/ontologies/2020/10/Ontology-ScenarioSecuritySegment"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariorelatesToVulnerability
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariorelatesToVulnerability"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <rdfs:range rdf:resource="http://www.semanticwe/ontologies/2020/10/Ontology-ScenarioVulnerability"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariosecured$_By$−
− >
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariosecured$_By$” >< $rdfs : domainrdf : resource =$ ”$http://www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioEnvironment$”/ >< $rdfs : rangerdf : resource =$ ”$http://www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioSecurity_Tool$”/ >< /$owl : ObjectProperty$ >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariotargeted$_By$−
− >
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariotargeted$_By$” >< $rdfs : domainrdf : resource =$ ”$http://www.semanticweb.org/john-/ontologies$/2020/10/$Ontology - ScenarioAgent$”/ >< $rdfs : domainrdf : resource =$ ”$http://www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioRisk$”/ >< /$owl : ObjectProperty$ >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioteamProtects
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioteamProtects"> <rdfs:range rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTeam"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariotypeofScenarioIs
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariotypeofScenarioIs"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <rdfs:range rdf:resource="http://www.semanticwe

/ontologies/2020/10/Ontology-ScenarioType"/> </owl:ObjectProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenariousesOperatingSystem
–>
<owl:ObjectProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenariousesOperatingSystem"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioServer"/> <rdfs:range rdf:resource="http://www.semanticweb.
/ontologies/2020/10/Ontology-ScenarioOperatingSytem"/> </owl:ObjectProperty>
<!– ///
// // Data properties // //
–>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironmentAsset
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioEnvironmentAsset"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironmentConfigurati
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioEnvironmentConfiguration"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironmentSecurityToo
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioEnvironmentSecurityTool"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironmentServer
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioEnvironmentServer"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvrionmentInfrastructu
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioEnvrionmentInfrastructure"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEventLikelihood
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioEventLikelihood"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLongDescription
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioLongDescription"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationActivity

–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationActivity"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationConsequence
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationConsequence"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationEvent
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationEvent"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationInjection
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationInjection"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationObjective
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationObjective"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationPhases
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperationPhases"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioArtifact
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioArtifact"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioAssumption
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioAssumption"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioChallenge
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioChallenge"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioGoal
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioScenarioGoal"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioImpact
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioScenarioImpact"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioPolicy
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioScenarioPolicy"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioRules
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioScenarioRules"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenarioStoryLine
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioScenarioStoryLine"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurityAffectedSystems
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioSecurityAffectedSystems"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurityAttackVector
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioSecurityAttackVector"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurityControl
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioSecurityControl"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurityExploit
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioSecurityExploit"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-

/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurityICIA
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioSecurityICIA"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurityRisk
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioSecurityRisk"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurityThreat
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioSecurityThreat"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioShortDescription
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioShortDescription"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStakeholderAffectedActo
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioStakeholderAffectedActors"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStakeholderOrganizatio
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioStakeholderOrganization"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStakeholderSuspectedAg
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioStakeholderSuspectedAgent"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStakeholderTeam
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioStakeholderTeam"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:DatatypeProperty>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioVersion
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioVersion"/>

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioVulnerabilities
–>
<owl:DatatypeProperty rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioVulnerabilities"> <rdfs:domain rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioVulnerability"/> </owl:DatatypeProperty>
<!– ///
// // Classes // ///
–>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioActivity
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioActivity"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioOperation"/> <layer>Technical</layer>
</owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAgent
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioAgent"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioStakeholder"/> <layer>Strategical</layer>
<layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioApplicationServerType
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioApplicationServerType"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioServer"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioArena
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioArena"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> <layer>Strategical</layer>
</owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioArtifact
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioArtifact"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioScenario"/> <layer>Strategical</layer>
<layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAsset
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioAsset"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioNode"/> <layer>Strategical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAssumption
–>

<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAssumption"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAttack$_v ector$– –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAttack$_v ector$" >< $rdfs : subClassOf\, rdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioSecurity"/ >< layer > Technical <$ $/layer >< /owl : Class >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioBlue$_T eam$– –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioBlue$_T eam$" >< $rdfs : subClassOf\, rdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology − ScenarioTeam"/ >< /owl : Class >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCIA –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCIA"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioChallenge –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioChallenge"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioClassifcation –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioClassifcation"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioConfiguration –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioConfiguration"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInfrastructure"/> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioConsequence –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioConsequence"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInfected$_S ystems$"/ >< $rdfs : subClassOf\, rdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioOperation"/ >< layer > Strategical < /layer >< layer > Tactical < /layer >< /owl : Class >$

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioControl
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioControl"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity"/> <layer>Strategical</layer>
<layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioDatabaseServer
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioDatabaseServer"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioServer"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioDomain
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioDomain"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <layer>Strategical</layer>
<layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironment
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironment"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEvent
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEvent"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperation"/> <layer>Strategical</layer>
<layer>Tacitcal</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioExpert$_T eam$–
– >
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioExpert$_T eam$" >< $rdfs:subClassOf\ rdf:resource = "http://www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioTeam$"/ >< $/owl:Class$ >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioExploit
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioExploit"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity"/> <layer>Strategical</layer>
<layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioGoal
–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioGoal"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <layer>Strategical</layer>
<layer>Technical</layer> </owl:Class>

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioImpact –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioImpact"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity"/> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInfected$_S ystems$– –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInfected$_S ystems$" >< $rdfs : subClassOf rdf : resource = "http : //www.semanticweb.org/john–/ontologies$/2020/10/$Ontology–ScenarioVulnerability$"/ >< $layer > Tactical < /layer ><$ /owl : Class >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInfrastructure –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInfrastructure"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironment"/> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInjection –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInjection"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEvent"/> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInsider$_a ttack$– –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInsider$_a ttack$" >< $rdfs : subClassOf rdf : resource = "http : //www.semanticweb.org/john-/ontologies$/2020/10/$Ontology–ScenarioAttack_v ector$"/ >< $/owl : Class >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLikelihood –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLikelihood"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEvent"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioMalware –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioMalware"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAttack$_v ector$"/ >< $/owl : Class >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNetwork –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNetwork"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInfrastructure"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNode

–>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNode"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironment"/> <layer>Strategical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioObjective –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioObjective"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperation"/> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperatingSytem –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperatingSytem"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironment"/> <rdfs:label>Operating System</rdfs:label> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperation –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOperation"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOrganization –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOrganization"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStakeholder"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPolicy –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPolicy"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <layer>Strategical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPurple$_T$eam– –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPurple$_T$eam" >< $rdfs:subClassOf\ rdf:resource = "http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTeam"/ >< /owl:Class >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRed$_T$eam– –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRed$_T$eam" >< $rdfs:subClassOf\ rdf:resource = "http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTeam"/ >< /owl:Class >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRisk –>

<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRisk"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity"/> <layer>Strategical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRules –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRules"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPolicy"/> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecuritySegment –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecuritySegment"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity"/> <rdfs:label>Security Segment</rdfs:label> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity$_{T}ool$– – >
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity$_{T}ool$" >< $rdfs:subClassOf\ rdf:resource = "http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironment"/ >< layer > Technical < /layer >< /owl : Class >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioServer –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioServer"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInfrastructure"/> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioService –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioService"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnvironment"/> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSource –>

<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSource"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStakeholder –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStakeholder"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStoryline –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStoryline"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategical$_{d}omain$– –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategical$_{d}omain$" >< $rdfs$: $subClassOf$ rdf : $resource$ = "$http$: //$www.semanticweb.org$/$john$–/$ontologies$/2020/10/$Ontology$–$ScenarioDomain$"/ >< /owl : $Class$ >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategy –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategy"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTeam –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTeam"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStakeholder"/> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTechnical$_{d}omain$– –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTechnical$_{d}omain$" >< $rdfs$: $subClassOf$ rdf : $resource$ = "$http$: //$www.semanticweb.org$/$john$–/$ontologies$/2020/10/$Ontology$–$ScenarioDomain$"/ >< /owl : $Class$ >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioThreat –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioThreat"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity"/> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioType –>

<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioType"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario"/> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioVulnerability –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioVulnerability"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity"/> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWebServerType –>
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWebServerType"> <rdfs:subClassOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioServer"/> </owl:Class>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWhite$_T eam$– – >
<owl:Class rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWhite$_T eam$" >< $rdfs : subClassOf\ rdf : resource = "http : //www.semanticweb.org/john-/ontologies/$2020/10/$Ontology - ScenarioTeam$"/ >< $/owl : Class >$
<!– http://www.w3.org/2002/07/owlThing –>
<owl:Class rdf:about="http://www.w3.org/2002/07/owlThing"/>
<!– // // // Individuals // // –>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAccountGovernance –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAccountGovernance"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategy"/> <rdfs:label>Account Governance</rdfs:label> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioApacheTomcat –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioApacheTomcat"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWebServerType"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioApacheWebServer –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioApacheWebServer"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWebServerType"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAtlantic$_C ouncil$– – >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-

ScenarioAtlantic$_{C}ouncil$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$
$/ontologies/2020/10/Ontology-ScenarioSource"/ >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAttack$_{o}n_{o}utdated_{s}yste$
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioAttack$_{o}n_{o}utdated_{s}ystems$" >< $rdf : typerdf : resource = "http :$
$//www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioThreat"/ ><$
$rdfs : comment > Manyattackstargetssystemsthatareusingolderthancurrentversion. <$
$/rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAttacker
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioAttacker"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAtttack$_{o}n_{p}ower_{d}istrbut$
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioAtttack$_{o}n_{p}ower_{d}istrbution_{s}ystems$" >< $rdf : typerdf : resource =$
$"http : //www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioThreat"/ ><$
$/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAvaliability
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioAvaliability"> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioCIA"/> <rdfs:comment>Data and con-
trol system not available.</rdfs:comment> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioBackdoor
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioBackdoor"> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioExploit"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioBad$_{r}outines$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioBad$_{r}outines$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$
$/ontologies/2020/10/Ontology-ScenarioExploit"/ >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioBriefings
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioBriefings"> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioActivity"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCTF
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioCTF"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontolo

ScenarioType"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCapture$_t he_f lag$—
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioCapture$_t he_f lag$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john$—
$/ontologies$/2020/10/$Ontology$—$ScenarioObjective$"/ >< $/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCode
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioCode"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Onto
ScenarioAsset"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCode$_w ith_s olution$—
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioCode$_w ith_s olution$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john$—
$/ontologies$/2020/10/$Ontology$—$ScenarioArtifact$"/ >< $layer >$ *Technical* <
$/layer >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCompromised$_s tructure$
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioCompromised$_s tructure$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/joh$
$/ontologies$/2020/10/$Ontology$—$ScenarioVulnerability$"/ >< $layer >$ *Strategical* <
$/layer >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioConfidentiality
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioConfidentiality"> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioCIA"/> <rdfs:comment>data poetentialy
out and accesible for people when it shouldnt be</rdfs:comment> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioConsultant
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioConsultant"> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioExpert$_T eam$"/ >< $/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioControl$_c enter$—
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioControl$_c enter$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john$—
$/ontologies$/2020/10/$Ontology$—$ScenarioInfected_S ystems$"/ >< $/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioControl$_d ata$—
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioControl$_d ata$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john$—
$/ontologies$/2020/10/$Ontology - ScenarioAsset$"/ >< $rdfs : comment >$

$Datainacontrolsystem.Couldbeanassest. < /rdfs:comment >< /owl:NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioControl$_system$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioControl$_system$" >< $rdf:typerdf:resource = ”http://www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–ScenarioNode”/ >< rdf:typerdf:resource =$
$”http://www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioTechnical_domain”$
$rdfs:comment > Theoverallsystemsusedinspecficinfrastructure. < /rdfs:$
$comment >< /owl:NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCoopeoration$_between_st$
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCoopeoration$_between_states$" >< $rdf:typerdf:resource = ”http:$
$//www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioInfrastructure”/ ><$
$layer > Strategical < /layer >< rdfs:comment > Somestatessharesastructuralinfrastructureto$
$/rdfs:comment >< /owl:NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCredentialManagement
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCredentialManagement"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategy"/> <rdfs:label>Credential Management</rdfs:label> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCyber9_12–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCyber9_12" >< $rdf:typerdf:resource = ”http://www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–ScenarioArena”/ >< layer > Strategical <$
$/layer >< rdfs:label > Cyber9/12 < /rdfs:label >< /owl:NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCyber$_attack$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCyber$_attack$" >< $rdf:typerdf:resource = ”http://www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology − ScenarioImpact”/ >< rdfs:comment >$
$Attackonsystemsusingcomponentsfromquot;cyberspacequot;< /rdfs:comment >< $
$/owl:NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioDNS
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioDNS"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioConfiguration"/> <rdfs:comment>Is a service and some places an asset</rdfs:comment> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioDOS
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-

ScenarioDOS"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontol
ScenarioRisk"/> <rdfs:comment>Denial of service is a risk that can happen.</rdfs:comment>
</owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioData$_c entral$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioData$_c entral$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john$–
$/ontologies$/2020/10/$Ontology$–$ScenarioInfectedSystems$"/ >< $/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioData$_c ontrol_c ode$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioData$_c ontrol_c ode$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john$–
$/ontologies$/2020/10/$Ontology$–$ScenarioInfrastructure$"/ >< $layer > Tactical <$
$/layer >< layer > Technical < /layer >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioDefender
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioDefender"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEU
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioEU"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontolog
ScenarioAgent"/> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioStrategical$_d omain$"/ >< $rdfs : comment >$
$EUisanagentusedinmanyscenariosasanagentorastrategicdomainarea. < /rdfs :$
$comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEnergy$_s upply_c hain$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioEnergy$_s upply_c hain$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john$–
$/ontologies$/2020/10/$Ontology$–$ScenarioInfrastructure$"/ >< $layer > Strategical <$
$/layer >< rdfs : comment > Powerplantandgaspipelinesaresuppliersof powerinachain <$
$/rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioExperts
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioExperts"> <layer>Strategical</layer> <layer>Tactical</layer> <layer>Technical</layer>
<rdfs:comment>Each group member in cyber 9/12 has a domain where their are
experts in</rdfs:comment> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioFind$_p urputrator$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioFind$_p urputrator$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john$–
$/ontologies$/2020/10/$Ontology - ScenarioGoal$"/ >< $LongDescription ><$

/LongDescription >< ShortDescription >< /ShortDescription >< /owl :
NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioForensic$_a$nalysis–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioForensic$_a$nalysis" >< rdf : typerdf : resource = "http : //www.semanticweb.org/john–
/ontologies/2020/10/Ontology–ScenarioActivity"/ >< /owl : NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioFriendliePixie
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioFriendliePixie"> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioMalware"/> <hasSeverity rdf:resource="http://www.semanticw
/ontologies/2020/10/Ontology-ScenarioMedium"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioGet$_t$he$_s$ystem$_b$ack$_u$p$_r$un
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioGet$_t$he$_s$ystem$_b$ack$_u$p$_r$unning" >< rdf : typerdf : resource = "http :
//www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioObjective"/ ><
rdfs : comment > Makethesystemsusuableagain. < /rdfs : comment ><
/owl : NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioGoal1
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioGoal1"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Onto
ScenarioGoal"/> <rdfs:label>My Goal</rdfs:label> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioHigh
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioHigh"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontol
ScenarioLikelihood"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioIIS
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioIIS"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontolog
ScenarioWebServerType"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioImproperConfigurationF
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioImproperConfigurationForDefaultAccount"> <rdf:type rdf:resource="http://www.semanticweb.c
/ontologies/2020/10/Ontology-ScenarioVulnerability"/> <inTheSegmentOf rdf:resource="http://www.s
/ontologies/2020/10/Ontology-ScenarioPrivilegedAccessManagement"/> <rdfs:label>Improper
configuration for default accounts</rdfs:label> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInefficent$_s$ystems–
– >

<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInefficent$_systems$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$ $/ontologies/2020/10/Ontology-ScenarioVulnerability"/ >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInformation –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInformation"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAsset"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInformation$_gathering$– – >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInformation$_gathering$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john$ $/ontologies/2020/10/Ontology-ScenarioObjective"/ >< rdfs : comment >$
$Informationgatheringaboutthesituationaroundandontheattack. < /rdfs :$
$comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInsider$_attack$– – >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInsider$_attack$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$ $/ontologies/2020/10/Ontology-ScenarioThreat"/ >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioIntegrity –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioIntegrity"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCIA"/> <rdfs:comment>Cyber 9/12 Integrity: NisPower datasystem are compromised and cant be trusted to work even if getting access to it</rdfs:comment> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInternational$_agent_might$– – >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInternational$_agent_might_intervene.$" >< $rdf : typerdf : resource =$
$"http : //www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioConsequence"/ >$<
$rdfs : comment > Ifascenarioaffectsmorethanastate, othergroupsorstatesmightwanttointervene$
$/rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioKarl –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioKarl"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontolo ScenarioBlue$_team$"/ >< /owl : NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLack$_of_security_policy$– – >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLack$_of_security_policy$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$ $/ontologies/2020/10/Ontology-ScenarioVulnerability"/ >< layer > Strategical <$

/layer >< /owl : NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLeastPrivilegeEnforceme
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioLeastPrivilegeEnforcement"> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioStrategy"/> <rdfs:label>Least Privilege
Enforcement</rdfs:label> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLinux
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioLinux"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Onto
ScenarioServer"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLockshield$_2$013–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioLockshield$_2$013" >< $layer > Tactical < /layer >< layer > Technical <
/layer >< $rdfs : comment > Isascenario < /rdfs : comment >< /owl :
NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLogin$_m$aterials–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioLogin$_m$aterials" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology - ScenarioAsset"/ >< rdfs : comment >$
$Datacollectedtousefor loginlikelogincredentialinadatabase < /rdfs : comment >< $
$/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLoose$_s$cenario–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioLoose$_s$cenario" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology - ScenarioGoal"/ >< rdfs : comment >$
$Onecanlooseascenarioandtheirshouldbesomethingforthat. < /rdfs : comment >< $
$/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLoss$_o f_c$ontrol–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioLoss$_o f_c$ontrol" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–ScenarioConsequence"/ >< rdfs : comment >$
$Anattackcanleadtolossofcontrolofsystems. < /rdfs : comment >< /owl :$
$NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLoss$_o f_d$ata–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioLoss$_o f_d$ata" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–ScenarioConsequence"/ >< /owl : NamedIndividual >$

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLow
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLow"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontolo ScenarioLikelihood"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioMalware$_attack$– – >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioMalware$_attack$" >< $rdf:typerdf:resource = "http://www.semanticweb.org/john–/ontologies$/2020/10/$Ontology–ScenarioThreat$"/ >< /owl:NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioMedium
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioMedium"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLikelihood"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioMeetings
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioMeetings"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEvent"/> <rdfs:comment>Common event to discuss a situation</rdfs:comment> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNATO
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNATO"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Onto ScenarioAgent"/> <rdfs:comment>NATO is an agent used in many scenarios as an agent or a strategic domain area.</rdfs:comment> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNCR
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNCR"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontol ScenarioSource"/> <rdfs:comment>Norwegian Cyber Range</rdfs:comment>
</owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNato$_secret$– – >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNato$_secret$"/ >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNetwork$_defence$– – >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNetwork$_defence$" >< $rdf:typerdf:resource = "http://www.semanticweb.org/john–/ontologies$/2020/10/$Ontology–ScenarioType$"/ >< /owl:NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNon$_technical_systems_in$ – – >

<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioNon$_t echnical_s ystems_i nf ected$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john−/ontologies$/2020/10/$Ontology−ScenarioConsequence$"/ >< $rdfs : comment > Infectionsofsystemandstructurenotinherentlyontechnicallayer, butisaffected /rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOld$_s ystems−$ –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOld$_s ystems$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john− /ontologies$/2020/10/$Ontology−ScenarioVulnerability$"/ >< $layer > Technical < /layer >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOrganizational$_s tructur$ –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioOrganizational$_s tructure$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john−/ontologies$/2020/10/$Ontology−ScenarioInfrastructure$"/ >< $rdfs : comment > Structureofaorganizationisansocietalinfrastructure < /rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPC –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPC"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontolog ScenarioAsset"/> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Onto ScenarioNode"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPhising –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPhising"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioMalware"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPhone –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPhone"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Onto ScenarioNode"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPoliciy$_B rief−$ –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPoliciy$_B rief$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john− /ontologies$/2020/10/$Ontology−ScenarioArtifact$"/ >< $/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPower$_d istribution_s yste −$ –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPower$_d istribution_s ystem$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john−/ontologies$/2020/10/$Ontology−ScenarioInfected_S ystems$"/ ><

$rdf:typerdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTechnical_domain"/><rdfs:comment>Adomaincenterfordistributingpowerlikeelectri/rdfs:comment></owl:NamedIndividual>$

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPowerregion –>

<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPowerregion"> <rdfs:comment>EU</rdfs:comment> </owl:NamedIndividual>

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPrinter1 –>

<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPrinter1"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAsset"/> </owl:NamedIndividual>

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPrivilegedAccessApprova –>

<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPrivilegedAccessApprovalAndWorkflows"> <rdf:type rdf:resource="http://www.semanticweb.org/ontologies/2020/10/Ontology-ScenarioControl"/> <rdfs:label>Privileged access approval and workflows</rdfs:label> </owl:NamedIndividual>

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPrivilegedAccessManage –>

<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioPrivilegedAccessManagement"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecuritySegment"/> <includesStrategy rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAccountGovernance"/> <includesStrategy rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioCredentialManagement"/> <includesStrategy rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioLeastPrivilegeEnforcement"/> <rdfs:label>Privileged Access Management</rdfs:label> </owl:NamedIndividual>

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRealistic –>

<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRealistic"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioAssumption"/> </owl:NamedIndividual>

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRestore$_functions$– –>

$<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRestore_functions"><rdf:typerdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioGoal"/><LongDescription>ThisisthelongDescription</LongDescription><ShortDescription>Onewouldwanttorestorefu/ShortDescription></owl:NamedIndividual>$

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioRestricted –>

<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-

ScenarioRestricted"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSCADA
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSCADA"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity$_{T}ool$"/ >< $rdfs : comment >$
$WhenusedrightSCADAisasecuritytool, butoutdatedonecanbeexploitedandisarisk <$
$/rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_1$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_1$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–ScenarioScenario"/ >< aChallengeIsrdf :$
$resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–$
$ScenarioUnreponsive_systems"/ >< attackerAttacksrdf : resource = "http :$
$//www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioControl_center"/ ><$
$belongsToArenardf : resource = "http : //www.semanticweb.org/john –$
$/ontologies/2020/10/Ontology–ScenarioCyber9_12"/ >< expertTeamInvestigaterdf :$
$resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–$
$ScenarioCyber_attack"/ >< hasEventrdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–Scenariocomitee_hearings"/ >< hasGoalrdf :$
$resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–$
$ScenarioRestore_functions"/ >< hasMalwarerdf : resource = "http : //www.semanticweb.org/john$
$/ontologies/2020/10/Ontology–ScenarioFriendliePixie"/ >< has_Objectiverdf :$
$resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–$
$ScenarioInformation_gathering"/ >< infrastructureAffectedIsrdf : resource =$
$"http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioPhone"/ ><$
$infrastructureAffectedIsrdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–ScenarioPower_distribution_system"/ >< infrastructure_Attacked_b$
$resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–$
$ScenarioSuspected_agent"/ >< EventLikelihood > NisPowerhasbeeninhighthreatofanattackforalo$
$/EventLikelihood >< OperationObjective > Collecttoknowledgetoasseswhatisgoingon.Usethattoo$
$/OperationObjective >< ScenarioArtifact > Policybrief, < /ScenarioArtifact ><$
$ScenarioAssumption > Someinformationcanbetrustedmorethanother.wontgetafullpicture.Needar$
$/ScenarioAssumption >< ScenarioChallenge > Notallinformationisknown.Notallinformationgiv$
$/ScenarioChallenge >< ScenarioGoal > Solvetheenergysituationin EU.solvethesecurityproblemsi$
$/ScenarioGoal >< ScenarioRules > Realistic.Don't fightthescenario.Thinkmulti–$
$dimensionally.Becreative.Analysetheissues. < /ScenarioRules >< ScenarioStoryLine >$
$NisPowerexecutedaplannedupgradeofitsSCADAandcomputernetworksystems.Theupgradefailedw$
$/ScenarioStoryLine >< StakeholderOrganization > NisPoweristargetedbyacyberattack. <$
$/StakeholderOrganization >< StakeholderSuspectedAgent > Mustelus, individualfromMustelusg$
$/StakeholderSuspectedAgent >< StakeholderTeam > Cybersecurityexpertteamundermandatefro$
$/StakeholderTeam >< layer > Strategical < /layer >< rdfs : comment >$
$Cyber9/122020 < /rdfs : comment >< /owl : NamedIndividual >$

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_2$– –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_2$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioScenario"/ >< AssetProtectedByrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioKarl"/ >< aTemdontwanttordf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioLoose_scenario"/ >< assetProtectedIsrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioPC"/ >< belongsToArenardf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioNCR"/ >< blueTeamsProtectsFromrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioDOS"/ >< hasGoalrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology − Scenariored_team"/ >< hasMalwarerdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioWorm"/ >< teamProtectsrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioDNS"/ >< typeofScenarioIsrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioNetwork_defence"/ >< layer > Technical < /layer >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_3$– –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_3$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioScenario"/ >< infrastructureAffectedIsrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioData_central"/ >< isSecretLevelrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioSecret"/ >< typeofScenarioIsrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioCTF"/ >< layer > Technical < /layer >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_4$– –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_4$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioScenario"/ >< belongsToArenardf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioNCR"/ >< typeofScenarioIsrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology − ScenarioNetwork_defence"/ >< layer > Tactical < /layer >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_5$– –>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_5$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioScenario"/ >< hasEnvironmentalComponentrdf : resource = "http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–$

$ScenarioServer1$"/ >< $relatesToVulnerabilityrdf : resource = "http : //www.semanticweb.org/jo$
$/ontologies/2020/10/Ontology-ScenarioImproperConfigurationForDefaultAccount$"/ ><
$/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioScenario$_example$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioScenario$_example$"/ >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecret
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioSecret"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSecurity$_routines$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioSecurity$_routines$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$
$/ontologies/2020/10/Ontology-ScenarioControl$"/ >< $/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioServer1
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioServer1"> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioServer"/> <hasVulnerability rdf:resource="http://www.semanti
/ontologies/2020/10/Ontology-ScenarioImproperConfigurationForDefaultAccount"/>
<isTypeOf rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioApacheWebServer"/> <usesOperatingSystem rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioUbutuLinux20.10"/> <Version>2.2.46</Version>
</owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioShellshock
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioShellshock"> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioVulnerability"/> <layer>Technical</layer>
</owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioState$_structure$–
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioState$_structure$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$
$/ontologies/2020/10/Ontology-ScenarioInfrastructure$"/ >< $layer > Strategical <$
$/layer >< rdfs : comment > Structureofastateisansocietalinfrastructure <$
$/rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSteven
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioSteven"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ont
ScenarioBlue$_Team$"/ >< $/owl : NamedIndividual >$

<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategical$_agent$–
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategical$_agent$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–ScenarioAgent"/ >< rdf : typerdf : resource =$
$"http : //www.semanticweb.org/john–/ontologies/2020/10/Ontology–ScenarioStrategical_domai$
$rdfs : comment > Grouporstatesdistributingpowerinascenario. < /rdfs :$
$comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategical$_security$–
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioStrategical$_security$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–ScenarioControl"/ >< layer > Strategcial <$
$/layer >< rdfs : comment > Strategicalconcerncsforincreasingofsecurity <$
$/rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSuspected$_agent$–
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSuspected$_agent$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology – ScenarioAgent"/ >< ShortDescription >$
$Anyscenariohasagentsthatarereponsiblefortheattackandsomeofthemarejustsuspected. <$
$/ShortDescription >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSystems
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSystems"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioInfrastructure"/> <layer>Tactical</layer>
<layer>Technical</layer> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSystems$_down$–
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioSystems$_down$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–ScenarioImpact"/ >< LongDescription ><$
$/LongDescription >< ShortDescription >< /ShortDescription >< rdfs :$
$comment > Multiplenudclearreactorsareshutdown.lossofgastransportationcapability.Conneecti$
$/rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTechnical$_agent$–
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTechnical$_agent$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john–$
$/ontologies/2020/10/Ontology–ScenarioAgent"/ >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTrojan
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-

ScenarioTrojan"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Onto
ScenarioMalware"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioTwo$_f actor_l ogin_r equire$
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioTwo$_f actor_l ogin_r equirements$" >< $rdf : typerdf : resource = "http :$
$//www.semanticweb.org/john-/ontologies$/2020/10/$Ontology-ScenarioControl$"/ ><
$/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUbutuLinux20.10
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioUbutuLinux20.10"> <rdf:type rdf:resource="http://www.semanticweb.org/john-
/ontologies/2020/10/Ontology-ScenarioOperatingSytem"/> <Version rdf:datatype="http://www.w3.org
<rdfs:label>Ubutu Linux 20.10</rdfs:label> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUnable$_t o_u se_d ata-$
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioUnable$_t o_u se_d ata$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$
$/ontologies$/2020/10/$Ontology-ScenarioConsequence$"/ >< $/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUnpatached$_s ystems-$
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioUnpatached$_s ystems$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$
$/ontologies$/2020/10/$Ontology-ScenarioVulnerability$"/ >< $/owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUnreponsive$_s ystems-$
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioUnreponsive$_s ystems$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$
$/ontologies$/2020/10/$Ontology-ScenarioRisk$"/ >< $rdfs : comment > Systemsthatcantbeaccesed.$
$/rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUnrestricted
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioUnrestricted"/>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUnusable$_s ystems-$
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioUnusable$_s ystems$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$
$/ontologies$/2020/10/$Ontology-ScenarioRisk$"/ >< $rdfs : comment > Systemsthatcantbeusedatal$
$/rdfs : comment >< /owl : NamedIndividual >$
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUpdate$_o n_s ituation-$
– >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
ScenarioUpdate$_o n_s ituation$" >< $rdf : typerdf : resource = "http : //www.semanticweb.org/john-$

/ontologies/2020/10/*Ontology−ScenarioObjective*”/ >< */owl* : *NamedIndividual* >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUpgrade
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUpgrade"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioEvent"/> <rdfs:comment>NIsPower upgrading their systems led to this malware springing out to life.</rdfs:comment>
</owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUse$_o f_s tate_o f_t he_a rt_p rod$
− >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioUse$_o f_s tate_o f_t he_a rt_p roducts$” >< rdf : $typerdf$: $resource$ = ”$http$: *//www.semanticweb.org/john−/ontologies*/2020/10/*Ontology−ScenarioControl*”/ >< */owl* : *NamedIndividual* >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioVirtual$_m achines$−
− >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioVirtual$_m achines$” >< rdf : $typerdf$: $resource$ = ”$http$: *//www.semanticweb.org/john−/ontologies*/2020/10/*Ontology−ScenarioConfiguration*”/ >< */owl* : *NamedIndividual* >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWin$_s cenario$−
− >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWin$_s cenario$” >< rdf : $typerdf$: $resource$ = ”$http$: *//www.semanticweb.org/john−/ontologies*/2020/10/*Ontology−ScenarioGoal*”/ >< */owl* : *NamedIndividual* >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWindows
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWindows"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioServer"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWorm
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioWorm"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Onto ScenarioMalware"/> <hasSeverity rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-ScenarioHigh"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioalarm
–>
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenarioalarm"> <rdf:type rdf:resource="http://www.semanticweb.org/john-/ontologies/2020/10/Onto ScenarioInjection"/> </owl:NamedIndividual>
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariocomitee$_h earings$−
− >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariocomitee$_h earings$” >< rdf : $typerdf$: $resource$ = ”$http$: *//www.semanticweb.org/john−*

/ontologies/2020/10/Ontology − ScenarioEvent”/ >< rdfs : comment >
Multipleorgansorcomiteeusualyhashearingsormeetingaseventstogetanunderstandingofasituatio
/rdfs : comment >< /owl : NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariored$_t$eam—
— >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
Scenariored$_t$eam” >< protectsAssetrdf : resource = ”http : //www.semanticweb.org/john—
/ontologies/2020/10/Ontology—ScenarioPrinter1”/ >< /owl : NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariosolve$_t$he$_c$ode—
— >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
Scenariosolve$_t$he$_c$ode” >< rdf : typerdf : resource = ”http : //www.semanticweb.org/john—
/ontologies/2020/10/Ontology—ScenarioObjective”/ >< /owl : NamedIndividual >
<!– http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-Scenariostatus$_u$pdate$_m$eeting—
— >
<owl:NamedIndividual rdf:about="http://www.semanticweb.org/john-/ontologies/2020/10/Ontology-
Scenariostatus$_u$pdate$_m$eeting” >< rdf : typerdf : resource = ”http : //www.semanticweb.org/john—
/ontologies/2020/10/Ontology − ScenarioActivity”/ >< rdfs : comment >
NisPowerhiredaconsultantteamtodoaforensicanalysisforthem < /rdfs : comment >< /owl : NamedIndividual >< /rdf : RDF >
<!– Generated by the OWL API (version 4.5.9.2019-02-01T07:24:44Z) https://github.com/owlcs/owlapi
–>

Bibliography

Bibliography

[1] G. C. Enrico Russo and A. Armando, 'Building next generation cyber ranges with crack,' 2020.

[2] A. A. Enrico Russo Gabriele Costa, 'Scenario design and validation for next generation cyber ranges,' 2018.

[3] C. F. Mazaher Kianpour Stewart James Kowalski Erjon Zoto and H. Øverby, 'Designing serious games for cyber ranges: A socio-technical approach,' 2019.

[4] M. N. Muhammad Mudassar Yamin Basel Katt, 'Serious games as a tool to model attack and defense scenarios for cyber-security exercises,' 2020.

[5] P. G. C. Hossein Ghodrati, 'A framework for designing attack strategies in cyber range scenarios,' p. 57, 2017.

[6] N.-a. cyber defence hub, 'Lockedshields13$_a ar$,' 2013.

[7] R. H. Wagner, 'Designing a network defense scenario using the open cyber challenge,' 2013.

[8] Y. T. Razvan Beuran Takuya Inoue and Y. Shinoda, 'Realistic cybersecurity training via scenario progression management,' 2019.

[9] J. A. Peter Øhrstrøm and H. Scharfe, 'What has happened to ontology,' 2005.

[10] D. Man, 'Ontologies in computer science,' 2013.

[11] S. T. Curtis L. Maines David Llewellyn-Jones and B. Zhou, 'A cyber security ontology for bpmn-security extensions,' 2015.

[12] N. F. Noy and D. L. McGuinness, 'Ontology development 101: A guide to creating your first ontology,' 2001.

[13] V. G. Muhammad Mudassar Yamin Basel Katt, 'Cyber ranges and security testbeds- scenarios, functions, tools and architecture,' 2019.

[14] K. F. Iasonas Somarakis Michail Smyrlis and G. Spanoudakis, 'Model-driven cyber range training: A cyber security assurance perspective,' 2020.

[15] G. D. T. F. M. L. A. S. Dashevskyi and J. Mirkovic, 'An experimental approach for estimating cyber risk: A proposal building upon cyber ranges and capture the flags,' 2020.

[16] E. Seker, 'The concept of cyber defence exercises (cdx): Planning, execution, evaluation,' 2018.

[17] J. M. Fabio Massacci and N. Zannone, 'An ontology for secure socio-technical systems,' 2019.

[18] A. D. M. E. B. C. G. S. G. Y. A. Z. L. Cavedon and G. Vigna, 'Hit 'em where it hurts: A live security exercise on cyber situational awareness,' 2011.

[19] V. Agrawal, 'Towards the ontology of iso/iec 27005:2011 risk management standard,' 2016.

[20] A. Council, 'Geneva cyber 9 12 2020 intelligence brief i,' 2020.