Modelo Hierárquico de um Simulador Cibernético

Edgar Toshiro Yano e André Ferreira Alves Machado
Instituto Tecnológico de Aeronáutica (ITA), Praça Marechal Eduardo Gomes, 50 – Vila das Acácias – São José dos Campos - SP

***Resumo* — A Cibernética está cada vez mais presente em nossos dias e, por este motivo, vem sendo alvo de estudos constantes. Uma forma de viabilizar o seu entendimento e capacitar recursos humanos aptos a trabalharem nesta nova área, pode ser obtida por meio de simuladores. Para isso, ferramentas que virtualizam um ambiente propício ao aprendizado cibernético é o foco do presente artigo. Neste trabalho apresento uma contextualização e motivação do estudo realizado, características principais dos simuladores, alguns softwares existentes, uma taxonomia e, por último, proponho um modelo hierárquico genérico para um simulador cibernético.**

***Palavras-Chave* — Cibernética, Simulador, Modelo Hierárquico.**

I. INTRODUÇÃO

No mundo atual, a tendência é estar conectado à nuvem. Todos os recursos eletrônicos devem possuir acesso a Internet, conter entrada USB, ser acessível via bluetooth, ter uma tela touchscreen, disponibilizar recursos multimídia, reconhecer sinal GPS. Assim, necessitamos de tecnologia para viver, crescer, estudar, aprender, trabalhar, comprar, desenvolver.

Com isso, especialistas [1] [2] [3] acreditam que, em um futuro próximo, tudo estará conectado e quem tiver controle digital, dominará a informação, a opinião, a política, a economia. Assim, diversas nações têm direcionado esforços no intuito de dominar o terreno digital. E, para isso, novas ferramentas surgem facilitando nossas vidas e por vezes, infelizmente, dificultando.

Ações criminosas deixaram de ser realizadas nas ruas escuras, de becos inóspitos. Hoje, somos atacados nas nossas próprias casas, no conforto do lar, diante da família e frente a um público global. Cracker, como são conhecidos, rastreiam a rede em busca de informações e utilizam a inteligência artificial, criatividade digital, e a antiga desonestidade, para enganar pessoas (usuários). Os valores subtraídos das contas de bancos, cartões de créditos, crescem vertiginosamente [4], abrindo caminho para novas profissões: os *Phreakers* (peritos em invadir equipamentos eletrônicos, sinais de TV a cabo e burlar sistemas telefônicos), *Carders* (especialistas em roubar senhas), *Black Hat* (hacker que não respeita a ética hacker).

Mas as ações meliantes não se restringem mais em atacar internautas e ultimamente tem despendido atenção para atacar órgãos públicos, entidades federais, usinas nucleares. [5] Enfim, vivemos uma avalanche de vírus, de todos os tipos, que contaminam as redes e provocam desastres sem precedentes.

Assim, o dicionário da nova geração recebe novas palavras: vírus, worm, trojan, sniffer, butnet, spyware, keylogger, backdoor, rootkit, DDoS, *malware*. Atualmente não basta ser roubado, também podemos ser clonados, infectados, deletados e "zumbizados", em uma rede botnet.

II. A TÉCNICA DA SIMULAÇÃO

Para defender a nação e nossos ativos, o governo brasileiro, por intermédio da Estratégia Nacional de Defesa (END), atribuiu ao Exército Brasileiro a missão de: planejar, desenvolver e disseminar ações, procedimentos e tecnologia para assegurar segurança da informação. [6]

Nesta direção, com o intuito de preparar os recursos humanos necessários e aparelhar a instituição, o Exército está desenvolvendo uma série de atividades relacionadas ao preparo e emprego de pessoal, focados na Tecnologia da Informação (TI). Um dos recursos adquiridos para realizar a capacitação de profissionais de TI é o Simulador de Operações de Guerra Cibernética (SIMOC).

Este tipo de iniciativa já foi estudada pela Academia Naval Americana, no sentido de utilizar simuladores nas salas de aula para facilitar o entendimento dos alunos na área de segurança computacional.

> "The U. S. Naval Academy is examining a new tool to teach computer security to determine if the complex concepts relating to computer security can be more effectively taught by including simulations in the classroom". [7]

Nos EUA, militares e civis executam diversas atividades em ambiente de redes distribuídas, contendo inúmeros usuários. Estas redes são dinâmicas e podem aumentar e diminuir, dependendo das tarefas realizadas. Assim, a entrada de novos usuários na rede significa a exposição dos sistemas a novas ameaças. No intuito de controlar estas possíveis ameaças, os profissionais do Departamento de Defesa Americano realizam treinamentos e exercícios operacionais com o apoio de simuladores. [7]

Assim, a utilização de simuladores na área educacional vem, há algum tempo, sendo utilizada pelo governo americano.

> "In recent U.S. history, the Department of War used simulations in preparation for and prosecution of World War II. These simulations, known as "war games" [7]

> "The United States Naval Academy will incorporate simulation into the senior-level Information Assurance course for the Information Technology Majors…" [7]

> "The use of a security laboratory and/or a simulated network scenario is very beneficial as a mechanism for

> supporting active learning strategies such as: learning-by-doing, learningby- example and learning-by-exploring." [8]

De acordo com Robert Schank [9], professor emérito de filosofia, educação e ciência da computação, o melhor modo de ensinar alguém consiste em dar a informação de que ele (instruendo) necessite para fazer algo. E quando utilizado softwares educacionais, a técnica de simulação pode ser utilizada e recomendada em várias áreas de atuação.

> "All learning takes place in the context of failure … The best way to teach someone something is to give them information they need to do something they already want to do…" [9]
> "The best educational software ever written is the flight simulator … A 747 pilot can try different strategies, even crash the plane repeatedly with no consequences." [9]

Deste modo, a simulação tem se tornado fundamental para ciência da computação, principalmente em exercícios de ciberataques. Sendo também utilizada por Indústrias e agências governamentais, envolvendo infraestruturas críticas, como energia e finanças. [10] [8]

Em muitos casos, a realização de testes de segurança em redes de computadores, contendo dispositivos reais, torna-se muito custoso. Assim, a utilização de ferramentas de modelagem e simulação, torna-se interessante. O uso destes instrumentos propicia rapidez de análise, economia de recursos financeiros, análise em alta escala e fidelidade na representação de redes de informação. [11]

Em uma situação real, o número de vulnerabilidades de um sistema cresce na mesma proporção que a sua complexidade, o que motiva a utilização de simulação baseada em amostragem randômica, ao invés de uma análise exaustiva do sistema. [10]

A técnica de simulação pode, ainda, ser combinada com técnicas de virtualização, o que possibilita testes mais realísticos. Assim, com a utilização de Máquinas Virtuais, muitas vantagens são criadas. Por exemplo, dado um hardware moderno (complexo), é possível virtualizar uma porção significativa das suas funcionalidades, habilitando vários serviços e dispositivos inerentes ao equipamento virtualizado. Possibilita, também, a criação de um autêntico tráfico de dados realizado por dezenas de sistemas sem, no entanto, ter que dispor de todos os equipamentos. Por fim, como pode ser visto na figura 1, a virtualização também pode ser utilizada para emular dispositivos que geralmente são encontrados nas redes típicas de produção. [11]

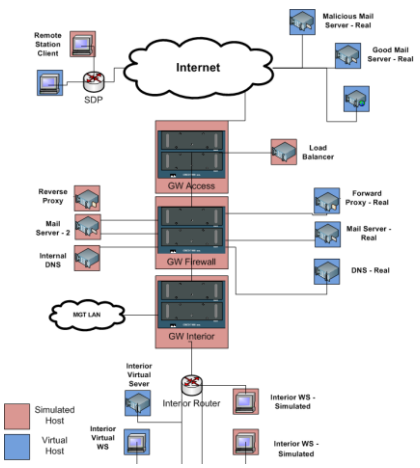

Fig. 1. Dispositivos virtualizados e emulados

Assim, verificamos que a técnica de simulação pode ser empregada na capacitação de recursos humanos aptos a operar no ambiente cibernético. O simulador viabiliza a segurança de pessoal (operadores, pilotos, engenheiros); gera economia de recursos materiais e financeiros; propicia velocidade de processamento; possibilita a realização de testes exaustivos (o que garante segurança e confiabilidade); e viabiliza a utilização de recursos não disponíveis (que são virtualizados).

III. SIMULADORES DE GUERRA CIBERNÉTICA

Atualmente, existe uma variedade de simuladores desenvolvidos com o intuito de propiciar treinamento de recursos humanos que atuam na área da informática. Neste artigo, serão citados alguns simuladores, e suas características principais, analisados no artigo "*State-of-the-art simulation systems for information security education, training and awareness*". [8]

A – CyberProtect, desenvolvido pelo Departamento de Defesa Americano. Foi criado para auxiliar o treinamento dos profissionais de segurança de rede e familiarizá-los com as novas terminologias dos sistemas de informação, concepções e políticas. É um computador que possibilita a realização de exercícios onde os usuários terão a oportunidade de configurar redes seguras e submete-las a ataques. Após os exercícios os usuários recebem um relatório contendo o seu desempenho.

B – *Military Academy Attack/Defense Network* (MAADNET), é uma arquitetura cliente servidor que utiliza simuladores de eventos discretos. Os usuários iniciam suas atividades construindo uma rede para o cliente, de acordo com um dado cenário que é submetido a um servidor, o qual irá simular diferentes eventos. A rede pode ser construída com diferentes componentes (switches, roteadores, estações de trabalho, pontos de acesso wireless, etc). Cada um destes componentes pode ter um ou vários tráficos de rede associados. O ataque criado pode vir da Internet (fora da rede), de um usuário interno a rede ou de ambos os lados. O simulador foi criado para auxiliar a formação dos cadetes da Academia Militar Norte Americana.

C – *CyberOps: NetWarrior*, desenvolvido pela Agência de Defesa de Sistemas da Informação, do Departamento de Defesa Norte Americano. A principal melhoria é a interatividade que o simulador propicia e a sua capacidade gráfica. A ferramenta é um ambiente virtual em 3D, com equipamentos de rede de aparência realista. Neste simulador, os recursos financeiros são limitados e os alunos devem avaliar os custos no momento em que montam as redes. O equipamento permite, em uma mesma simulação, a formação de diversos "times" que podem ser atacantes, defensores ou juízes.

D - *The cyber Defense Technology Experimental Research laboratory* (DETERlab), desenvolvido pela Universidade de Utah. É utilizado como um laboratório nas aulas de segurança cibernética. Suporta experimentos complexos para propiciar pesquisas a respeito do planejamento, criação e interação de cenários. Algumas ferramentas incluem a geração de tráfico de rede, ataques, configuração de rede e coleta de dados. Na data do artigo (2010), o sistema era composto por 2 clusters, com aproximadamente 300 nós experimentais.

E – *CyberCIEGE*, do Centro de Estudos de Segurança de Sistemas de Informação e Pesquisas, da Universidade de Pós-graduação dos EUA. O objetivo do simulador (chamado de jogo) é de proteger o sistema utilizando apropriadas medidas de segurança envolvendo procedimentos, segurança física e técnica. Inclui cenários desenvolvidos para criar novas situações e um vídeo-enciclopédia que educa os alunos durante os exercícios.

F – *Real-Time Immersive Network Simulation Enviromment* (RINSE), é um poderoso simulador desenhado para realizar treinamento e exercício de segurança cibernética em tempo real. O simulador consiste em cinco componentes: o simulador de rede iSSFNet; um gerenciador de banco-de-dados; um banco-de-dados, um servidor de banco-de-dados, e um cliente da rede (telespectador). Os comandos do simulador incluem as ações de: ataque; defesa; diagnostico da rede; controle de dispositivos; e simulação de dados.

G - *Reconfigurable Cyber-Exercise Laboratory (RCEL)*, é o resultado da Tese de Mestrado do aluno R. J. Guild, apresentada na Universidade de Pós-graduação Norte Americana, em 2004. O laboratório é composto por várias estações as quais são responsáveis por funções específicas, tais como: autenticação; controle de domínio; servidores de DNS, DHCP, FTP, syslog, e-mail, banco-de-dados, imagem de disco; certificação PKI; autoridades de registro; ponto de acesso sem fio; honeynet; vulnerabilidades de acesso; switches; roteadores; firewall; sistemas de detecção de intruso; e dispositivos com redes privadas.

No referido artigo [8], outros simuladores são apresentados, contudo nem todos estão dentro do escopo deste trabalho.

IV. TAXONOMIA DOS SIMULADORES CIBERNÉTICOS

Em 2008, Saunders [12] [13] produziu uma taxonomia classificando os simuladores de segurança da informação em 5 categorias distintas: *PacketWars*; *Sniffers* e ferramentas de rede, ambiente de ataque e defesa; simuladores de voos; e *Role-playing*.

Segundo os autores [12] [8], *PacketWars* refere-se a um tipo de simulação que utiliza a rede em ataques e defesas em níveis táticos. A maioria dos simuladores desta categoria são implementados em redes reais, com equipamentos reais, não necessariamente contendo todas as características simuladas ou virtualizadas.

Na sequência, os *Sniffers* compreendem as ferramentas de Simulação e Modelagem de rede, com o uso de analise de protocolo de rede. Os ambientes de ataque e defesa incluem a maioria das ferramentas analisadas pelos autores, podendo ser usada como um jogo. Os simuladores de voo são aplicações construídas usando sistemas dinâmicos ou ferramentas de simulação de eventos discretos.

Por último, os Role-playings são um tipo de simulação que não utiliza recurso computacional, mas diferentes papeis dentro de cenários.

Assim, de acordo com a classificação de Saunders, os simuladores citados no item anterior foram categorizados conforme a tabela a seguir:

TABELA I Classificação dos Simuladores

Nome do Simulador	Categoria
CyberProtect	Ambiente de ataque / defesa
MAADNET	PacketWars
CyberOps: NetWarrior	Ambiente de ataque / defesa
DETERlab	PacketWars
CyberCIEGE	Simulador de voo
RINSE	PacketWars
RCEL	PacketWars

V. MODELO HIERÁRQUICO

Para a análise do simulador cibernético, se propõe um modelo hierárquico que tem por objetivo facilitar a identificação das áreas gerais de atuação do simulador e, em um nível abaixo, destacar as necessidades básicas que atendam as metas traçadas anteriormente. Como último nível do modelo, sugiro relacionar as funcionalidades fundamentais do simulador.

Assim, o modelo apresentado a seguir possuirá 3 níveis hierárquicos denominados: metas, necessidades e funcionalidades.

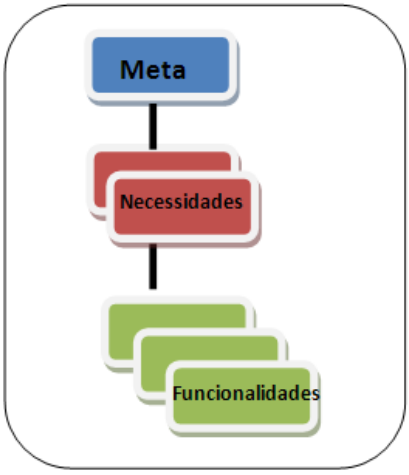

Fig. 2. Níveis do Modelo Hierárquico

Meta (primeiro nível do modelo)

Como nível mais elevado do modelo hierárquico adotado, a Meta identificará a finalidade básica do simulador em estudo, ou seja, qual o seu propósito principal.

Dentro deste nível, identificamos duas grandes vertentes. A primeira é a utilização do simulador como ferramenta facilitadora no processo ensino aprendizagem (foco deste artigo). Como vimos, nos itens anteriores deste artigo, o simulador já é empregado em outros países (que inclusive são referência na área da computação) para complementar o ambiente acadêmico e propiciar formas seguras e realísticas de treinamento.

A segunda grande vertente, para o primeiro nível do modelo sugerido, é a utilização de simuladores para a análise de segurança de redes de computadores.

> "Although the model is primarily designed to be used in testing cyber situational awareness and analysis tools, other applications such as training of systems analysts may also make effective use of the model". [14]

> "...impact assessment for determining how security measures affect system and application performance." [10]

> "To overcome the problems with security analysis using either na exclusive hardware CIS testbed or a simulation of a CIS, Sandia National Labs has developed a cyber security analysis capability using physical hardware, emulated machines, and simulation." [11]

Esta vertente tem por objetivo analisar redes reais, utilizadas por organizações e entidades (civis ou militares), identificar possíveis vulnerabilidades e propor melhorias. Desta forma, será possível identificar possíveis "portas abertas" e fechá-las antes que sejam exploradas.

Fig. 3. Metas para o Simulador Cibernético

Necessidades (segundo nível do modelo)

No segundo nível hierárquico do modelo utilizado, denominado de Necessidades, listamos as características básicas que o simulador deverá possuir para atender a Meta anteriormente identificada.

Para a primeira Meta identificada (treinamento), as seguintes necessidades poderão ser exigidas (Fig. 4):

1) Realismo.
2) Atores. Os atores serão os diferentes níveis de usuários do simulador. Ex: aluno, instrutor, administrador, gerente.
3) Cenários. É o aspecto que indica a necessidade de múltiplos cenários para o treinamento de pessoas com conhecimentos variados.
4) Avaliação. Indica a necessidade de existir formas (funcionalidades) que possibilitem a avaliação dos alunos por parte dos instrutores/professores.

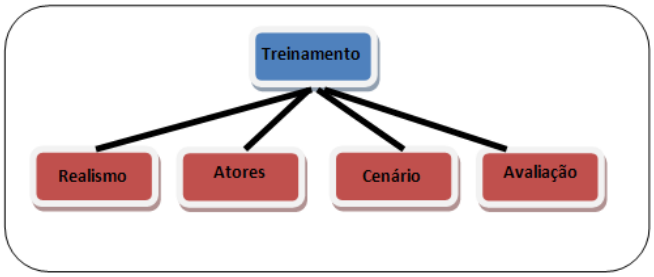

Fig. 4. Necessidades da Meta - Treinamento

Para a segunda Meta (análise de segurança), as seguintes necessidades poderão ser exigidas (Fig. 5):

1) Leitura/Análise da Rede.
2) Identificação de Vulnerabilidades na rede analisada.
3) Simulação de Correções. Possibilita a simulação de alterações na rede analisada para mitigar as vulnerabilidades identificadas.

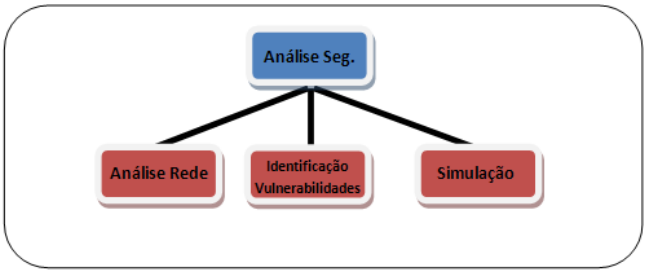

Fig. 5. Necessidades da Meta - Análise de Segurança

Funcionalidades (terceiro nível do modelo)

Como último nível do modelo proposto, denominado de Funcionalidades, identificamos os aspectos funcionais que o simulador de treinamento pode conter para atender cada necessidade identificada anteriormente.

Assim, com base no Simulador de Operações de Guerra Cibernética (SIMOC) [15], algumas funcionalidades podem ser identificadas (Fig. 6):

Necessidade: Atores

1) Cadastrar atores (Aluno, Instrutor, Analista de Segurança, Administrador) que devem ter acesso ao sistema.
2) Gerir Usuário. O administrador deve gerir usuário e senha para os tipos de perfis que acessarão o sistema. Ex: o ator administrador terá acesso a níveis mais altos que os demais atores.
3) Elaborar Treinamento. Consentir que o ator instrutor elabore treinamentos de táticas de defesa e/ou ataque.

Necessidade: Cenário

1) Editar Cenário. Alterar os cenários que foram previamente cadastrados pela firma contratada.
2) Gerir Eventos (ações que influenciarão no ambiente de simulação).
3) Gerir Métricas (são as quantidades medidas e testadas contra os critérios de comparação, a fim de determinar se a condição de acionamento de um dado evento foi atendida ou não).
4) Configurar Objeto (todo e qualquer elemento passível de ser empregado na criação do ambiente de simulação).

Necessidade: Avaliação

1) Relatório de Treinamento. O aluno deverá registrar as ações realizadas durante a simulação, com o objetivo de facilitar a sua avaliação pelo instrutor.
2) Acompanhar Simulação. Permitir que o instrutor monitore a simulação e as atividades executadas pelos aluno.
3) Realizar treinamento. O aluno deverá executar as atividades para ser avaliado.
4) Manual de Apoio. Possibilitar ao instrutor realizar as orientações necessárias para a avaliação.
5) Gerar Log. O programa deverá gerar relatório do treinamento (para avaliação do sistema).

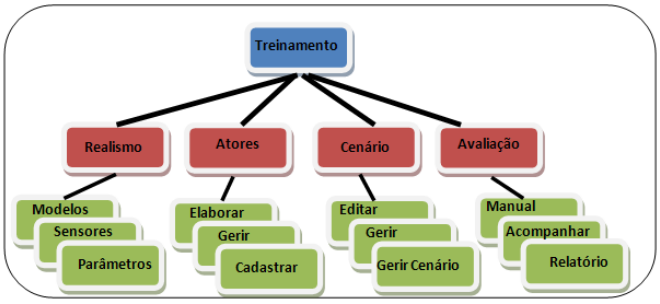

Fig. 6. Modelo Hierárquico (3 níveis)

No intuito de complementar as funcionalidades relacionados acima (com base no SIMOC), identifico as seguintes possibilidades complementares:

1) Para aumentar o realismo, parâmetros adicionais podem ser adicionados aos eventos. Por exemplo: eficiência, descrição, habilidade, criatividade. [14]

2) A medida temporal pode estar presente na simulação, devendo ser: real quando dispositivos são emulados; não real para agilizar o processamento e permitir a análise; e aleatória para comandar os eventos que não temos o controle. [14]

3) Sensores podem estar presentes no simulador, podendo acusar alertas falsos ou verdadeiros. [14]

4) Em um sistema real, possuímos regiões com diferentes velocidades de fluxo e até perda completa de dados. Assim, é importante que o simulador tenha condições de recriar estas situações. [10] Situações que não ocorrem no mundo real não devem ser criadas. [11]

5) Complexidade variável de vulnerabilidades pode ser administrada para possibilitar o treinamento de diferentes níveis de alunos.

6) Possibilidade de utilizar equipamentos reais, conectados ao simulador, para produzir trafego de rede, economizar o poder computacional do simulador, analisar questões em tempo real, dentre outras funcionalidades. [11]

7) Aos moldes do simulador *CyberOps: NetWarrior* [8] o simulador pode possuir recursos financeiros limitados, trazendo mais realidade ao simulador.

8) Utilizar recursos de Inteligência Artificial, no intuito de aprimorar o simulador e propiciar mais uma forma de backup do sistema (utilizando o conhecimento dos alunos).

9) Outras possibilidades: utilização de ferramentas de busca (Ex: Google), com recursos de refinamento de pesquisa (ferramentas lógicas); criar máquinas virtuais para realizar a análise dinâmica de malware; disponibilizar programas de análise de malware (Ex: LordPE, BintText, Process Monitor); realizar análise de rede (Ex: Wireshark); disponibilizar linguagens de programação, para a confecção de exploits, bibliotecas de ataques, etc.

Concluindo; as funcionalidades do simulador com meta de análise de segurança não serão apresentadas por fugir ao escopo do trabalho. Sua análise parcial teve por objetivo proporcionar uma comparação entre as abordagens na tentativa de facilitar o entendimento do modelo proposto. No entanto, identifico igual valor entre as metas apresentadas para o simulador cibernético e saliento a importância do estudo.

VI. OBSERVAÇÕES FINAIS

As ações cibernéticas deixaram de ser realidade virtual, de filmes de ficção. Seus efeitos já podem ser sentidos com todas as suas implicações, boas ou ruins.

Os simuladores são ferramentas poderosas no campo da educação e estão sendo usados, há alguns anos, com excelente aceitação. Segundo o pesquisador David N. Nicol, da Universidade de Illinois [10], a utilização de simuladores no estudo de ciberataques é adequado e prometedor.

Por características especiais do campo cibernético, seu estudo e treinamento necessitam de um amplo número de cenários realísticos, sem, no entanto, que cause prejuízo a pessoas ou instituições, ou ainda que fira leis existentes. Hoje, no Brasil, uma má utilização das ferramentas cibernéticas pode, por exemplo, ser enquadrada nas leis 9.296, de 24 de julho de 1996 ou na lei 12.527, de 18 de novembro de 2011. Cabe ressaltar que no dia 15 de maio do corrente ano, a Câmara dos Deputados aprovou o primeiro texto do Projeto de Lei 2793/2011, que trata sobre a tipificação criminal de delitos cometidos a partir de novas tecnologias, inclusive pela internet. A lei pretende garantir a segurança das pessoas que utilizam a internet e dispositivos eletrônicos, tratando como crime as ações de: falsificação de cartões de crédito, invasão de dispositivos eletrônicos, criação e propagação de "vírus de computador" e ações de interrupção ou prejuízo de tráfego de dados.

Embora atualmente a legislação brasileira ainda esteja deficiente a este respeito, o mundo cibernético não tem fronteiras (conforme ressalta, em diversas obras e artigos, Raphael Mandarino Júnior, diretor do Departamento de Segurança da Informação e Comunicação, da Presidência da República) e podemos descuidadamente atravessar as barreiras nacionais e transcorrer em crime capitulado pela legislação internacional.

Assim, a utilização de simuladores na educação cibernética tende a ser uma realidade, mas para o desenvolvimento de softwares, e a sua adequada exploração, é fundamental a edificação de um conhecimento profundo a respeito do assunto [14].

Por se tratar de um software de uso estratégico, que visa o treinamento de civis e militares na segurança institucional e governamental, seu desenvolvimento se reveste de particularidades. A princípio, a sua aquisição no mercado internacional pode significar falta de segurança do produto adquirido. Pois, como é de conhecimento, um software pode conter bombas lógicas, *backdoors*, e diversos tipos de vulnerabilidades (*zero day)* de difícil identificação.

Desta forma, chegamos a conclusão: tecnologia de segurança nacional não se compra em prateleira internacional. Neste ímpeto, o Exército Brasileiro, por força da Estratégia Nacional de Defesa (END), receberá, nos próximos dias, o Simulador Operacional de Guerra Cibernética (SIMOC), que foi desenvolvido pela empresa nacional DECATRON para ser utilizado no primeiro Curso de Guerra Cibernética da América Latina, coordenado pelo Centro de Defesa Cibernético brasileiro. Órgão que vem

despertando grande interesse dos países vizinhos e de potências cibernéticas.

Mas, o SIMOC não é um produto finalístico e certamente terá muito a ser aprimorado. Assim, o intuito deste trabalho foi de, partindo de um modelo hierárquico sugerido, identificar e ensaiar algumas funcionalidades possíveis para um simulador cibernético, vocacionado a capacitação de recursos humanos. A intenção é de auxiliar em trabalhos futuros no desenvolvimento de um simulador desta natureza.

Com um simulador nacional, criado para as necessidades internas, com as características brasileiras, estaremos desenvolvendo uma verdadeira "arma" de defesa ou, se necessário, de ataque para ser utilizada na Guerra Cibernética.

REFERÊNCIAS

1. FLÁVIO CARVALHO. Information Week. **O Futuro da Segurança da Informação**, 25 junho 2012. Disponivel em: <http://informationweek.itweb.com.br/8980/o-futuro-da-seguranca-da-informacao/>. Acesso em: 24 julho 2012.
2. PERSONA, M. O poder da Informação, 28 dezembro 2006. Disponivel em: <http://www.youtube.com/watch?v=HgIn7wwyY7w>. Acesso em: 24 julho 2012.
3. WILSON BIANCARDI COURY. Revista de Tecnologia da Informação. **Poder da Informação**, 13 setembro 2001. Disponivel em: <http://www.timaster.com.br/revista/artigos/main_artigo.asp?codigo=424>. Acesso em: 24 julho 2012.
4. FUSCO, C.; MATOS, C. Folha.com. **Economia hacker gira US$ 150 bilhões em todo o mundo**, 05 junho 2011. Disponivel em: <http://www1.folha.uol.com.br/mercado/925608-economia-hacker-gira-us-150-bilhoes-em-todo-o-mundo.shtml>. Acesso em: 05 julho 2012.
5. MACHADO, C.; CRUZ, L. Guerra Anônima, v. Info Exame, n. 306, 2011.
6. ESTRATÉGIA Nacional de Defesa. Brasília: [s.n.], 2008.
7. DELOOZE, L.; MCKEAN, ; GRAIG,. Incorporating Simulation into the Computer Security Classroom, Savannah, 2004. ISSN 0-7803-8552-7/04.
8. PASTOR, ; DÍAZ, ; CASTRO,. State-of-the-art simulation systems for information Security Education, Training and Awereness, Madri, 2010. ISSN 978-1-4244-6571-2/10.
9. SRIKUMAR, S. The Simulator Classroom: Why Corporations are Betting Heavily on Sophisticated New Simulation Software, v. Vol. 164 (3), p. 56.
10. LICOL, D. M. Modeling and Simulation in Security Evaluation, Urbana-Champaign, 2005. ISSN 1540-7993/05.
11. LEEUWEN, V. et al. CYBER SECURITY ANALYSIS TESTBED: COMBINING REAL, EMULATION, AND SIMULATION, Albuquerque, 2010. ISSN 978-1-4244-7402-8/10.
12. SAUNDERS, J. H. **The Case for Modeling and Simulation of Information**. Disponivel em: <http://www.johnsaunders.com/paper/securitysimulation.htm>. Acesso em: dezembro 2008.
13. SAUNDERS, J. H. **Modeling the Silicon Curtain**. [S.l.]: SANS Institute, 2001.
14. KHUL, M. et al. CYBER ATTACK MODELING AND SIMULATION FOR NETWORK SECURITY ANALYSIS, EUA, 2007. ISSN 1-4244-1306-0/07.
15. SIMULADOR de Operações de Guerra Cibernética (SIMOC) - Projeto Executivo. Rio de Janeiro: [s.n.], 2012.