Competências para os cyber red teams no contexto militar

Article *in* RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao · March 2020

CITATIONS
0

READS
460

6 authors, including:

José Augusto De Almeida Junior
University of Brasília
1 PUBLICATION **0** CITATIONS
SEE PROFILE

William Giozza
University of Brasília
88 PUBLICATIONS **240** CITATIONS
SEE PROFILE

Robson Albuquerque
University of Brasília
100 PUBLICATIONS **420** CITATIONS
SEE PROFILE

Georges Amvame-Nze
University of Brasília
42 PUBLICATIONS **99** CITATIONS
SEE PROFILE

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 31/10/2019
Aceitação/Acceptance: 03/12/2019

Competências para os *cyber red teams* no contexto militar

José Augusto de Almeida Junior[1], William Ferreira Giozza[1], Robson de Oliveira Albuquerque[1], Georges Daniel Amvame Nze[1], Edna Dias Canedo[2], Demétrio Antônio da Silva Filho[3]

augustojaaj16@gmail.com, giozza@unb.br, robson@redes.unb.br, georges@unb.br, ednacanedo@unb.br, dasf@unb.br

[1] Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE), Departamento de Engenharia Elétrica - Universidade de Brasília, Brasília-DF, Brasil - Zipcode 70910-900

[2] Departamento de Ciências da Computação - Universidade de Brasília, Brasília-DF, Brasil - P.O. Box 4466

[3] Instituto de Física, Universidade de Brasília, Brasília-DF, Brasil, Zipcode 70919-970

Pages: 612–623

Resumo: Os *cyber red teams* podem ser utilizados pelos mais variados tipos de organizações, para que suas defesas possam ser testadas de modo completo. Entretanto, determinados nichos como no caso das organizações militares possuem certas peculiaridades que precisam ser bem compreendidas antes da implantação de um *cyber red team*. Apesar do termo *red team* ter se originado por razão das atividades militares, necessita-se de uma visão mais direcionada às suas atuações específicas nesse contexto. Neste trabalho são identificadas as competências que um *cyber red team* deve ter no contexto militar. Foram identificadas quatro competências macros, de onde se originaram mais oito competências, a partir das suas intersecções sucessivas. Com isso, pretende-se apresentar uma visão mais clara das competências necessárias para um *cyber red team* militar, de forma a aumentar a eficiência de sua montagem e ação nesse contexto.

Palavras-chave: *cyber red teams*; competências cibernéticas; guerra cibernética; habilidades cibernéticas; cibernética militar.

Skills for cyber red teams in the military context

Abstract: Cyber red teams can be used by a wide range of organizations to test their defenses in a complete way. However, certain niches as in the case of military organizations have peculiarities that must be well understood before to implement a cyber red team. Although the term red team had been originated because of military activities, it is necessary to have a more focused view of its specific actions in this context. This work identifies the competencies required for a cyber red team in the military context. Four macro competences were specified, originating by their successive intersections eight more competences. In this context, we expect to

provide a better vision of the skills needed for a military cyber red team, in order to increase the efficiency of its composition and action in this context.

***Keywords**:* cyber red teams; cyber competitions; cyber warfare; cyber skills; military cybernetics.

1. Introdução

A expressão *red team* originou-se da época da guerra fria e passou a ser conhecida pelos militares como uma maneira de pensar e simular a ação do inimigo. As técnicas de *red team* são até hoje utilizadas dentro das forças armadas em exercícios operacionais de guerra, onde essa equipe representa o oponente (Brangetto, Caliskan, & Roigas, 2015).

A utilização do *red team* no contexto da cibernética está ligada também aos exercícios militares, onde o *red team* é a equipe responsável pelo ataque e o *blue team* a equipe responsável pelas defesas. No entanto, com a expansão da cibernética e sua grande utilização como ambiente operacional de guerra (Defesa, 2014), viu-se a necessidade de manter um *red team* de modo permanente. A estes dá-se o nome de *cyber red teams* que, no contexto militar, tem o objetivo de constituir uma frente operacional de guerra no ambiente cibernético (Parks & Duggan, 2011).

Os *cyber red teams* não se restringem apenas ao meio militar, sendo também fornecidos por empresas de segurança, como um serviço, para avaliar de modo completo as defesas de seus clientes. Dessa forma, um *cyber red team* pode ser percebido como uma metodologia de teste de penetração (BlackBerry, 2019). No entanto, é importante ressaltar que estas são atividades distintas, já que o *cyber red team* atende a um escopo muito mais amplo, profundo e especializado do que o teste de penetração ou *pentest*, como também é conhecido (Mansfield-Devine, 2018).

O ambiente cibernético, em um contexto militar, permeia todos domínios de guerra (Defesa, 2014). Grandes impactos cinéticos podem ocorrer em virtude de ações no meio cibernético, ainda mais quando leva-se em conta as infraestruturas críticas que, se afetadas, trazem enormes prejuízos a toda uma nação. Por isso, a implantação de *cyber red teams* tem sido recorrente em diversos países e até a OTAN (Organização do Tratado do Atlântico Norte) possui uma equipe preparada para ações nesse contexto (Brangetto et al., 2015).

A preocupação com o ambiente cibernético torna-se cada vez mais intensa no meio militar, pois, a partir dos princípios da *cyber warfare* é possível realizar ações com grandes efeitos cinéticos danosos. Esses danos podem ser altamente prejudiciais como, por exemplo, a abertura indesejada das comportas de uma barragem ou o desligamento de uma subestação elétrica, entre outros (Parks & Duggan, 2011).

Este trabalho tem por objetivo identificar e expor de forma clara e objetiva quais as competências inerentes a um *cyber red team* no contexto militar. Espera-se que a partir da definição dessas competências, o setor tático possa selecionar ou desenvolver as metodologias para recrutamento de pessoal e prever os treinamentos necessários antes do emprego operacional do *cyber red team*. O conhecimento prévio dessas competências permite uma melhor estruturação da equipe, de forma que o setor operacional possa cumprir eficientemente todos os objetivos estratégicos e táticos exigidos para o meio militar.

Este trabalho está organizado conforme a seguir. A Seção 2 apresenta alguns trabalhos correlatos, abordando a conceituação, estruturação e definição de competências para a formação de *cyber red teams* num contexto geral. Na Seção 3, discute-se as diferenças do *cyber red team* para com a metodologia de *pentest*. Na Seção 4 é apresentada uma proposta de estruturação e definição de competências para um *cyber red team* atuar no contexto militar. Por fim, a Seção 5 apresenta as conclusões do trabalho.

2. Trabalhos correlatos

Diversas obras já trabalharam de alguma forma o tema red team. No entanto, essas obras não tem o seu estudo direcionado para identificação das habilidades necessárias a um cyber red team, de forma que possuem maior ênfase nos estudos das técnicas e metodologias de emprego. Da mesma forma, poucas obras trabalham de forma específica a identificação dessas mesmas habilidades no contexto militar. Isso abre uma lacuna de conhecimento e faz com que o emprego de técnicas e metodologias não aconteçam de forma a aproveitar a maior eficiência possível. A Tabela 1 exibe propostas de algumas obras em relação às habilidades necessárias aos cyber red teams.

A estrutura de um cyber red team com objetivos militares já é implementada pela OTAN. Em (Dandurand, 2011) foi definido um modelo de estrutura organizacional de um cyber red team no contexto militar da OTAN, um modelo flexível composto na parte administrativa pelo chefe do cyber red team, um adjunto e um chefe específico para o suporte. A parte técnica do cyber red team é composta por um líder técnico para cada objetivo, acompanhado pelos demais especialistas, já a do suporte é composta por desenvolvedores de infraestrutura e de exploits e administradores de sistemas operacionais.

Em (Sharma, 2018), considera-se que um *cyber red team* utiliza de meios como engenharia social, segurança física e *pentest* para alcançar seus objetivos. Porém, dentro das forças armadas, algumas atividades fogem desse escopo, como por exemplo, as questões de inteligência.

Obra	**Proposta de habilidades**
Dandurand, L. (2011, June) - Rationale and blueprint for a cyber red team within nato.	Segurança cibernética, sistemas e redes, protocolos, redes sem fio, comunicações militares, criatividade, buffer overflow, arquitetura de computadores, vulnerabilidades, suporte, segurança física e gestão de pessoal.
Sharma. (2018) - Hands-on red team tactics.	Engenharia social, segurança física e pentest.
Dalziel, H. (2015) - Next generation red teaming.	Eletrônica, social, física e outras.
Brangetto, P., Caliskan, E., & Roigas, H. (2015) - Cyber red teaming-organisational, technical and legal implications in a military context.	Vulnerabilidades nos sistemas ou em operador humano.
Eom, J., Kim, N., Kim, S., & Chung, T. (2012, June) - Cyber military strategy for cyberspace superiority in cyber warfare.	Estratégias, táticas, infraestrutura e cibernética, outros meios que afetem a cibernética.

Tabela 1 – Propostas de habilidades para cyber red teams.

Em (Dalziel, 2015), define-se quatro competências bases para um *cyber red team*, sendo elas, eletrônica, social, física e outras. Apesar de conter bons parâmetros para definir competências, o escopo ficou extremamente grande, dificultando seu enquadramento dentro do contexto das forças armadas.

Em (Brangetto *et al*., 2015), considera-se que um *cyber red team*, no contexto militar, precisa encontrar e explorar vulnerabilidades nos sistemas ou em operador humano, e que para isso precisa de habilidades específicas que vão além dos conhecimentos de cibernética.

Em (Eom *et al*., 2012), considera-se que a superioridade em uma *cyber warfare*, depende de quão bem o *cyber red team* atende às competências necessárias neste meio, exigindo, estratégias, táticas, infraestrutura e componentes que dominem de modo completo as atividades cibernéticas ou que possam ser usadas para afetá-la.

Em (Oakley, 2018), observa-se que a importância dos *cyber red teams* não está ligada apenas à razão de se ter uma frente operacional para guerra cibernética, mas também por ser uma maneira de aumentar a eficiência das defesas de uma forma completa, ampla e contínua, por meio do emprego da segurança ofensiva. A segurança ofensiva visa identificar e aproveitar as vulnerabilidades antes do agente mal intencionado. Isso pode ser feito por meio de *hackers* éticos, que simulam ataques contra a organização. Esse conceito claramente pode ser atendido a partir de uma estruturação correta de um *cyber red team* (Ragan, 2019).

Dos trabalhos relacionados estudados, observa-se que não há uma convergência clara e objetiva sobre a estrutura e competências de um *cyber red team* para atuação no contexto militar. Nesse contexto, este trabalho pretende apresentar uma visão mais clara das competências necessárias para um *cyber red team* militar, de forma a aumentar a eficiência de sua montagem e ação.

3. *Cyber Red Team versus Pentest*

A possibilidade de grandes prejuízos causados por meio do domínio cibernético obriga as forças armadas a implementarem projetos de defesa complexos, mas sempre há dúvidas acerca da eficiência, mediante a ataques reais. Para tentar validar seus sistemas quanto à segurança, as organizações geralmente utilizam o *pentest*, no entanto, apenas isso não é capaz de avaliar todas as suas defesas. Por exemplo, o *pentest* não é capaz de avaliar deficiências humanas, tecnológicas e de processos em conjunto. Por outro lado, como os *cyber red teams* costumam ser fornecidos por empresas como um serviço (Mansfield-Devine, 2018) acabam por ser confundidos com uma metodologia de *pentest*, até mesmo pela própria organização prestadora do serviço.

	Pentest	**Cyber red team**
Metodologias	Utiliza de forma sistemática metodologias como: PTES, OSSTMM, ISSAF, OWASP, entre outras.	Flexível. Não são obrigatórias, porém podem ser utilizadas por completo, em parte ou serem adaptadas, conforme as necessidades para o cumprimento dos objetivos.
Escopo	Restritivo, geralmente anunciado, sistema ou infraestrutura alvo.	Toda a organização, geralmente não anunciado, testar blue teams, políticas, ferramentas e habilidades.

	Pentest	Cyber red team
Técnicas	Caixa preta, cinza ou branca.	Simulação, sondagens de vulnerabilidade, análises alternativas.
Objetivo	Encontrar vulnerabilidades.	Realizar explorações, em prol de um objetivo.
Emprego	Em razão da defesa cibernética.	Em equipes de segurança cibernética, inteligência e no contexto militar.

Tabela 2 – Diferenças entre *pentest* e *cyber red team*.

O *pentest* visa encontrar o maior número de vulnerabilidades em um sistema e para isso segue à risca alguma metodologia para simular ataques, de forma a avaliar o quão vulnerável é um sistema (Kim, 2018). Já o *cyber red team* é guiado por objetivos e seu alvo é sempre uma organização. O *cyber red team* deve ser composto de especialistas que sejam capazes de compreender os interesses, intenções e capacidades do alvo, a fim alcançar os objetivos (Zenko, 2015; Dandurand, 2011). A missão do *cyber red team* é emular as táticas, técnicas e procedimentos (TTPs) dos oponentes, com objetivo de fornecer os fatos concretos, para que a postura de segurança de uma organização seja aumentada (Kim, 2018). No contexto militar, leva-se em conta também, sua utilização para manter a superioridade mediante uma guerra cibernética (Eom *et al.*, 2012).

A Tabela 2 resume as principais características diferenciando o *pentest* do *cyber red team*.

4. Competências de um *cyber red team* no contexto militar

De acordo com o estudo realizado, entende-se que um *cyber red team* depende de determinadas características para sua formação. Esses aspectos são detalhados a seguir.

4.1. Competências macro

De forma macro, pode-se identificar que no contexto militar, um *cyber red team* deve possuir 4 competências, conforme ilustrado na Figura 1. São eles: a engenharia social (*Social engineering*) para o conhecimento humano; a segurança física (*Physical security*) para ativos cinéticos; as ações cibernéticas (*Cyber action*) no contexto das comunicações;, e o suporte (*Support*) que representa as atividades de apoio, como administração, informática e conhecimentos altamente especializados em áreas não comuns.

As ações cibernéticas *(Cyber action)* são atividades como reconhecimento, ataque e manutenção de acessos no meio cibernético. Em um mundo onde até pequenos dispositivos estão conectados, como na Internet das coisas (Ferreira & de Sousa Junior, 2017), essas ações exigem grandes conhecimentos das tecnologias de comunicação, incluindo as ações com softwares, redes cabeadas e sem fio, tecnologias móveis, entre outras (Dalziel, 2015). As ações de reconhecimento são necessárias pela parte de inteligência e, também, exigem conhecimentos especializados. Para um *cyber red team*, a competência cibernética é o principal fator para superioridade das forças armadas em meio à guerra cibernética (Eom *et al.*, 2012).

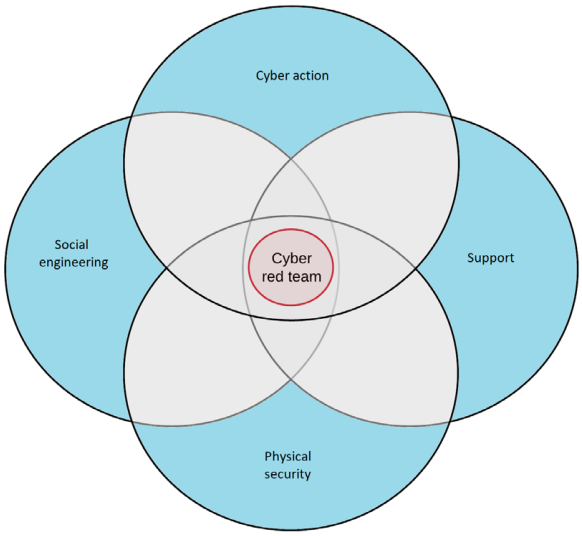

Figura 1 – As competências macro de um *cyber red team*.

De um modo geral, confia-se muito no fator humano, porém as pessoas possuem características emocionais que permitem a extração de informações valiosas para um ataque cibernético (Kim, 2018). Esses aspectos são explorados por meio do emprego da engenharia social *(Social engineering)*. Um *cyber red team*, por sua vez, deve ser capaz de explorar o fator humano das mais variadas formas. A engenharia social é uma competência importante, por propiciar grandes atalhos para o cumprimento dos objetivos. Ela dispensa muitas das vezes, até mesmo as habilidades técnicas, no entanto, quando integradas, propiciam grandes vantagens cibernéticas. Essas vantagens, geralmente, se dão por meio de ataques de *phishing*, via telefone, ou até mesmo, ao catalogar informações em redes sociais (Dalziel, 2015).

Além do domínio cibernético, a segurança física *(Physical security)* também pode ser melhorada por meio de técnicas empregadas por *cyber red teams* (Zenko, 2015). Deve-se levar em consideração que a segurança física é composta por vários ativos como cartões de controle de acesso, câmeras, proteções físicas para transmissão de dados, fechaduras, etc. Para todos esses ativos, existem formas de exploração (Kim, 2018). Com isso, sempre existirá a possibilidade do deslocamento físico de integrantes do *cyber red team*, o que dependerá da disponibilidade de uma gama de profissionais especializados conforme o objetivo. Principalmente nas forças armadas, que com esse conceito, podem obter vantagens cibernéticas em ações cinéticas.

O suporte *(Support)* é responsável pelo desenvolvimento de ferramentas, pela manutenção dos sistemas, administração das redes e criação das infraestruturas lógicas demandadas pelos times de ataque (Dandurand, 2011). No entanto, as atividades de suporte vão além das atividades de informática. As atividades como administração são altamente necessárias ao funcionamento do *cyber red team* e isso também faz parte do suporte. Existem também diversos conhecimentos específicos que, via de regra, não são

utilizados por um *cyber red team*, mas em situações peculiares são indispensáveis. Todas essas informações são trabalhadas dentro do campo de suporte, a mais heterogênea das competências necessárias ao *cyber red team*.

4.2. Competências por Intersecções de 1º grau

Observa-se que apesar do conhecimento sobre as quatro competências macros agora ser conhecido para o ambiente militar, apenas isso não é o suficiente para se ter uma visão clara e objetiva das competências necessárias para montagem de um *cyber red team*. Por exemplo, a partir de intersecções das quatro competências macros, é possível identificar mais quatro outras competências necessárias dentro das forças armadas, conforme ilustrado na Figura 2.

A união entre as competências de ações cibernéticas e suporte, origina a competência de defesa ativa e passiva *(Active and passive defense)*. A defesa ativa é uma ação defensiva para destruir, anular ou reduzir a eficácia das ameaças cibernéticas contra os ativos de uma organização (Denning, 2014). Já a defesa passiva são todas as medidas, com exceção da defesa ativa, para minimizar a eficácia das ameaças cibernéticas. Para acontecer a defesa ativa, além das competências necessárias de cibernética, precisa-se do suporte para implementar todas as observações nos ativos. Para um *cyber red team* é de fundamental importância que exista competências que permitam o entendimento do que acontece em relação a defesa do oponente, pois a defesa cibernética faz parte das barreiras a serem vencidas.

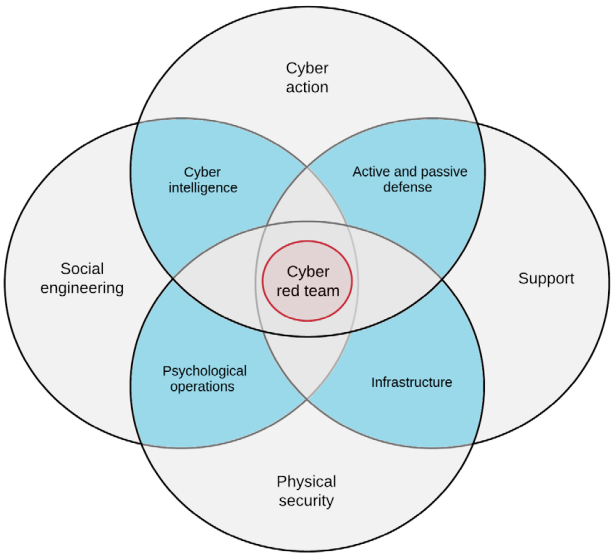

Figura 2 – Competências por intersecções de 1º grau para um *cyber red team*.

Da intersecção entre as ações cibernéticas e a engenharia social, surge uma competência altamente importante para as forças armadas, que é a inteligência cibernética *(Cyber intelligence)*. Com o objetivo principal de obter informações, a inteligência também se

faz necessária dentro do contexto da cibernética, com mesma função. A competência em inteligência cibernética é um pré-requisito para manter a superioridade no espaço cibernético (Eom *et al.*, 2012). Para que a captura de informações seja possível é necessário o conhecimento humano e cibernético, de forma que as informações possam ser adquiridas também de pessoas que usam este meio. Cabe ressaltar também que, a inteligência cibernética no contexto militar, não leva em consideração todas as peculiaridades de um serviço de Estado, sendo apenas para capturar informações para a própria força armada.

Desde a Segunda Guerra Mundial, os manuais militares norte-americanos e da OTAN definem "guerra psicológica" ou "operações psicológicas" como táticas variadas como propaganda, operações secretas, guerrilha e, mais recentemente, diplomacia pública (Simpson, 2015). Com isso, tem-se mais uma intersecção, que deve ser competência de um *cyber red team*, sendo a união das competências macros de engenharia social, pelo conhecimento humano, e segurança física, pela necessidade de implante em ambiente de combate cinético. As operações psicológicas *(Psychological operations)* são uma realidade e vem sendo aplicada em ambiente militar desde muito tempo, constituindo-se altamente importante como competência.

Da intersecção da segurança física com a área de suporte surge a infraestrutura *(Infrastructure)*, uma área essencial para a cibernética. Por exemplo, o setor de infraestrutura de tecnologia da informação, necessário para o emprego dos *cyber red teams*, é composto por diversas áreas de conhecimentos como redes, servidores, banco de dados, manutenção de ativos, sistemas operacionais e hardwares (Monteiro & Freitas, 2015). Com essa afirmação, torna-se claro que infraestrutura está dentro das competências de segurança física e suporte.

4.3.Competências por intersecções de 2º grau: as mais próximas do *cyber red team*

Da análise feita em torno das competências até esse momento, chega-se à existência de quatro competências macros e mais quatro, originadas de intersecções. Ao total tem-se oito competências identificadas para um melhor mapeamento de um *cyber red team* no contexto militar. No entanto, o que foi listado até agora, ainda não demonstra claramente todas as competências necessárias. Pode-se por exemplo detalhar mais um pouco as intersecções, de forma a chegar, em competências mais próximas ao *cyber red team*, conforme ilustrado na Figura 3.

Conforme dito anteriormente, diferentemente do processo de teste de penetração *(pentest)*, um *cyber red team* não visa encontrar o maior número de vulnerabilidades possíveis e sim, conquistar o objetivo imposto. Porém, não se tem um *cyber red team* sem os profissionais de *pentest*, os quais são partes integrantes. Metodologias de *pentest*, como por exemplo o PTES (*Penetration Testing Execution Standard*) preveem fases de reconhecimento passivo e ativo, exploração de falhas, preservação do acesso e geração de relatórios (PTES, 2009). Os *pentesters* devem utilizar as mais variadas técnicas, inclusive aprender com crimes digitais, por exemplo com as fraudes bancárias, onde existem formas criativas e inovadoras para realizar ataques (Rocha & de Sousa Junior, 2010). Essas atividades, devem ser incorporadas dentro do *cyber red team*, sendo claramente uma união das competências de inteligência cibernética, pelo fato de possuir fases de reconhecimento e

defesa ativa e passiva, por ter que interagir com o meio. Considera-se também, dentro de um *pentest,* as competências macros, engenharia social, ações cibernéticas e o suporte.

Para que se possa moldar o ambiente de informação, de acordo com os interesses, é preciso o desenvolvimento de operações de informação *(Information operations)*, inclusive em redes. Deve- se potencializar "pontos fortes" na exploração e reduzir o máximo possível os impactos dos ataques que pretendam explorar os "pontos fracos" (Nunes, 2012). Então, com base no exposto, existe uma competência que surge da intersecção da inteligência cibernética com as operações psicológicas. Isso vem da necessidade do *cyber red team* obter informações, independentemente da forma com que é feita, se é fisicamente mediante persuasões ou apenas de forma cibernética.

Ao levar em conta a possibilidade de um confronto, um *cyber red team*, mesmo sendo ele focado em cibernética, deve estar preparado para obter informações provenientes de combate físico. Para isso, é necessário que membros do *cyber red team* sejam capazes de permear esse meio. Então, origina-se uma intersecção menos provável para o *cyber red team*, porém, importante. A junção das operações psicológicas com a infraestrutura, com grande influência da competência macro de segurança física, gera as operações especiais *(Special operations)*. Percebe-se que à medida em que as operações de influência vão se afastando do campo das operações psicológicas e aproximando-se de ações paramilitares e guerrilha, as operações especiais entram em ação com as tropas de elite (Cepik, 2002). Com isso, torna-se necessário o mapeamento das operações especiais como competência, mesmo que sua utilização seja de baixa probabilidade, sendo usada, apenas nos níveis avançados de combate ou de exercício.

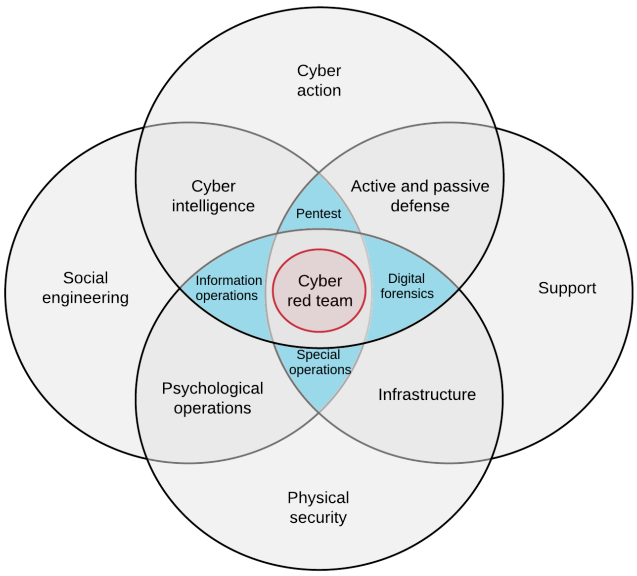

Figura 3 – Diagrama de competências por intersecções de 2º grau para um *cyber red team* no contexto militar.

Como última intersecção definida antes de se chegar ao *cyber red team*, está a competência que dispensa a interação direta de acontecer com o ser humano, mas é essencial. Com grande influência das competências macros e sendo a intersecção da infraestrutura com as atividades de defesa ativa e passiva, está a perícia digital *(Digital forensics)*. Para que uma perícia aconteça deve haver segurança no armazenamento dos dados, conhecimentos de cibernética para que a coleta seja feita e um grande aparato de suporte, com máquinas de poder computacional considerável para quebras de senhas e processamento de *hashs* (ABNT, 2013). Para um *cyber red team* é de fundamental importância a competência em perícia digital para permitir a extração de dados de meios computacionais, inclusive em dispositivos móveis (Simao, Sicoli, de Melo, de Deus, & de Sousa Junior, 2011), e também para que os seus componentes possam aplicar a anti-perícia. Com isso o trabalho feito pelo *cyber red team*, torna-se de difícil rastreamento.

5. Conclusão

No contexto militar existem diversas peculiaridades, que são incomuns aos outros tipos de organizações. Mediante isso, torna-se complexa a montagem de um *cyber red team* nesse contexto. É preciso abranger uma vasta gama de competências não exigidas em outro tipo de organização.

A partir do estudo feito, chegou-se a conclusão que existem quatro competências macro, as quais devem ser atendidas por um *cyber red team*. Com base nessas competências, foram encontradas outras quatro, originadas por meio de suas intersecções em conjunto com as peculiaridades de um ambiente operacional militar. Essas, por sua vez, já demonstram características inerentes apenas ao meio militar. No entanto, ainda não trazem o refino necessário para que a efetividade de um *cyber red team* militar seja aumentada.

Como último detalhamento, foram definidas mais quatro competências, todas elas identificadas a partir de intersecções sucessivas com todas as anteriores. Essas, porém, são as mais próximas das ações de um c*yber red team* militar e finalizam o estudo de identificação das competências inerentes a este contexto. Com base no estudo feito neste trabalho, é proposto um diagrama de competências que leva em consideração as peculiaridades no contexto militar e apresenta de forma sucinta e visual todas as competências necessárias, para formulação de um *cyber red team* em nesse contexto.

Agradecimentos - Os autores agradecem o apoio das Agências brasileiras de pesquisa, desenvolvimento e inovação CNPq (Projeto INCT em Segurança Cibernética 465741/2014-2), CAPES (Projeto FORTE 23038.007604/2014-69 e PROBRAL 88887.144009/2017-00) e Fundação de Apoio à Pesquisa do Distrito Federal FAPDF (Projetos UIoT 0193.001366/2016 e SSDDC 0193.001365/2016) e do CCA-BR (Centro de Computação da Aeronáutica de Brasília) juntamente ao ComDeCiber (Comando de Defesa Cibernética), bem como do Gabinete de Segurança Institucional da Presidência da República (TED 002/2017) e do Laboratório LATITUDE/UnB (Projeto SDN 23106.099441/2016-43).

Referências

ABNT - Associação Brasileira de Normas Técnicas (2013, Dec.). Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital (Tech. Rep.). (ABNT NBR ISO/IEC 27037:2013)

BlackBerry, C. (2019). *Report: Thin Red Line - Penetration Testing Practices Examined*. Irvine, CA, USA: ThreatVector. URL: https://threatvector.cylance.com/en_us/home/report-thin-red-line-penetration-testing-practices-examined.html.

Brangetto, P., Caliskan, E., & Roigas, H. (2015). Cyber red teaming-organisational, technical and legal implications in a military context. NATO CCD CoE . (Filtri tee 12, Tallinn 10132, Estonia. URL:https://ccdcoe.org/uploads/ 2018/10/Cyber_Red_Team.pdf)

Cepik, M. (2002). Inteligência e políticas públicas: dinâmicas operacionais e condições de legitimação. Security and Defense Studies Review, 2 (2), 246–267.(URL:https://www2.mppa.mp.br/sistemas/gcsubsites/upload/60/Intelig%C3%83%C2%AAncia%20e%20Pol%C3%83%C2%ADticas%20P%C3%83%C2%BAblicas(1).pdf ISSN 1533-2535)

Dalziel, H. (2015). Next generation red teaming (first ed.). 225 Wyman Street, Waltham, MA 02451, USA: Syngress. (ISBN: 978-0-12-804171-0)

Dandurand, L. (2011, June). Rationale and blueprint for a cyber red team within nato: An essential component of the alliance's cyber forces. In 2011 3rd international conference on cyber conflict (p. 1-16). (Tallinn, Estonia. ISSN 2325-5366)

Defesa, M. (2014, nov). Doutrina militar da defesa cibernética. D.O.U. n o 224 . (Portaria normativa nº 3.010/MD. URL: https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf)

Denning, D. E. (2014). Framework and principles for active cyber defense. Computers Security, 40, 108 - 113. Retrieved from http://www. sciencedirect.com/science/article/pii/S0167404813001661 (ISSN: 0167-4048) doi: https://doi.org/10.1016/j.cose.2013.11.004

Eom, J., Kim, N., Kim, S., & Chung, T. (2012, June). Cyber military strategy for cyberspace superiority in cyber warfare. In Proceedings title: 2012 international conference on cyber security, cyber warfare and digital forensic (cybersec) (p. 295-299). (Kuala Lumpur, Malaysia. DOI 10.1109/CyberSec.2012.6246114) doi: 10.1109/CyberSec.2012.6246114

Ferreira, H. G. C., & de Sousa Junior, R. T. (2017, Mar 01). Security analysis of a proposed internet of things middleware.Cluster Computing,20(1), 651–660. Retrieved from https://doi.org/10.1007/s10586-017-0729-3doi:10.1007 /s10586-017-0729-3

Kim, P. (2018). The hacker playbook 3: Practical guide to penetration testing. Secure Planet LLC. (ISBN-13 978-1980901754)

Mansfield-Devine, S. (2018). The best form of defence – the benefits of red teaming. Computer Fraud Security, 2018 (10), 8 - 12. Retrieved from http://www.sciencedirect.com/science/article/pii/S1361372318300976 (ISSN: 1361-3723) doi: https://doi.org/10.1016/S1361-3723(18)30097-6

Monteiro, G. A. P., & Freitas, A. L. P. (2015). Análise importância-desempenho aplicada à avaliação da qualidade em serviços de infraestrutura de ti. Simpósio de Engenharia de Produção-SIMPEP, 22 , 15. (Av. Eng. Luiz Edmundo Carrijo Coube, 14-01, Bauru - SP. ISSN: 1809-7189)

Nunes, P. (2012). A definição de uma estratégia nacional de cibersegurança. Nação e defesa, 133, 113–publicacoes/nacaodefesa/textointegral/NeD133.pdf. ISSN: 0870-757X)

Oakley, J. (2018). Improving offensive cyber security assessments using varied and novel initialization perspectives. In Proceedings of the acmse 2018 conference (pp. 3:1–3:9). New York, NY, USA: ACM. Retrieved from http://doi. acm.org/10.1145/3190645.3190673 (ISBN 978-1-4503-5696-1) doi: 10.1145/3190645.3190673

Parks, R. C., & Duggan, D. P. (2011, Sep.). Principles of cyberwarfare. IEEE Security Privacy, 9 (5), 30-35. (ISSN: 1540-7993) doi: 10.1109/MSP.2011.138

PTES. (2009). Penetration testing execution standard. (URL: http://www.pentest-standard.org/index.php/ PTES_Technical_Guidelines. Access in 01 jun 2019 19:36)

Rocha, B., & de Sousa Junior, R. (2010, 10). Identifying bank frauds using crisp-dm and decision trees. International Journal of Computer Science Information Technology,2.doi: 10.5121/ijcsit.2010.2512

Ragan, R. (2019). *Red teaming: Why a forward offense is the best defense.* Skokie, IL, USA: (IN) SECURE Magazine. URL: https://www.helpnetsecurity.com/2019/08/19/red-teaming/

Sharma. (2018). Hands-on red team tactics: A practical guide to mastering red team operations. Livery Place, 35 Livery Street, Birmingham B3 2PB, UK.: Packt Publishing Limited. (ISBN 978-1-78899-523-8)

Simao, A. M. d. L., Sicoli, F. C., de Melo, L. P., de Deus, F. E., & de Sousa Junior, R. T.(2011). Acquisition of digital evidence in android smartphones. In 9th australian digital forensics conference (p. 116)

Simpson, C. (2015). Science of coercion: Communication research & psychological warfare (Vol. 13). 180 Maiden Lane, Suite 8A New York, NY 10038: Open Road Media. (ISBN-13 978-0195102925)

Zenko, M. (2015). Red team: How to succeed by thinking like the enemy. 250 West 57th Street, New York, NY 10107: Basic Books. (ISBN 978-0-465-07395-5)