Uma Ontologia de Apoio a Defesa Cibernética

Sylvio Andre Diogo Silva – Instituto Tecnológico de Aeronáutica, José M Parente de Oliveira - Instituto Tecnológico de Aeronáutica e Edgar Toshiro Yano - Instituto Tecnológico de Aeronáutica

***Resumo* — O artigo se propõe a apresentar um estudo analítico sobre uma proposta de construção de uma ontologia para uso no desenvolvimento de um sistema de defesa cibernética. Através de pesquisa teórica foi possível construir uma ontologia que vislumbra o conhecimento e os conceitos envolvidos na Defesa Cibernética para servir de apoio na definição de requisitos e padrões metodológicos. A construção da ontologia para defesa cibernética foi realizada com o uso de métodos conhecidos para construção de ontologias e com a utilização de ferramentas de uso livre.**

***Palavras-Chave* — ontologia, defesa cibernética.**

I. INTRODUÇÃO

Vivemos uma época de intenso desenvolvimento de diversos setores que contribuem para o bem-estar da humanidade. Dentre eles podemos destacar o tecnológico que tem proporcionado grandes facilidades a humanidade, em particular no início do século XXI, como os aparelhos de comunicação, computadores, televisores, dentre outros.

O advento dos equipamentos para comunicação criou um ambiente de comunicação e de conflitos, diferente dos tradicionais, conhecido como ciberespaço[1] e refere-se a um espaço de comunicação que descarta a necessidade da presença física do homem como fonte de relacionamento como os que ocorrem por intermédio de celulares, pagers, comunicação entre rádio-amadores e por serviços do tipo "tele-amigos". O principal ambiente virtual ou ciberespaço que se conhece hoje é a internet devido a sua popularização e sua natureza de hipertexto.

Por outro lado, o ciberespaço possibilitou também a existência de um novo tipo de conflito diferentes dos tradicionais conhecido como Guerra Cibernética, onde o principal ambiente de combate na atualidade é a internet. Neste ambiente um ataque bem sucedido pode causar o bloqueio de serviços bancários, interferir na bolsa de valores ou mesmo causar um colapso nos sistemas de transporte e de saúde. Um dos ataques cibernéticos mais devastadores, que se tem notícia contra um país, ocorreu em 2007 e atingiu a Estônia. Bancos, agências governamentais e até o site do governo ficaram desconectados por vários dias.

Em virtude de tal magnitude dos ataques grandes potências mundiais, como a China e Estados Unidos estão investindo em Defesa Cibernética para mitigar ou neutralizar os efeitos de um ataque realizado aos ativos de instituições governamentais ou privadas.

Para que seja possível realizar uma defesa eficiente e eficaz é necessário um profundo conhecimento sobre o assunto por intermédio da definição de conceitos, propriedades, relações e conhecimentos envolvidos na Defesa Cibernética. Tal conhecimento pode ser representado por intermédio da construção de uma ontologia para servir de apoio a gestão de um sistema de defesa. Uma ontologia faz uma especificação formal de uma área de conhecimento e se compõe de cinco componentes para formalização dos termos: conceitos, relações, funções, axiomas e instâncias [2].

Este artigo apresenta uma proposta de construção de uma ontologia envolvendo os conceitos de Defesa Cibernética, em alto nível, com a finalidade de apoiar um processo de implantação e gerenciamento de um sistema de defesa em uma organização. A ontologia aborda os conceitos fundamentais de Defesa Cibernética não envolvendo processos utilizados na atualidade. O artigo está organizado da seguinte forma: na seção 2 é exposto as bases teóricas do uso de ontologias para construção de conhecimento, na seção 3 apresenta-se a descrição do processo de construção de ontologia utilizado, na seção 4 é realizado a construção da uma ontologia de apoio a defesa cibernética e na seção 5 são apresentadas as considerações finais.

II. ONTOLOGIAS

O vocábulo ontologia foi introduzido no estudo da filosofia de modo a fazer uma distinção entre o estudo do ser e o estudo dos vários tipos de seres vivos existentes no mundo natural. O objetivo da ontologia é o fornecimento de sistemas de categorização para organizar a realidade.

Uma ontologia é uma especificação explícita dos objetos, conceitos e outras entidades que se assume existirem em uma área de interesse, além das relações entre estes conceitos e restrições expressados através de axiomas[3].

Em ciências da computação, o termo ontologia refere-se a um artefato de engenharia, constituído por um vocabulário específico que descreve um modelo particular do mundo, adicionando um conjunto explícito de suposições relacionando os significados das palavras no vocabulário [3]. Os vocabulários são usualmente organizados em taxonomias.

Existem diversas propostas de metodologias para apoiar o processo de construção de ontologias, entretanto, nenhuma delas é a mais adequada em virtude da particularidade de cada aplicação, ou seja, uma combinação de metodologias se torna pertinente no processo de desenvolvimento de ontologias[3].

O trabalho se propõe a desenvolver uma ontologia, que envolve os conceitos de Defesa Cibernética, utilizando como base o processo proposto por Sandro Rautenberg, da Universidade do Centro Oeste, José L. Todesco e Fernando A. O. Gauthier, estes últimos da Universidade Federal de Santa Catarina. O processo proposto toma como base as seguintes metodologias para construção de ontologias com suas respectivas contribuições [4]:

• Ontology Development 101: contribui com uma visão clara de como se dá um processo iterativo para o desenvolvimento de ontologias.

• On-to-Knowledge: contribui na especificação dos requisitos da ontologia, por meio do emprego de questões de competência como modo simples e direto para confirmar o propósito e o escopo de uma ontologia. Tal contribuição permite identificar antecipadamente, conceitos, propriedades, relações e instâncias.

• METHONTOLOGY: contribui com alguns artefatos de documentação e na atividade de avaliação de ontologias.

III. O PROCESSO DE CONSTRUÇÃO DE ONTOLOGIA PROPRIAMENTE DITO

No processo de desenvolvimento de ontologias de utilizado como base, os autores partiram de duas premissas: a não existência um modo correto ou metodologia de desenvolvimento de ontologias; e a utilização da combinação das melhores práticas metodológicas dos processos como algo pertinente em um processo de desenvolvimento de ontologias.

Considerando as premissas, o processo proposto combina as melhores práticas das metodologias On-to-Knowledge, METHONTOLOGY e da Ontology Development 101. O processo proposto baseou-se em cinco grandes atividades com suas respectivas tarefas, como se segue [4]:

1. Especificação

Nesta atividade tende-se a discernir a respeito dos custos do desenvolvimento da ontologia, onde pretende-se:

a. **identificar o escopo da ontologia**: responder "quem são os usuários", "quais são as intenções de uso", entre outras.

b. **identificar o propósito da ontologia**: identificar por que a ontologia deve ser construída, entre outros.

c. **identificar as fontes de conhecimento**: procurar por livros, artigos, entre outras fontes, das quais pode-se abstrair o entendimento dos conceitos presentes na ontologia.

d. **considerar o reuso de ontologias**: verificar a existência de ontologias correlacionadas, das quais pode-se aproveitar conceitos já estabelecidos.

e. **gerar as questões de competência**: entrevistar especialistas de domínio na perspectiva que estes elaborem questões que a ontologia deva responder e que relacionem os termos, jargões e relacionamentos presentes no domínio.

2. Conceitualização

Atividade que visa descrever um modelo conceitual da ontologia a ser construída, de acordo com as especificações encontradas no estágio anterior. Tem como tarefas:

a. **listar os termos da ontologia**: a partir das fontes de conhecimento e das questões de competência, pode-se enumerar os termos comumente utilizados pelos especialistas de domínio.

b. **agregar os elementos reutilizáveis**: das ontologias que tem aderência à ontologia em desenvolvimento, pode-se capturar novos elementos ou a definição de elementos já estabelecidos.

c. **classificar os termos**: com a lista de termos disponível, é possível classificar os elementos de acordo com a compreensão que se tem do domínio.

d. **definir os termos**: para cada termo presente na ontologia é necessário explicitar o seu significado para com o domínio em questão.

3. Formalização

Atividade que visa transformar o modelo conceitual em um modelo formal, passível de ser implementado computacionalmente. As tarefas desta atividade são:

a. **definir a hierarquia de classes**: uma vez a lista de termos classificada, atém-se somente às classes.

b. **mapear as relações às classes**: para cada classe agregam-se os termos tidos como "relação" e que associam explicitamente o relacionamento da classe em questão para com as demais classes do domínio.

c. **mapear as propriedades de dados às classes**: para cada classe agregam-se os termos tidos como "propriedade de dados" e que pertencem explicitamente como dimensão da classe em questão.

d. **mapear as restrições às classes**: para cada classe verificar a existência de regras que possam restringir o conteúdo de suas propriedades de dados ou relações.

e. **mapear as instâncias às classes**: para cada classe associar os termos tidos como "instâncias", que caracterizam-se como exemplos concretos da classe em questão.

f. **refinar as relações das classe**: para cada relação, definir as classes a serem apontadas pela relação em questão.

g. **refinar as propriedades de dados das classes**: para cada propriedade de dados, definir qual o tipo de dados a ser armazenado (string, número ou booleano) e definir se esta é funcional.

4. Implementação

É uma atividade de menor interação com especialistas de domínio, sendo reservada às tarefas de:

a. **valorar as propriedades de dados**: para cada instância da ontologia é preciso atribuir o valor de suas propriedades internas.

b. **valorar as relações**: para cada instância da ontologia deve-se valorar as relações das instâncias para com outras instâncias da ontologia; e

c. **valorar as restrições das classes:** para cada classe deve-se valorar as restrições presentes no domínio quanto aos valores possíveis para as suas propriedades de dados e para as suas relações admitidas com as classes da ontologia.

5. Avaliação

Trata-se de uma atividade onde se retoma maior interação com especialistas de domínio e também com os usuários da ontologia, com a finalidade de avaliar a ontologia. Realizam-se as tarefas:

a. **avaliar a ontologia perante as fontes de conhecimento**: é a avaliação técnica da ontologia de acordo com o entendimento aceito sobre o domínio em fontes de conhecimento especializadas, verificando a coerência do conhecimento representado na ontologia;

b. **avaliar a ontologia perante um frame de referência**: é a avaliação técnica da ontologia ao confrontá-la com um

frame de referência gerado a partir do propósito, do escopo e das questões de competência da ontologia, verificando a precisão e a completude da ontologia; e

c. **avaliar perante a visão do usuário**: a avaliação da ontologia juntamente com os especialistas de domínio e usuários envolvidos para certificar a usabilidade e utilidade da ontologia.

A equipe que realizou a proposta do processo de construção de ontologias, também, realizou a implementação da ferramenta ontoKEM. A plataforma é uma ferramenta para especificação, conceitualização, formalização e documentação de ontologias. A principal vantagem e justificativa da utilização desta ferramenta é a geração automática de artefatos customizados para documentar projetos de ontologias. Ademais, cabe ressaltar que os documentos gerados pela ontoKEM são subsídios pertinentes para a atividade de avaliação de ontologias [4].

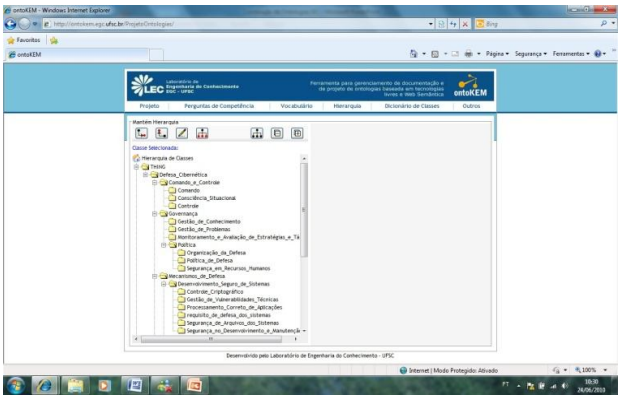

Fig. 1 – Ferramenta ontoKEM

A outra ferramenta que pode ser utilizada é o Protégé. É uma plataforma livre de código-aberto que provê um conjunto de ferramentas para construir modelos de domínio e aplicações baseadas em conhecimento com ontologias [5].

IV. CONSTRUÇÃO DE UMA ONTOLOGIA PARA UM SISTEMA DE DEFESA CIBERNÉTICA

Conforme proposto no artigo base[4] foi realizada a construção de uma ontologia para um sistema de Defesa Cibernética realizando-se os passos especificados no modelo sendo os seguintes: especificação, conceitualização, formalização, implementação e avaliação. As etapas foram realizadas seguindo os passos abaixo discriminados:

1. Especificação

a. **escopo da ontologia**: a ontologia auxiliará as atividades de gerenciamento e gestão de Defesa Cibernética em organizações ou instituições que possuem ativos[1] passíveis de sofrerem ataques oriundos do espaço cibernético.

A informação e os sistemas de informação são ativos que, como qualquer outro ativo importante, são essenciais para os negócios de uma organização e, portanto, necessitam de serem protegidos adequadamente. Assim a Defesa Cibernética, que é um ramo da Guerra Cibernética, trata do emprego defensivo de metodologias, processos, equipamentos e estratégia para defesa e proteção de informações, sistemas de informações e redes de computadores.

b. **identificação do propósito da ontologia**: a ontologia será de grande valia na especificação, representação, formalização e compartilhamento de conhecimento a despeito da defesa cibernética. A ontologia pode ser considerada como um ponto de partida para facilitar o desenvolvimento de diretrizes específicas de Defesa Cibernética e Segurança da Informação em uma organização. Os termos relacionados na ontologia estão contidos em normas, processos de qualidade e bibliografias sobre gerenciamento e gestão da segurança da informação e defesa cibernética.

c. **identificação das fontes de conhecimento**: as fontes de conhecimento para construção da ontologia foram:

- o artigo "Cyber War: Arto to Science", de Saydjari que especifica os elementos fundamentais em um sistema complexo de Defesa Cibernética [6];
- a Norma Brasileira ABNT NBR ISO/IEC 27001 que trata do código de prática para a gestão da segurança da informação [7]; e
- a Publicação Especial 800-53 do National Institute de Standards and Technology (NIST 800-53) que trata dos controles de segurança recomendados para sistemas de informação [8].

d. **consideração do reuso de ontologias**: por ser tratar de assunto complexo e relativamente recente não foi possível encontrar uma ontologia sobre o assunto em questão para ser reutilizada.

e. **geração das questões de competência**: uma ontologia deve ser capaz de responder as questões de competência do assunto em pauta [4]. Por intermédio da análise das fontes de conhecimento foram eleitas as questões chaves que devem ser respondidas pela ontologia para servir de apoio no gerenciamento de um sistema de defesa, sendo as seguintes[6]:

1. Se a organização estiver sob ataque cibernético como identificar a natureza e origem?
2. Quais as causas do ataque?
3. O que os atacantes podem fazer?
4. Qual o impacto do ataque na missão da organização?
5. O perímetro de Segurança foi ultrapassado?
6. Quais são as opções de defesa?
7. Qual a melhor opção de defesa?
8. Qual a vulnerabilidade explorada pelo atacante?
9. Como impedir tais ataques no futuro?

2. Conceitualização

a. **listar os termos da ontologia**: Conforme análise das fontes de conhecimento verificou-se que os termos que se relacionam com a Defesa Cibernética são os seguintes: Política, Estratégia, Táticas, Comando e Controle, Mecanismos de Defesa, Supervisão da Defesa, Política de Defesa, Monitoramento e Avaliação de Estratégias e Táticas, Gestão de Problemas, Gestão de Conhecimento, Consciência Situacional, Serviços de Segurança, Segurança Física e do Ambiente, Segurança Pessoal, Desenvolvimento Seguro, Operação Segura, Manutenção Segura, Monitoramento de Mecanismos de Defesa, Política de Defesa, Organização de Defesa, Segurança em Recursos Humanos, Comando,

Controle, Controle de Acesso, Identificação e autorização, Confidencialidade, Disponibilidade, Integridade, Proteção de Mídia, Áreas Seguras, Segurança de Equipamentos, Proteção dos Sistemas e Comunicações, Pessoal Terceirizado, Requisitos de Defesa dos Sistemas, Processamento Correto de Aplicações, Controles Criptográficos, Segurança dos Arquivos do Sistema, Segurança no Desenvolvimento e Manutenção, Gestão de Vulnerabilidades Técnicas, Gestão de Incidentes, Testes de Invasão e Auditoria, dentre outros.

b. **agregar os elementos reutilizáveis**: não foi encontrado uma ontologia para reutilização de elementos.

c. **classificar os termos**: com a lista de termos disponíveis foi possível classificar os elementos de acordo com a compreensão que se tem do domínio e foi realizada a classificação dos elementos em classes, relações, propriedades de dados, instâncias e restrições a serem visualizadas na ontologia final.

3. Formalização

A atividade foi realizada utilizando a ferramenta Protégé (Fig. 2) sendo realizadas as seguintes atividades:

- definição da hierarquia de classes entre os conceitos envolvidos;
- mapeamento das relações entre as classes por intermédio da definição e a correlação entre os conceitos;
- propriedade de dados às classes visando a particularidade de cada elemento se for o caso;
- restrição das classes se for o caso;
- instâncias das classes que são os processos usados na atualidade ou especificamente a atividade de defesa específica;
- refinamento das relações das classes; e
- refinamento das propriedades de dados das classes.

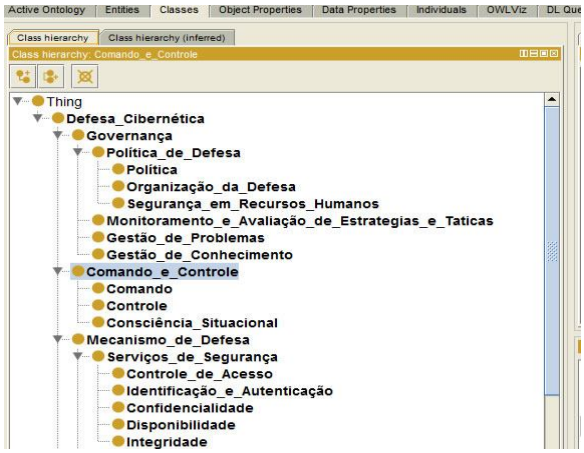

Fig 2. Atividade de Formalização e Implementação na Ferramenta Protégé

4. Implementação

A implementação foi realizada utilizando como base a ferramenta Protégé (Fig. 2) para geração da documentação da ontologia, como as definições dos termos, as relações de classes e também foi utilizada a ferramenta CMAP para a construção do Mapa Conceitual e da Ontologia Final, que pode ser visualizada na Fig. 3. O mapa conceitual constitui-se de todos os conceitos, relações, funções, axiomas e instâncias que envolvem o assunto em tela de um modo geral. A ontologia é um refinamento do mapa conceitual com os elementos suficientes para responderem as questões de competência.

As atividades desenvolvidas nesta etapa foram: atribuição de valor as propriedades de dados, a atribuição de valor as relações e a atribuição de valor as restrições das classes.

5. Avaliação

A avaliação da ontologia perante as fontes de conhecimento mostrou contribuir de forma significativa para a compreensão do assunto uma vez que engloba os conceitos de defesa cibernética em alto nível.

Utilizando os itens previstos na especificação pode-se avaliar a ontologia confrontando com as informações geradas a partir do propósito, do escopo e das questões de competência da ontologia. Assim, verificou-se a precisão e a completude da ontologia (Fig. 3) uma vez que respondeu as questões de competência tomando como base os conceitos relacionados na base de conhecimento e na ontologia. As respostas as questões de competência podem ser atendidas da seguinte forma:

- Se a organização estiver sob ataque cibernético como identificar a natureza e origem? A resposta para o questionamento pode ser verificada por intermédio da supervisão da defesa que realiza o monitoramento dos mecanismos de defesa.
- Quais as causas do ataque? As causas dos ataques podem ser identificadas por intermédio da consciência situacional que dentre outras coisas identificam o histórico dos ataques e as finalidades específicas.
- O que os atacantes podem fazer? Os atacantes podem destruir, sabotar, espionar ou negar os serviços disponibilizados e podem ser verificados por intermédio dos mecanismos de defesa.
- Qual o impacto do ataque na missão da organização? O impacto poderá ser verificado com precisão por intermédio da Governança no que diz respeito a estratégia da organização, e ainda, com a análise dos ativos envolvidos.
- O perímetro de Segurança foi ultrapassado? A Supervisão da Defesa pode informar se o perímetro físico da rede de computadores da organização foi invadido pelo atacante.
- Quais são as opções de defesa? A consciência situacional possui condições de informar quais as melhores opções de defesa para fazer frente ao ataque realizado.
- Qual a melhor opção de defesa? A melhor opção de defesa será verificada pelo melhor comando por intermédio das informações disponibilizadas pela consciência situacional e pela supervisão da defesa.
- Qual a vulnerabilidade explorada pelo atacante? Por intermédio da auditoria da supervisão da defesa é possível verificar a vulnerabilidade explorada pelo atacante especificando as características técnicas debilitadas.
- Como impedir tais ataques no futuro? Por intermédio do suporte e manutenção oriunda do desenvolvimento seguro de sistemas é possível verificar quais as medidas necessárias para corrigir a vulnerabilidade explorada pelo atacante.

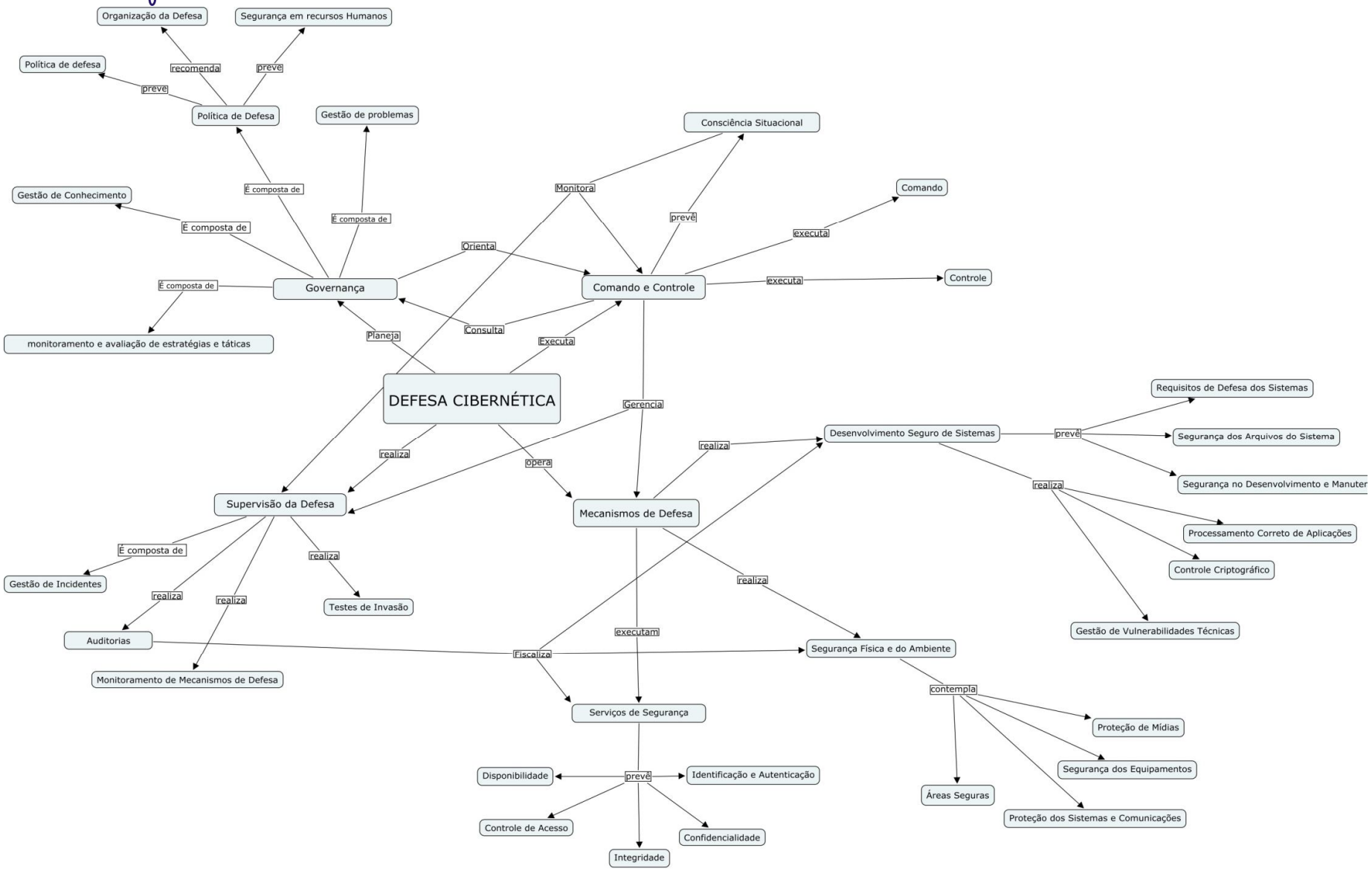

Fig. 3 – Uma Ontologia de apoio a Defesa Cibernética

V. CONSIDERAÇÕES FINAIS

A proposta da ontologia construída com base nos conceitos e cenários para defesa cibernética é um importante meio de representar, formalizar e compartilhar conhecimento a despeito desta nova área de pesquisa.

O método proposto para construção de ontologias que é baseado na combinação de metodologias estabelecidas facilitou sobremaneira o trabalho realizado sendo um excelente guia de desenvolvimento. A proposta das grandes atividades e tarefas associadas permite que os trabalhos de desenvolvimento sejam realizados de modo ordenado e organizado.

Certamente, a defesa cibernética requer o fortalecimento em nível nacional e internacional, da cooperação técnica e da busca do conhecimento. A proposta de construção da ontologia serve de subsídio para constante avaliação na busca da melhoria contínua e, portanto, está longe de esgotar o assunto.

REFERÊNCIAS

[1]- William Gibson . Neuromancer. 1984. 20th Anniversary Edition. New York: Ace Books, 2004

[2]- Gruber, T. Ontolingua: a mechanism to support portable ontologies. 1992. Toward Principles for the Design of Ontologies Used for Knowledge Sharing. In . 1993.

[3] - Gruber, T. R. (1995) “Toward principles for the design of ontologies used for knowledge sharing”. International Journal of Human-Computer Studies, v. 43, p. 907-928.

[4] – Rautenberg, Sandro. ontoKEM: uma ferramenta para construção e documentação de Ontologias. Disponível em http://www.uff.br/ontologia/artigos/27.pdf. Acesso em maio de 2010.

[5] – Protégé. Platform supports two main ways of modeling ontologies via the Protégé-Frames and Protégé-OWL editors. Disponível em http://protege.stanford.edu/. Acesso em Julho de 2010.

[6] – SAYDJARI, O. Sami. Cyber Defense: Art to Science, Communications of the ACM, v.47, n.3, pp52-57. 2004

[7] - ABNT NBR ISO/IEC 27002:2006. Técnicas de Segurança – Código de Prática para a Gestão de Segurança da Informação.

[8] - NIST (2010). Guide for assessing the security controls in federal information systems and organizations. Special Publication 800-53A Revision 1, Consistent with NIST SP 800-53, Revision 3, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930.