TENDÊNCIAS INTERNACIONAIS EM CIBERCAPACITAÇÃO: EQUIPES DE TRATAMENTO DE INCIDENTES DE REDE

Tenente-Coronel Aristides Sebastião Lopes Carneiro

O Tenente-Coronel de Comunicações Lopes Carneiro serve no Centro de Defesa Cibernética do Exército. É doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME); especialista em Tecnologia e Projeto de Redes de Computadores (Universidade Estácio de Sá), em Educação (Centro de Estudos de Pessoal) e em Bases Geo-históricas para as Operações Militares (ECEME); bacharel em Ciências Militares (Academia Militar das Agulhas Negras) e Engenharia Elétrica (Universidade Gama Filho). Serviu no Estado-Maior do Exército, como formulador da doutrina de Comando e Controle. (lcarneiro1994@yahoo.com)

O objeto de estudo do presente artigo consiste nas contribuições internacionais da França, do Reino Unido, da Alemanha, da Itália, da Espanha e dos Estados Unidos da América (EUA), que podem ser úteis para o desenvolvimento das competências dos membros das equipes de tratamento de incidentes de rede (ETIR) do Exército Brasileiro (EB). O viés sob o qual o assunto foi abordado foi o educacional, procurando-se ressaltar as principais estratégias e práticas educacionais utilizadas para esse propósito. A escolha desses países é fundamentada no fato de que se trata de países centrais, de estatura geopolítica comparável ou superior à do Brasil e cujas experiências no setor podem servir de subsídio às iniciativas brasileiras. O aspecto linguístico foi outro fator predominante por facilitar a coleta de material em fonte primária.

A escolha do tema deve-se ao fato de que os *Computer Emergency Readiness Team* (CERT) são órgãos de grande importância no setor cibernético, em termos operativos e técnicos, constituindo verdadeira linha de frente contra os ataques cibernéticos, os quais têm aumentado exponencialmente nos últimos anos. No EB, a infraestrutura para tratamento de incidentes de redes no Exército (ITIREx) é constituída pelo Centro de Coordenação para Tratamento de Incidentes de Rede (CCTIR/EB), localizado no Centro Integrado de Telemática do Exército (CITEx), e pelas seções de tratamento de incidentes de rede (STIR) situadas nos centros de telemática de área (CTA) e nos centros de telemática (CT).

Este artigo foi elaborado com o objetivo de buscar a investigação do seguinte problema: quais são as principais contribuições desses países no desenvolvimento de competências para a atuação na segurança cibernética (Seg Ciber), particularmente em uma ETIR? Tomou-se por hipótese que existem diversos aspectos da capacitação conduzida nesses países que podem ser considerados na capacitação realizada no EB.

Para isso, utilizou-se o método observacional, visto que o trabalho teve base na identificação de aspectos essenciais e acidentais de fenômenos ou eventos empíricos relativos à capacitação de recursos humanos (RH) em Seg Ciber. Adicionalmente, empregou-se o método comparativo ao se identificarem semelhanças e diferenças na maneira de conduzir a cibercapacitação nesses países. Na pesquisa, foram utilizadas as seguintes técnicas: estudo exploratório, pesquisa qualitativa e discurso do sujeito coletivo. A seguir, serão apresentados os resultados mais significativos resultantes da aplicação das técnicas mencionadas.

COMPETÊNCIAS PARA ATUAR EM UMA ETIR

Inicialmente, procurou-se investigar quais são as competências requeridas para a atuação como membro de uma ETIR. Por meio da pesquisa documental, foram colhidos estudos da *European Network and Information Security Agency* (ENISA), do *Help Desk Institute* (EUA) e da *Carnegie Mellon University* (EUA), cujos conteúdos foram aplicados à metodologia das Normas para Projetos-Piloto de Ensino por Competências do EB. A investigação foi complementada com a pesquisa de campo para que fosse feito o cruzamento de dados, o que resultou no seguinte elenco de competências necessárias à atuação na ETIR, que podem ser agrupadas em duas categorias: competências técnicas e pessoais.

Alguns outros aspectos, que não se enquadram nas categorias anteriores, foram considerados como "outras competências".

Competências Técnicas

Atuar como profissional certificado em Segurança de Sistemas de Informação:

- aplicar conhecimentos atualizados dos elementos de uma infraestrutura de rede (*routers, switches, DNS, proxy,* correio eletrônico, etc) no tratamento de incidentes, auxiliando, do ponto de vista da segurança, na configuração das ferramentas, das aplicações e da infraestrutura de rede;
- aplicar conhecimentos de protocolos e tecnologia de internet no tratamento de incidentes;
- aplicar conhecimentos de sistemas Linux e Unix para fortalecer a segurança em plataformas de *hardware* e *software* diferentes (sistemas Linux e Unix);
- fortalecer a segurança em plataformas de *hardware* e *software* diferentes (sistemas Windows); e
- aplicar conhecimentos de aplicações da internet (SMTP, HTTP(s), FTP, *Telnet*, SSH, etc) no tratamento de incidentes.

Atuar como *incident handler:*

- organizar e operar um CERT;
- tratar ameaças de segurança (DDoS, falsificação de identidade, *sniffing,* alterações de páginas ou *web-defacement*);
- operar e manter dispositivos de detecção/prevenção de intrusão, de correlação de registros e de *honeypots;*
- analisar artefatos cibernéticos maliciosos; e
- aplicar técnicas de ataque e de defesa.

Atuar como perito forense computacional:

- analisar riscos e implementar medidas de segurança para realizar auditoria de segurança e para homologar e certificar soluções de TI;
- aplicar conhecimentos sobre os instrumentos de gerência administrativa de rede; e
- preservar artefatos dos incidentes tratados, quando puderem ser parte de ato ilícito previsto na legislação brasileira, transgressão disciplinar ou crime militar.

Atuar segundo as medidas de inteligência e contrainteligência:

- tratar com documentos sigilosos;
- atuar com discrição;
- atuar seguindo as medidas contraengenharia social;
- saber reportar-se às pessoas certas;
- tratar e armazenar dados; e
- colocar discos em cadeias de custódia.

Saber realizar *pentesting:*

- realizar varredura;
- realizar enumeração;
- identificar falhas e vulnerabilidades;
- saber burlar a proteção (realizar engenharia social, explorar falhas e más configurações, realizar negação de serviço;
- saber realizar *cross-site scripting, directory traversal, antivirus avoidance, manual shellcode encoding);*
- aplicar técnicas e ferramentas de *hacking;*
- realizar *pentesting* em redes *wireless*;
- realizar *pentesting* em redes Windows e Linux; e
- explorar e atacar as modernas aplicações *front-facing web.*

Projetar redes para atender à segurança da informação:

- projetar redes que atendam a aspectos abrangentes da Seg Info;
- projetar redes que atendam a aspectos relativos à segurança das infraestruturas;
- projetar redes que atendam a aspectos relativos à segurança do sistema de TI, especificando componentes de redes, como servidores, roteadores, *switches, firewalls,* entre outros;
- projetar redes que atendam a aspectos de segurança de rede; e
- e projetar redes que atendam a aspectos de segurança nas aplicações.

Gerar estatísticas:

- aplicar conhecimentos sobre estatística em um CERT; e
- empregar ferramentas computacionais (*hardware* e *software)* na geração das estatísticas.

Validar ativos para o SisTEx:

- validar *hardware* do servidor; e
- validar *softwares* do servidor.

Dominar o idioma inglês:

- ler e compreender textos diversos, particularmente sobre segurança computacional;
- expressar-se no idioma inglês, particularmente sobre segurança computacional, em situações diárias de um CERT, em aulas ou em eventos (como palestrante);

- redigir textos em inglês, particularmente sobre segurança computacional;

- empregar expressões da língua inglesa segundo as normas gramaticais; e

- ouvir e compreender anglofônicos em situações diversas, particularmente na vida diária de um CERT, em aulas ou em eventos sobre segurança computacional.

Possuir conhecimentos técnicos específicos de sua área de especialização.

Competências Pessoais

- capacidade de sensibilização do público interno;

- disciplina e responsabilidade para o cumprimento de normas e de missões;

- agir com flexibilidade, criatividade e espírito de equipe enriquecedor;

- boas capacidades analíticas, pois a análise forense exige meticulosidade;

- capacidade para explicar assuntos técnicos difíceis com linguagem simples;

- boa atitude para a confidencialidade e trabalho de maneira procedimental (ser metódico);

- boas capacidades organizativas e gerenciais;

- habilidade para lidar com situações de estresse;

- sólidas habilidades comunicativas e de redação;

- atitude aberta e vontade de aprender;

- capacidade de decisão; e

- capacidade de priorização.

Outras Competências

- disposição para trabalhar em um sistema de vinte e quatro horas por dia durante os sete dias da semana ou sempre que seja necessário (dependendo do modelo do serviço);

- máxima mobilidade (em caso de emergência);

- disponibilidade para viajar;

- nível educativo; e

- experiência de trabalho no âmbito da segurança em TI.

ORGANISMOS SUPRANACIONAIS

Uma vez consolidado o elenco sintetizado, a questão central da investigação passou a ser a abordagem das alternativas para o desenvolvimento dessas competências. Ficou evidenciado na pesquisa o relevante papel dos organismos supranacionais nessa capacitação. Entre esses organismos, merece destaque a já mencionada ENISA. Esta possui um programa de exercícios [1] com características do ensino orientado por competências. Esse material insere o aluno em diversos cenários, ou situações-problemas relacionadas ao trabalho de uma ETIR. No desenvolvimento das capacidades do profissional da ETIR, merece também destaque a construção do conhecimento por meio da colaboração e do intercâmbio de conhecimentos profissionais proporcionado pelos seguintes organismos supranacionais: *European Government* CERTs (EGC), *Task Force* CSIRT (TF-CSIRT), *Forum for Incident and Security Teams* (FIRST), *European Network and Information Security Agency* (ENISA) e CSIRT. A seguir, serão mencionadas as principais contribuições de cada país em particular.

FRANÇA

A existência do Centro de Formação para a Segurança dos Sistemas de Informação (*Centre de Formation a la Sécurité des Systémes d'Information* - CFSSI), serviço da Agência Nacional de Segurança dos Sistemas de Informação (*Agence Nationale de la Sécurité des Systèmes d'Information* - ANSSI) encarregado da formação de agentes públicos na área da segurança dos sistemas de informação (SSI), demonstra a preferência dos franceses por um modelo de capacitação voltado para as necessidades peculiares de seus ministérios. Segundo a ANSSI [2], os cursos do CFSSI incluem desde os de rápida duração até os de mestrado, sendo que seus pré-requisitos, disciplinas, duração, estrutura dos cursos, são informações que podem servir como subsídio para o design curricular dos cursos brasileiros. O embasamento teórico do CFSSI é combinado à práxis laboral, considerada fundamental. Por outro lado, segundo o modelo de proteção ativa do Estado – ciberespaço e infraestruturas críticas, o enfoque pragmático é o foco da capacitação realizada na empresa Thales [3], caracterizada pela busca de soluções para os problemas reais dos ministérios da França, pela ênfase nas práticas laboratoriais e no treinamento empregando um sistema de simulação de ataque e de reação do operador. Outro ensinamento refere-se ao CERT das Forças Armadas (FA), denominado CALID. As FA da França possuem CERT com status "credenciado". No Brasil, isso não ocorre. Inclusive, não há um CERT comum das três Forças. As ligações do CERT localizado no CITEx são mais intensas com o CERT.BR. As principais implicações desse status "credenciado" referem-se basicamente à maior facilidade de troca de informações com os demais CERT ao redor do mundo, com o consequente ganho para a atualização dos seus membros.

Os principais centros civis franceses são o Centre *de Formation a la Sécurité des Systèmes d'Information* (CFSSI), onde são realizados o curso de Especialista em

Segurança de Sistemas de Informação (ESSI) e o curso sobre Incidentes de Segurança; e a Empresa Thales, onde são realizados os cursos de Monitoramento Operacional, Resposta e Alerta, Teste de Penetração e Perícia Forense Computacional.

Entre os centros militares, destacam-se o *Centre de Recherche des Écoles Saint-Cyr Coëtquidan*, onde é ministrada a disciplina de *Cyber Defense*, e a *École de Transmission*, em *Cesson-Sévigné*, onde é mininistrado o Curso *Systèmes d'Information* (SINF).

REINO UNIDO

A estratégia de segurança cibernética britânica inclui um fluxo de trabalho sobre habilidades e educação, propiciando, entre outros aspectos, a aproximação entre governo e indústria. A *Royal Holloway University* destaca-se como um dos maiores grupos acadêmicos de segurança do mundo, com estudos na área há cerca de 20 anos, que conta com contribuições de muitos professores, visitantes internacionais, colegas e consultores com uma grande variedade de experiências, o que é muito enriquecedor. Assim, é possível desenvolver e lançar soluções para aprimorar a formação, mediante o fornecimento de credenciamento ou de incentivos, planos de carreira dentro e fora do governo. As conexões com grande número de companhias, líderes na área de Segurança da Informação, trazem literalmente esses atores para dentro da universidade. Ademais, quanto às estratégias de ensino, merecem menção o *Coaching* [4] *e Mentoring* [5], entre as principais inovações no ensino organizacional, aplicáveis ao caso de um CERT. No Reino Unido, ficou evidenciada a existência de planos de carreira no setor cibernético. O país possui parcerias em certificação com os países do *Commonwealth,* do Oriente Médio, Singapura, Hong Kong, China, realizando consulta para governos e agências e participando do esquema europeu, principalmente com a Irlanda, em atividades da polícia.

A *Royal Holloway University* possui o curso de Pós-Graduação em Segurança da Informação e o curso de Resposta a Incidentes (2 dias), que pode ser inserido no contexto do programa de Pós-Graduação.

Entre as escolas militares, merece menção a *Cranfield University Defence and Security*, que conta com os seguintes cursos de Pós-Graduação:

- Defesa Cibernética (Def Ciber) e Segurança da Informação; e
- Computação Forense: especialização ou mestrado.

Essa escola militar também possui os seguintes cursos de curta duração:

- Computação Forense;
- Computação Forense Avançada;
- Computação Forense: Fundamentos;
- Computação Forense: *Internet*;
- Computação Forense: Questões Jurídicas e Audiências;
- Computação Forense: documentos do *Microsoft Office*;

Royal Holloway University, Londres.

- Computação Forense: Programação para Profissionais;
- Computação Forense: Usando o Linux;
- Análise Forense Computacional: Redes;
- Segurança Cibernética;
- Segurança e Gestão de Riscos;
- Informática: Segurança Corporativa; e
- Redes Neurais.

ALEMANHA

Segundo o CERT-*Verbund* [6], a cooperação entre os CERT alemães é colocada em uma base uniforme, com vistas à proteção das redes nacionais de tecnologia da informação, a fim de ser capaz de responder, conjunta e rapidamente, a ocorrências que surgirem. Outra contribuição é o modelo de proteção básica em TI, proposto pelo BSI [7] que, por ser um modelo nacional de capacitação gradativo, organizado em camadas, com excelente detalhamento, pode servir de referência no planejamento dos cursos de segurança cibernética. Dessa forma, primeiro se constrói o conhecimento básico, para que se possam abordar questões mais especializadas, relativas ao tratamento de incidentes de rede.

Esse modelo alemão de proteção básica em TI é organizado em camadas básicas e camadas específicas sobre tratamento de incidentes.

Camadas Básicas

- Aspectos abrangentes: 16 módulos;
- Infraestrutura: 12 módulos;
- Sistemas de TI: 8 módulos;
- Redes: 7 módulos; e
- Programas: 17 módulos.

Camadas Específicas sobre Tratamento de Incidentes

- Planejamento e Concepção: 3 módulos;
- Execução: 12 módulos; e
- Ambientes Empresariais: 17 módulos.

Pela análise curricular do curso de mestrado em segurança em TI da *Freie Universität Berlin*, a qual segue as orientações do BSI, verifica-se que esse modelo de capacitação evidencia a vocação para a pesquisa de aspectos atuais em segurança em TI, proporcionando embasamento teórico mais amplo. Quanto ao processo de certificação na Alemanha, segundo o BSI, o qual tem ciclo de três anos, é notória a preocupação com a manutenção, com a supervisão de competências e com a gerência da concessão da capacitação, devido à rápida evolução tecnológica. Há também grande ênfase nas pesquisas sobre o alerta antecipado, estando esse assunto presente na recente estratégia de segurança cibernética alemã [8] e, consequentemente, o assunto tem sido discutido em conferências, workshops e artigos científicos de pesquisadores alemães, conforme o DFN-CERT. Merece, ainda, destaque a participação da Alemanha no *Cyber Europe* 2010, segundo a ENISA , entre os 22 estados-membros, atividade que complementa a formação das ETIR. No campo

Freie Universität Berlin

educacional, a *Bundeswehr Universität*, Universidade das Forças Armadas, localizada em Munique, possui um programa de educação para indivíduos com altas habilidades (superdotados). Acredita-se que superdotados quanto à inteligência lógico-matemática podem vir a ser recrutados para o setor cibernético.

Há estreito relacionamento CERT – Academia, com destaque para a ligação DFN-CERT. Na *Freie Universität Berlin*, são oferecidos os seguintes cursos de mestrado em segurança de TI (2 anos) e de testes de penetração.

No âmbito militar, há os seguintes cursos de mestrado na B*undeswehr Universität*, em Munique: *Cyber Defense & Management* (IT -Sicherheit)e Gestão em TI.

Destacam-se, ainda, os cursos ministrados pela NATO School (Escola da Organização do Tratado do Atlântico Norte), em Oberamergau:

- *Cyber Incident Handling & Disaster Recovery Planning Course;*
- *Network Vulnerability Assessment Course;*
- *Network Security Course;*
- *Network Traffic Analysis Course; e*
- *NATO Security Course.*

ITÁLIA

Na Universidade de Milão, como nas outras universidades analisadas, há cadeiras de segurança na graduação e em cursos de rápida duração, como o *Sicurezza dei Calcolatori e delle Retti* [9]. Entretanto, é prioritariamente no curso de mestrado que se estuda a segurança computacional. Pela análise do material

Universidade de Milão

do curso e da coleta de informações na pesquisa de campo, a metodologia de ensino é tradicional, com ênfase em aulas expositivas, palestras e práticas laboratoriais. O desenvolvimento de competências tem caráter subsidiário, apesar da égide da Declaração de Bolonha. Segundo o CERT-IT, um ponto de destaque é a organização do Campeonato Nacional de *Hacking* [10] pela Universidade, juntamente com o Centro de Tratamento de Incidentes de Rede, o que demonstra haver forte ligação entre eles. Além disso, segundo a ENISA, o país também participou do *Cyber Europe* 2010, o que expressa a busca de atividades hands-on para atestar e aprimorar a capacitação das ETIR.

Quanto às instituições civis, merece destaque a Universidade de Milão, onde há os seguintes cursos de mestrado em segurança computacional e de *Sicurezza dei Calcolatori e delle Retti* (3 meses).

Entre os centros militares, pode-se citar a NATO Communications and Information Systems School, em Latina, onde são conduzidos o NATO *Computer Security* (COMPUSEC) *Practitioners Course* e o NATO *Information Systems Security* (INFOSEC) Officer Course.

ESPANHA

Para o Ministerio de Defensa da Espanha (MINISDEF) [11], a Criptologia nacional é princípio irrenunciável tanto para a proteção das comunicações como para a cibercapacitação. Nas FA, os militares realizam os cursos do Centro Criptológico Nacional (CCN), além de outros cursos on-line, seminários, cursos de formação e aperfeiçoamento das três FA, cursos conjuntos, mestrado por diferentes universidades, jornadas técnicas de temas específicos no *Centro Superior de Estudios de la Defensa Nacional* (CESEDEN) e Jornadas de Segurança da Informação do MINISDEF. Entre os *Ejercicios de ciberdefensa*, estão os organizados pelos EUA (*US DoD International Cyber Defense Workshop)*, os dois primeiros exercícios de Defesa Cibernética da OTAN, em 2009 e 2010, os dois Exercícios de Def Ciber das FA, em 2009 e 2010, o *Cyber Europe* 2010, além da criação de uma comunidade de Defesa Cibernética no Ministério. Desses exercícios, também participaram todos os outros países estudados, os quais fazem parte da OTAN.

Os cursos do CCN na área de Segurança de Tecnologia da Informação e Comunicações (STIC), realizados no primeiro semestre em 2010, foram os seguintes:

- Cursos Informativos e de Conscientização em Segurança;
- VII Curso STIC (2 meses);
- Cursos Básicos de Segurança (todos com duração de 5 dias);
- V Curso Básico STIC: Meios Windows;
- V Curso Básico STIC: Meios Linux;
- V Curso Básico STIC: Banco de dados;
- V Curso Básico STIC: Infraestrutura de Rede;
- *Cursos Específicos de Gerenciamento de Segurança (5 dias)*
- III Curso *Common Criteria*;
- Cursos de Especialização em Segurança (todos 5 dias)
- VII Curso Credenciamento STIC: Meios Windows;
- V Curso STIC - Redes Sem Fio.

No segundo semestre de 2010, foram ministrados os seguintes cursos, na área de STIC:

- Cursos Específicos de Gerenciamento de Segurança
- VII Curso de Gerenciamento STIC (2 meses);
- XXII Curso de Especialidades Criptológicas (CEC) (3 meses);
- Cursos de Especialização em Segurança (todos com duração de 5 dias)
- VI Curso STIC: Programa de Segurança; e
- VI Curso STIC: Detecção de Intrusão.

ESTADOS UNIDOS

Entre as 168 instituições de ensino superior que disponibilizam cursos relacionados à área, destacam-se os cursos de treinamento e educação da *Carnegie Mellon University*, destinados a profissionais do setor público e privado. Outras instituições dignas de nota são o SANS *Institute e o International Information Systems Security Certification Consortium* (ISC)².

Com o Instituto de Engenharia de *Software*

(SEI), são oferecidos cursos para gestores de CSIRTs e *experts* técnicos incluindo técnicas práticas em cenários fictícios. Estes são cursos de curta duração baseados em palestras, exercícios com perguntas teóricas, alguns cenários e *role playing*, em que os alunos executam papéis variados. O material do curso, o qual é constantemente atualizado, é fundamentado em apostilas nas quais há descrições sobre os slides das palestras.

Merecem também menção os cursos da *Offensive Security,* que incluem *pentesting.* Outro ponto forte dos americanos é a existência de um plano de carreira formalizado para os militares que atuam na área, segundo o Departamento da Força Aérea dos EUA [12].

Além disso, na área do ensino, os EUA têm inúmeras publicações que trazem ensinamentos sobre a forma de desenvolver competências. Por exemplo, merecem menção os *cases* (estudos de caso) da *Harvard University*, a aplicação dos conceitos e recursos de Memória Total no ambiente escolar [13], estratégias de aproximação de universidades com empresas, como ocorre no Vale do Silício, recursos de TIC e aprendizagem híbrida (integração de aspectos formais e informais do aprendizado) [14]. Entre os exercícios de simulação mais importantes, encontram-se o *Red Team versus Blue Team, Cyber Defense Exercise, Capture the Flag,* ICDW, *Treasure Hunt, Botnet-inspired Competition.* Os EUA são também um país em que há a valorização da educação de indivíduos com altas habilidades, como na Universidade de *Stanford* [15].

Os *Computer Emergency Readiness Team* (CERT) são órgãos de grande importância no setor cibernético, em termos operativos e técnicos, constituindo verdadeira linha de frente contra os ataques cibernéticos.

Entre os cursos da *Carnegie Mellon University,* relacionados à Segurança de Rede, destacam-se:

- Visão Geral de Criação e Gestão CSIRTs;

-Segurança de Informação para Pessoal Técnico;

-Segurança de Informação Avançada para Pessoal Técnico;

- Introdução ao Modelo de Gestão de Resiliência CERT;

- Administração da Segurança de Informação de Empresa: uma Abordagem Técnica para Alcançar uma Defesa em Profundidade;

- Codificação de forma segura em C e C++;

- Tratamento de incidentes;

- Criação de uma Equipe de Resposta a Incidentes a Segurança de Computadores (CSIRT);

- Gerenciamento de Gerenciando CSIRTs;

- Fundamentos de Tratamento de Incidentes;

- Tratamento Avançado de Incidentes;

- Programa de Aprendizado de *Malware*;

- *Risk Management, Internal Controls, and Auditing for Leading* (RIA);

- *Cyber Security for Information Leaders* (SEC); e

- *Terrorism and Crime in Cybersapace* (TCC).

Entre as instituições militares, merece ser mencionado o *iCollege, da National Defense University,* o qual possui os seguintes cursos:

- Mestrado *Governement Information Leadership* (GIL);

- *Information Assurance and Critical Infrastructure Protection* (AII);

- *Approval to Operate: Information System Certification and Accreditation* (ATO);

- *Cyberlaw* (CBL);

- *Critical Information Infrastructure Protection* (CIP);

- *Critical Information Systems Technologies* (CST);

- *Data Management Strategies and Technologies: a Managerial Perspective* (DMS);

- Enterprise Information Security and Risk Management (ESS);

- *Governance in Cyberspace* (GIC);

- *International Perspective on Cyberspace (*IPC);

- *Information Warfare, and Military Strategy* (IWS); e

- *National Intelligence & Cyber Policy* (NIC).

CONSIDERAÇÕES FINAIS

Da análise do elenco de competências necessárias ao membro da ETIR e pela observação da metodologia de recrutamento para os CERT nos países estudados, observa-se que o perfil mais recomendado é preferencialmente o de engenheiro da computação, ainda que essa graduação não seja considerada

obrigatória. O ideal é que o engenheiro tenha concluído mestrado em segurança computacional e que tenha experiência profissional de, no mínimo, seis meses. Além disso, é importante que tenha conhecimentos sobre as interfaces entre os diferentes tipos de redes, sobre a estrutura das organizações e a compreensão de como elas interagem. No caso do EB, evidentemente, deve-se ter o cuidado de não restringir demais o universo selecionável ao se buscar apenas um profissional com todas as qualificações ideais, tendo-se em vista a realidade atual do Brasil, relativa à escassez de profissionais na área.

Quanto ao desenvolvimento dessas competências, por tudo o que foi exposto, foi comprovada a hipótese de que existem diversos aspectos da capacitação realizada nesses países que podem ser considerados úteis na capacitação das ETIR do EB. Tanto sob o ponto de vista educacional, relativo às diferentes estratégias e práticas educacionais para desenvolver competências, como sob o viés técnico do tratamento de incidentes, há inúmeras contribuições que podem subsidiar o trabalho dos gestores de ensino e dos tomadores de decisão no EB.

A capacitação em segurança cibernética destinada aos militares é semelhante àquela dedicada aos civis, sendo complementada com a abordagem específica realizada em escolas militares.

Como tendência geral nos países estudados, fica evidente a combinação entre educação acadêmica (graduação, pós-graduação, mestrado e doutorado) e cursos práticos de rápida duração. No âmbito de cada curso, o fator-chave para o sucesso de um programa de desenvolvimento de competências bem sucedido é a integração das diferentes estratégias e práticas docentes, tais como:

- práticas laboratoriais;
- exercícios de simulação e jogos, como os exercícios *americanos Red Team versus Blue Team, Cyber Defense Exercise, Capture the Flag, ICDW, Treasure Hunt, Botnet-inspired Competition*;
- projetos de pesquisa;
-projetos de programação;
- tarefas escritas;
- tarefas de leitura/relatórios;
- estudos de caso;
- estágios;
-projetos interdisciplinares;
- *role playing*;
-*computer-based training;*
- *e-learning;*
-participação em olimpíadas de informática; e
- aproximação com empresas.

Essas práticas docentes também podem ser enriquecidas com a utilização das seguintes Tecnologias de Informação e Comunicações (TIC):

- ambientes virtuais de aprendizagem (AVA), como o *Moodle* e o *Blackboard*;
- produtores de vídeos educativos, como o *Camtasia Studio*;
- publicadores, como o ISUU;
- mapas conceituais, como o *X Mind, Visual Mind, Free Map e C Map*;
- recursos de compartilhamento, como o *MediaWiki*, e o *Google Docs*;
- construtores de Blogs, como o b2 *evolution*;
- gestores de fóruns, como o phpBB;
- gerenciadores de vídeo, como o *Clip Bucket*;
- servidores *Web*, como o LAMP;
- tecnologias de comunicação, como e-mail, teleconferência e vídeoconferência, IRC;
- tecnologias de organização e apresentação, como o *Powerpoint, o Semantic Networking Tools e o Gift Construction*;
- tecnologias de busca de informação e de gestão da informação, como web, internet, bases eletrônicas de dados, o proclte e o endnotes;
- tecnologias de áudio e vídeo, como áudio e *videotape, Compact audio/vídeo, streaming audio/vídeo*; e
- ferramentas de criação e manipulação, como bases de dados estatísticos, o *Toolbook e o Authorware,* o *E-memory*, o *Voice mail,* os grupos na internet e as tecnologias de multimídia.

É preciso que a capacitação seja up-to-date, com estruturação gradativa, orientada pelos princípios da religação dos saberes [16] e da interdisciplinaridade [17].

Outra tendência é que, até o presente momento, a capacitação em *Seg Ciber* destinada aos militares é semelhante àquela dedicada a civis, sendo complementada com a abordagem específica realizada em escolas militares.

Na pesquisa de campo, observou-se que a capacitação é feita mediante certificações americanas combinadas a cursos nacionais. Assim, esses países não abdicam de certificações próprias. Em face do dinamismo do setor cibernético, os países analisados têm adotado soluções nacionais em capacitação, as quais buscam atender da melhor forma às necessidades internas, por estarem mais adequadas às características do próprio país. No meio acadêmico, cursos sobre tratamento de incidentes são mais comuns no mestrado, o qual é feito normalmente em dois anos na União Europeia. Na graduação, geralmente, não existe tal curso, podendo haver disciplinas relacionadas à Segurança Computacional, complementado por cursos modulares de rápida duração, oferecidos por empresas. Para agentes públicos, a capacitação é feita em cursos promovidos pela iniciativa privada ou por órgãos do próprio governo, buscando-se atender às necessidades da administração pública. Há a formação forense e o *pentesting* em todos os países analisados, com diferenças na forma de conduzir esses cursos.

Há também a busca de ligações com empresas principalmente da área industrial. Enquanto no meio acadêmico, geralmente a metodologia tem caráter mais tradicional, nas empresas, o enfoque é mais prático, aproximando o ensino ao treinamento. Na Academia, nota-se o distanciamento entre a retórica e a prática, quando se aborda a questão do ensino por competências. Ali, na realidade, o ensino costuma ser híbrido, não ficando restrito à orientação do ensino por competências, conjugando diversas práticas educacionais, as quais costumam variar ao longo dos estudos.

Com exceção do Reino Unido, não foram constatadas parcerias para certificação, cada país conduz sua própria capacitação. Pode haver colaborações de pesquisa, sem que sejam caracterizadas parcerias. Entretanto, não há diferenças substanciais quanto a possíveis vantagens competitivas na capacitação de RH entre um país e outro, além daquelas derivadas do emprego das diferentes ferramentas, visto que os procedimentos dos CERT estão mundialmente padronizados.

Quanto às práticas laboratoriais, estas dependem do campo no qual são utilizadas. Há laboratórios em plataformas de teste e simuladores de ataques. Trabalha-se tanto no âmbito malware como no âmbito real. Geralmente usam-se redes isoladas (e não redes reais) nas simulações. Há laboratórios virtuais e laboratórios físicos. Em centros com grande número de alunos, esses laboratórios virtuais apresentam-se mais flexíveis, sendo utilizados para exercícios curtos. Quanto às ferramentas, podem ser de quatro categorias principais: de auditoria, de proteção, de detecção e de reação.

Há também a busca de ligações com empresas da área industrial. Enquanto no meio acadêmico, a metodologia tem caráter mais tradicional, nas empresas, o enfoque é mais prático, aproximando o ensino ao treinamento.

Os exercícios de simulação têm como principal problema o custo e o tempo para organização. Normalmente, os exercícios são promovidos por órgãos ou empresas que têm relação com o Ministério da Defesa. As universidades fazem as simulações no âmbito interno, geralmente no nível mestrado. No âmbito internacional, há exercícios da OTAN (destaque para os do *Cooperative Cyber Defence Centre of Excellence* – CCDCOE, na Estônia) e da União Europeia. Não obstante, há necessidade de mais testes de simulação e de treinamento.

Por fim, mas não menos importante, está a conscientização de que o desenvolvimento de competências deve ser compreendido como processo contínuo, o qual merece a orientação por um fluxo de carreira, segundo uma visão sistêmica.

NOTAS / REFERÊNCIAS

[1] ENISA. **Ejercícios CERT***: Paquete de herramientas. Heraklion, 2008b.* Disponível em*: <www.enisa.europa.eu>.* Acesso em: 22 mai. 2010.

[2] ANSSI. Agence nationale de la sécurité des systèmes d'information Paris, 2011. Disponível em: <www.ssi.gouv.fr> Acesso em: 10 jan. 2011.

[3] Empresa Thales. Modelo de proteção ativa do Estado – Ciberespaço e Infraestruturas Críticas. Catálogo. Paris, *2011.*

[4] Mind Tools. What´s coaching. Disponível em*: <www.mindtools.com>.* Acesso em: 20 jan. 2012.

*[5] Mind Tools. What´s mentoring. Disponível em***:** *<www.mindtools.com>. Acesso em 20 jan. 2012.*

[6] DFN-CERT Services GmbH. Deutscher Cert-Bund. Hamburg, 2010. Disponível em <www.cert-verbund.de/> Acesso em: 20 dez. 2010.

[7] BSI. Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2010. **Disponível em** *<www.bsi.bund.de> Acesso em: 20 dez. 2010.*

[8] BMI. Cyber Security Strategy for Germany. Berlin, 2011. Disponível em *<www.bmi.bund.de>* Acesso em: 20 mar. 2011.

[9] BRUSCHI, Danilo. Sicurezza dei Calcolatori e delle Retti. Milão, 2010. Disponível em: <http://security.dsi.unimi.it/sicurezza0809/> Acesso em: 20 jan. 2011.

[10] COMPUTER EMERGENCY RESPONSE TEAM ITALY. Campionato Nazionale di Hacking. Milão, 2010. Disponível em *<http://cert-it.dico.unimi.it/ctf>.* Acesso em: 20 jan. 2011.

[11] MINISTERIO DE DEFENSA, Ciberseguridad: Retos y Amenazas a la Seguridad Nacional. Madri, 2011.

[12] Department of the Air Force. Cyber Systems Operations: Career Field Education and Training Plan, CFETP 3D0X2, parts I and II. Washington, 2009.

[13] BELL, Gordon; GEMMEL, Jim. O Futuro da Memória: como essa transformação mudará tudo o que conhecemos. [Tradução de Ricardo Bastos Vieira]. Rio de Janeiro: *Elsevier,* 2010.

[14] ROSENBERG, Marc J. Além do e-learning: abordagens e tecnologias para a melhoria do conhecimento, do aprendizado e do desempenho organizacional. Trad. Celso Roberto Paschoal, Rio de Janeiro*:* Qualitymark, *2008.*

[15] Stanford University. The Education Program for Gifted Youth (EPGY), 2008. Disponível em*: < http://epgy.stanford.edu/> Acesso em: 23 fev. 2012.*

[16] MORIN, Edgar. A religação dos saberes: o desafio do século XXI. Trad. Flávia Nascimento. Rio de Janeiro*: Bertrand, 2001. Trad. Relier les Connaissance.*

[17] OLIVEIRA, Berenice Picanço de. Currículo. Apostila do Curso de Coordenação Pedagógica do Centro de Estudos do Pessoal. Rio de Janeiro: 2006.

[18] O tema do presente artigo foi objetivo parcial da Tese de Doutorado "Capacitação de Recursos Humanos no Exército Brasileiro para a Segurança Cibernética: desenvolvimento de competências para a atuação em uma Equipe de Tratamento de Incidentes de Rede" para a Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.