ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM CAIO TAVARES DA CUNHA

PROPOSTA DE MEDIDAS PARA IDENTIFICAÇÃO DE AMEAÇAS PERSISTENTES AVANÇADAS:

UMA ABORDAGEM PARA O DESTACAMENTO CONJUNTO DE DEFESA CIBERNÉTICA A LUZ DO CYBER KILL CHAIN.

Rio de Janeiro
2018

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM CAIO TAVARES DA CUNHA

PROPOSTA DE MEDIDAS PARA IDENTIFICAÇÃO DE AMEAÇAS PERSISTENTES AVANÇADAS:
UMA ABORDAGEM PARA O DESTACAMENTO CONJUNTO DE DEFESA CIBERNÉTICA A LUZ DO CYBER KILL CHAIN.

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Segurança dos Sistemas.

Rio de Janeiro
2018

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEx - DESMil
ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS
(EsAO/1919)

ASSESSORIA DE PESQUISA E DOUTRINA / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: **Cap Com CAIO TAVARES DA CUNHA**

Título: **PROPOSTA DE MEDIDAS PARA IDENTIFICAÇÃO DE AMEAÇAS PERSISTENTES AVANÇADAS:** UMA ABORDAGEM PARA O DESTACAMENTO CONJUNTO DE DEFESA CIBERNÉTICA A LUZ DO CYBER KILL CHAIN.

Trabalho Acadêmico, apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da especialização em Ciências Militares, com ênfase em Segurança dos Sistemas, pós-graduação universitária lato sensu.

APROVADO EM _____/_____/_____ *CONCEITO:* _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ **DARDANO DO NASCIMENTO MOTA - Maj** Cmt Curso e Presidente da Comissão	
_____ **RAPHAEL ALVES DA SILVA - Cap** 1º Membro	
_____ **FLÁVIO CORSI - Cap** 2º Membro e Orientador	

_____
CAIO TAVARES DA CUNHA – Cap
Aluno

PROPOSTA DE MEDIDAS PARA IDENTIFICAÇÃO DE AMEAÇAS PERSISTENTES AVANÇADAS:
UMA ABORDAGEM PARA O DESTACAMENTO CONJUNTO DE DEFESA CIBERNÉTICA A LUZ DO CYBER KILL CHAIN

Caio Tavares da Cunha[*]
Flávio Corsi[**]

RESUMO
No presente trabalho, foram elencados subsídios que justificassem o emprego do *Cyber Kill Chain (CKC)* em favor da Proteção Cibernética realizada pelo Dst Cj Def Ciber. A finalidade foi realizar o levantamento das características necessárias e propor um modelo de emprego deste *framework* que possa ser utilizado para identificação de ameaças persistentes avançadas *(APT)*. Para tanto, esse artigo foi desenvolvido, de outubro de 2017 a agosto de 2018, por meio de uma pesquisa bibliográfica e descritiva, utilizando-se, também, questionários e grupo focal como meios de coleta de dados. Além do material de fontes abertas, o relatório de pesquisa conta com a experiência pessoal vivida pelo autor como integrante de Dst Cj Def Ciber e as informações colhidas durante o seminário internacional de defesa cibernética 2018. Ao longo da dissertação foi possível determinar que os benefícios da aplicação deste modelo podem estender-se a todas as atividades de guerra cibernética (G Ciber). Como consequência, na visão dos analistas, os conceitos do *CKC* também podem ser empregados em favor do trabalho de planejamento e emprego do Dst Cj Def Ciber**.** Em seguida foi evidenciado que o método em estudo poderia agregar, principalmente, a tarefa Consciência Situacional, contribuindo assim para identificação de ataques. Por fim foi verificado a capacidade deste modelo de influenciar decisivamente a produção de manuais técnicos de G Ciber. Na conclusão, as ideias expressas ao longo do trabalho são ratificadas por meio da apresentação de uma proposta de medida que favorece a identificação de *APT* sob a ótica do *CKC*.

Palavras-chave: Guerra cibernética. Proteção cibernética. Ameaças Persistentes Avançadas. *Cyber Kill Chain*. Consciência situacional.

ABSTRACT
In this paper, subsidies that justified the use of Cyber Kill Chain (CKC), in favor of Cyber Protection by Joint Cyber-Defense Detachment, were listed. The purpose was to carry out the survey of characteristics needed and propose an employment model of this framework that can be used to Advanced Persistent Threat (APT) identification. Therefore, this essay was developed, from October 2017 to August 2018, by bibliographic and descriptive research. As means of data collection, questionnaires and Focus Group were used as well. In addition to open source material, the research report relies on the author's personal experience as a member of Cyber Defense Joint Detachment and the information gathered during the 2018 International Cyber-Defense Summit & Expo, hosted in Brazil. Throughout the text it was possible to set the benefits of this model to all Cyberwarefare activities. As a consequence, in the view of analysts, CKC concepts can also be used to improve the planning and employment work of Cyber Defense Joint Detachment. Foremost, it was highlighted that the method under study could add, mainly, the Situational Consciousness task, thus contributing to the identification of attacks. Finally, the ability of this model to influence as decisively form the production of Cyberwarefare technical manuals was verified. In conclusion, the ideas expressed throughout the paper are ratified by presenting a proposal for a measure that improve the APT identification from the CKC perspective.

Keywords: Cyberwarfare, Cyber protection, Advanced Persistent Threat. Cyber Kill Chain. Situational awareness.

---

[*] Capitão da Arma de Comunicações. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2007. Pós-Graduado em Guerra Eletrônica pelo Centro de Instrução de Guerra Eletrônica em 2010.

[**] Capitão da Arma de Comunicações. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2005. Pós-Graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) em 2014.

À minha amada esposa, fonte incondicional de apoio, exemplo de determinação e fé.

1 INTRODUÇÃO

No auge da guerra fria, em junho de 1982, um satélite americano detectou uma grande explosão na Sibéria. O que parecia ser um teste nuclear foi confirmado, posteriormente, como uma explosão em um gasoduto soviético. O motivo foi o mau funcionamento no sistema de controle o qual utilizava um software roubado por espiões soviéticos de uma empresa canadense. Segundo Thomas Reed, ex-secretário da força aérea americana, a CIA havia adulterado o software para que, após algum tempo de utilização, o gasoduto entrasse em colapso. O resultado, segundo ele, "foi a mais monumental explosão não-nuclear já vista do espaço".[1]

Esta foi uma das primeiras manifestações do poder de uma “bomba lógica”. Nas três décadas seguintes ocorreu um exponencial crescimento no emprego de sistemas informacionais vitais ligados em rede tornando evidente que, num contexto de hostilidades e/ou beligerância entre dois Estados, a exploração das redes de computadores do país oponente constitui uma eficiente maneira de obter vantagens sobre o mesmo.

Atualmente já se tem exemplos de ataques cibernéticos massivos a países como a Estônia que em 2007 sofreu por sete dias com o comprometimento de infraestruturas críticas como bancos, ministérios, jornais e o parlamento.[2]

Também é possível destacar os modernos ataques cibernéticos de escala global realizados por meio do *ransomware Wannacry*.[3]

No contexto militar, a exploração dos sistemas de informação computadorizados estabelecidos pelas forças inimigas pode levar a uma superioridade no campo de batalha.[4] Como consequência, a Guerra Cibernética passou a compor o rol de capacidades militares.[5]

---

[1] THE ECONOMIST. **War in the fifth domain**. 2010. Disponível em < http://www.economist.com/node/16478792 >, acessado em: 08 de novembro de 2017.

[2] CAVELTY, Myrian Dunn. **Critical information infraestructure:** vulnerabilities, threats and responses. 2007.

[3] PORTAL G1. **Ciberataques em Larga Escala Atingem Empresas no Mundo e Afetam Brasil.** Disponível em: < https://www.g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-são-alvo-cyber-ataques-em-larga-escala.ghtml >, acessado em: 01 de maio de 2018.

[4] CARVALHAIS, André Melo Dutra. **Introdução à Guerra Cibernética:** a necessidade de um despertar brasileiro para o assunto. São José dos Campos, SP. 2007. Disponível em: < http://www.sige.ita.br/anais/IXSIGE/Artigos/GE_39.pdf >, acessado em 16 de outubro de 2017.

[5] BRASIL. Exército. Estado-Maior. **EB20-C-07.001: Catálogo de Capacidades do Exército**. Brasília-DF, 2015.

1.1 PROBLEMA

O trabalho desenvolvido pelo Destacamento Conjunto de Defesa Cibernética (Dst Cj Def Ciber) durante os Jogos Olímpicos e Paralímpicos Rio 2016 (JOP Rio 2016) foi planejado no Centro de Defesa Cibernética (CDCiber) e envolveu diversas etapas realizadas entre junho de 2015 até a ocasião do encerramento da operação em 18 de setembro de 2016.[6]

Dentre as ameaças cibernéticas atuais, as mais preocupantes são as *advanced persistente threat* (*APT*) em virtude de sua difícil identificação e grande potencial de dano.[7]

Visto o *Cyber Kill Chain* (*CKC*) ser um modelo, voltado para detecção de *APT*, amplamente experimentado[8]; seria possível o CDCiber utilizá-lo como fonte para aprimorar as medidas de proteção cibernética, por parte do Dst Cj Def Ciber, buscando identificar ameaças persistentes avançadas?

1.2 OBJETIVOS

Como forma de imprimir maior robustez ao processo de organização e planejamento do emprego da proteção cibernética, o escopo deste trabalho busca analisar o modelo *Cyber Kill Chain* juntamente com as soluções apresentadas pelo universo de militares consultados, os quais trabalharam em prol do CDCiber por meio do Dst Cj Def Ciber para os JOP Rio 2016.

Para viabilizar a consecução do objetivo geral de estudo, foram formulados os objetivos específicos, abaixo relacionados, que permitiram o encadeamento lógico do raciocínio descritivo apresentado neste estudo:

a) Definir os conceitos pertinentes;

b) Determinar a importância da identificação de *APT* no aprimoramento da eficiência na Proteção Cibernética;

c) Identificar benefícios e desafios da implementação do *CKC*;

d) Apresentar a capacidade de influência do *CKC* na produção de doutrina militar;

---

[6] DA CUNHA, Caio Tavares. **Relatório de Missão Jogos Olímpicos e Paralímpicos Rio- 2016 – CDS Deodoro**. Rio de Janeiro, 2016. 19p.

[7] FIREEYE. **M-Trends.** 2018. Disponível em: < https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf >, acessado em 01 de maio de 2018.

[8] SPITZNER, Lance. **Applying Security Awareness to the Cyber Kill Chain.** 12 de fevereiro de 2018. Disponível em < https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain >, acessado em 01 de maio de 2018.

e) Relacionar o *CKC* com as capacidades previstas ao Dst Cj Def Ciber;

f) Analisar os resultados; e

g) Propor um modelo de emprego do *CKC* que contribua para a identificação de *APT* por parte do Dst Cj Def Ciber.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

Tendo em vista que o emprego do CDCiber é um tema recente[9], existem poucos estudos doutrinários tratando deste assunto[10]. Isso fica mais acentuado quando se procura a função do Dst Cj Def Ciber na doutrina, pois sua atividade técnica ainda é pouco explorada em pesquisas pelas escolas militares. *

Visando contribuir para o desenvolvimento do tema proteção cibernética e a segurança dos sistemas sob responsabilidade do Dst Cj Def Ciber, primeiramente foram elencadas as principais ameaças recorrentes. Dentre essas, foi possível destacar as *APT* por serer a maior fonte de demanda (FIREEYE, 2018). Como consequência observou-se a necessidade da busca pelo aprimoramento da capacidade de identificação destas ameaças.

Durante o Simpósio de Defesa Cibernética 2018, organizado pelo ComDCiber em Brasília-DF, o *CKC* foi apresentado por Laios Felipe Barbosa, Capitão do Centro Integrado de Telemática do Exército (CITEx), como fonte proeminente de auxílio no mapeamento do processo de defesa contra ataques cibernéticos avançados.

Com a consolidação do *CKC* como processo eficaz de classificação das fases que compreendem a maioria dos ataques cibernéticos mais nocivos (SPITZNER, 2018), comumente atrelados a *APT*, surge a necessidade de verificar um possível emprego deste *workflow* em favor da Proteção Cibernética realizada pelo EB por meio do CDCiber.

Fruto deste levantamento, a presente pesquisa visa elencar quais capacidades devem ser exigidas dentro de um Dst Cj Def Ciber a fim de que esse apresente condições mínimas de preparar um campo de batalha resiliente e eficiente na identificação de *APT*, visto que a demora em sua identificação tem sido apresentada como o maior indicador de vulnerabilidade dos sistemas atacados (FIREEYE, 2018).

---

* Nota do autor com base em busca efetuada através da Biblioteca Digital do Exército e no Portal Google.

[9] BRASIL. Ministério da Defesa. **MD31-M-07:** Doutrina Militar de Defesa Cibernética. 1ª Edição. Brasília-DF, 2014.

[10] _____. Exército. Estado-Maior. **EB70-MC-10.232:** Manual de Campanha Guerra Cibernética. 1ª Edição. Brasília-DF, 2017.

Diante disso e da necessidade constante de aprimoramento das técnicas e rotinas voltadas para proteção de sistemas, o trabalho proposto reúne dois assuntos de vanguarda. Ambos são inovadores e caminham integrados gerando subsídio para atualização das ações de proteção cibernética realizadas no âmbito dos Dst Cj Def Ciber (BRASIL, 2014).

2 METODOLOGIA

Quanto ao método de pesquisa utilizado, foi priorizado o método de estudo de caso tendo em vista a singularidade do evento tema e do direcionamento da bibliografia necessária.

O tipo de pesquisa escolhida quanto à forma de abordagem foi a qualitativa focando, principalmente, nas observações dos especialistas consultados.

Quanto ao objetivo geral, foi empregada a modalidade exploratória a fim de apresentar e desenvolver o conhecimento sobre os assuntos abordados na construção de um produto que atenda à especificidade do problema.[11]

2.1 REVISÃO DE LITERATURA

A fim de formular uma proposta como resposta para a pergunta em pauta, esta pesquisa contemplou leitura analítica e fichamento de fontes nacionais e internacionais, entrevistas com especialistas, frequência a simpósio sobre Defesa Cibernética, argumentação e discussão de resultados.

A pesquisa foi baseada em uma revisão de literatura que teve como base três intervalos temporais. O primeiro intervalo visando encontrar os eventos mais antigos com fins introdutórios á Guerra Cibernética compreendendo dados a partir de 1946 (invenção do MARK I, maquina a partir da qual se deu inicio ao desenvolvimento de computadores) até 2018. O segundo intervalo foi de jan/2007 até jul/2018 tendo em vista as primeiras publicações federais, colocando o Brasil no contexto da guerra cibernética, serem de 2008. O terceiro intervalo foi de jan/2010 até jul/2018 tendo em vista que o ano de registro do *Cyber Kill Chain* pela empresa Lockheed Martin foi 2011 e a necessidade de verificar suas interações com as ameaças mais nocivas ao tempo da pesquisa. Entretanto, após verificar a necessidade de buscar informações sobre a doutrina militar dos Estados Unidos da América, foi necessário expandir a janela temporal para o intervalo 2006-2018.

---

[11] BRASIL. Exército Brasileiro. Escola de Aperfeiçoamento de Oficiais. **Manual para Apresentação de Trabalhos Acadêmicos e Dissertações – MTAD 2017.** 4ª Edição. Rio de Janeiro-RJ, 2017.

Foram utilizadas as palavras chave: guerra cibernética, origem, início, primeiro, Doutrina Militar de Guerra Cibernética, Centro de Defesa Cibernética, Destacamento de Guerra Cibernética, Destacamento Conjunto de Defesa Cibernética, Dst Cj Def Ciber, cibernética, relatório grandes eventos, lições aprendidas, grandes eventos, Jogos Paraolímpicos Rio 2016, *Cyber Kill Chain,* ameaças persistentes avançadas e ameaças cibernéticas. Essas palavras e seus termos correlatos em inglês foram pesquisados na base de dados do portal Google.com, Biblioteca Digital do Exército Brasileiro, manuais de campanha, catálogos, notas técnicas, relatórios do Centro de Defesa Cibernética, Portal Fireeye de cibersegurança, Portal do instituto SANS, Portal Lockheed Martin. Também foi realizada busca manual por manuais e relatórios de operação e ocorreu complemento de coleta por meio de participação no Simpósio Brasileiro de Defesa Cibernética 2018.

Quanto ao tipo de operação militar, a revisão de literatura limitou-se a operação JOP Rio 2016.

No que tange à Doutrina Cibernética foram utilizados apenas resultados referentes a publicações militares e governamentais na linha de responsabilidade que incluíssem o Exército Brasileiro. Nos demais temas incluiu-se resultados tendo como fontes trabalhos científicos publicados e mídias de instituições reconhecidas. Foram admitidos resultados referentes a portais de consulta que servem como referência mundial no estudo de ataque e proteção cibernética. Dentre esses resultados foram excluídos aqueles que não realizavam uma abordagem voltada para *framework* visando proteção de sistemas.

2.2 COLETA DE DADOS

Dando prosseguimento à pesquisa teórica a respeito do assunto, a sequência dos trabalhos contemplou a coleta de dados pelos seguintes meios: questionário e grupo focal.

2.2.1 Questionário

O universo a ser estudado compreende os militares das três forças que trabalharam sob coordenação do ComDCiber durante os JOP Rio 2016 compondo os diversos Dst Cj Def Ciber.

Portanto, utilizando-se dados obtidos nos relatórios de missão das operações e em consultas ao CDCiber, a quantidade de pessoas envolvidas foi de 145 militares

e civis que mobiliaram funções ligadas direta ou indiretamente ao trabalho desenvolvido pelos Dst Cj Def Ciber. Uma seleção inicial foi feita excluindo-se 74 militares que não detinham perfil técnico ou que não estavam com seus dados de contato atualizados. A população a ser estudada foi estimada em 71 militares. Tudo isso a fim de maximizar o efeito das respostas obtidas. Entretanto, foi verificado a necessidade de limitar a pesquisa a um grupo de militares que reunisse conhecimento doutrinário envolvendo o assunto e, portanto, imprimindo mais uma limitação a população consultada na qual se inserissem apenas oficiais superiores e intermediários. Assim, foram distribuídos questionários para uma população final a ser estudada de 24 militares da Marinha, Exército e Força Aérea Brasileira nos postos de oficial superior e intermediário.

O universo selecionado, devido ao apoio prestado por mais de 20 unidades militares, hoje está completamente distribuído pelo território nacional, em diferentes Organizações Militares, de maneira a não haver interferência de respostas em massa. A sistemática de distribuição dos questionários ocorreu de forma indireta por e-mail para 24 militares que atendiam aos requisitos. Entretanto, devido a diversos fatores, somente 19 respostas foram obtidas. Ocorreu ainda a necessidade de exclusão de uma dessas respostas tendo em vista o militar não ter participado da operação JOP Rio 2016 e nem apresentar experiência de trabalho relativa ao Dst Cj Def Ciber. Nos demais questionários não houve necessidade de invalidar nenhuma resposta por preenchimento incorreto ou incompleto.

O resultado de 18 respostas válidas (75% dos questionários enviados) mantém o erro amostral de 10% e nível de confiança de 90% para o universo consultado. A seletividade complexa dos especialistas e a impossibilidade de meios diversos para contato individual não viabilizou maior índice de respostas mas atendeu à meta estabelecida. O nível de especialização da amostra, sua potencial influência para o futuro da Guerra Cibernética Brasileira e o ineditismo do tema garantiram resultados proveitosos.

Foi realizado um pré-teste com um instrutor da Escola de Aperfeiçoamento de Oficiais (EsAO) no posto de capitão, três capitães-alunos da EsAO e um Major do CDCiber. Quatro destes militares atendiam aos pré-requisitos para integrar a amostra proposta no estudo com a finalidade de identificar possíveis falhas no instrumento de coleta de dados. Ao final do pré-teste, foram observados erros que justificaram alterações no questionário que foi distribuído após as correções.

2.2.2 Grupo Focal

Devido à natureza exploratória da pesquisa e finalizando a coleta de dados, foi conduzido um grupo focal, visando a debater os resultados colhidos nos questionários, com os seguintes especialistas:

Nome	Justificativa
PEDRO HENRIQUE OLIVEIRA SOUZA – Cap EB	Realizou o curso de Guerra Cibernética, participou dos JOP Rio 2016 pelo CDCiber e serviu no CDCiber.
FELIPE RODRIGUES DE VASCONCELLOS – Cap EB	Foi instrutor do curso de Guerra Cibernética no CIGE, tem mestrado internacional na área Cibernética e serviu no CIGE.
ASAEL DA SILVA VAZ – Cap EB	Realizou o curso de Guerra Cibernética, participou dos JOP Rio 2016 pelo 5º CTA, desempenhou a função de chefe da Seç de Operações do 5º CTA.

QUADRO 1 – Quadro de Especialistas participantes do Grupo Focal
Fonte: O autor

Durante a orientação do referido grupo focal, foram propostas três pautas:

a) Sintetizar em uma resposta as características mínimas necessárias a fim de propor um modelo de medidas para identificação de *APT* que atenda ao Dst Cj Def Ciber;

b) Escolha de modelo a ser adotado como exemplo de emprego do *CKC* e que contemple as características levantadas por meio dos questionários; e

c) Preenchimento e apresentação do modelo proposto.

3 RESULTADOS E DISCUSSÃO

As pesquisas sobre ameaças cibernéticas indicam, de acordo com o relatório anual da FireEye, que o nível de sofisticação das ameaças cibernéticas vem atingindo patamares cada vez mais elevados com o passar dos anos. Nesse contexto o Brasil frequentemente aparece no topo do ranking de países latino-americanos vitimas de *APT* (FIREEYE, 2018).

Esse termo é usado para descrever uma campanha maliciosa de larga duração que objetiva obter o máximo de dados sensíveis dos alvos selecionados. Esse tipo de ataque tem como pré-requisito uma pesquisa profunda e prolongada sobre os alvos e a preparação do ataque envolve diversas etapas.[12]

[12] HUTCHINS, Eric; CLOPPERT, Michael; AMIN, Rohan. **Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains**, 2010. Disponível em: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>, acessado em 01 de maio de 2018.

As *APT* diferem das ameaças tradicionais por apresentarem elevado nível de sofisticação. São utilizadas por *hackers* que tem objetivos mais claros e definidos, buscando atingi-los a qualquer custo, mesmo que levem meses para burlar todas as camadas de segurança do alvo.

Entretanto, para a amostra estudada, parece não haver consenso sobre a identificação de *APT* ocupar uma posição de protagonismo como meio de aprimoramento da eficiência na Proteção Cibernética. Com isso é possível inferir que existem outros fatores relevantes que guardam importância semelhante a esse quesito. Essa afirmativa será explorada por ocasião da conclusão do trabalho como fonte relevante. Além disso a equidade das respostas obtidas reforça o valor do tema em voga.

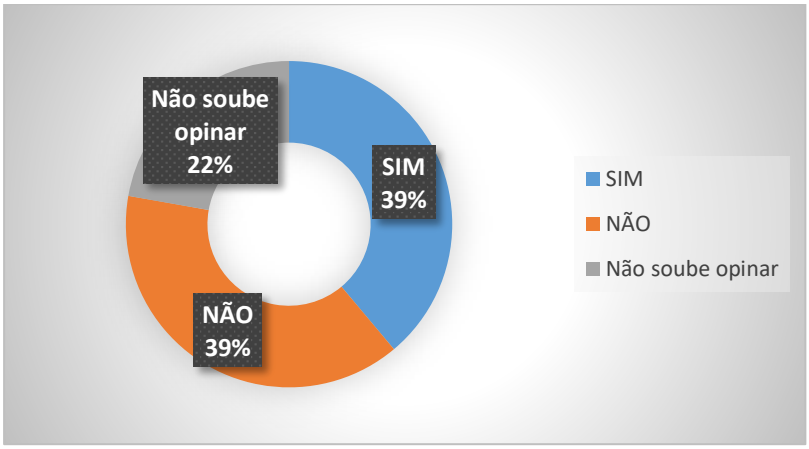

GRÁFICO 1 – Opinião da amostra, em valores relativos, sobre a identificação de *APT* ser considerada, no contexto da atualidade, o principal meio de aprimoramento da eficiência na Proteção Cibernética.
Fonte: O autor

A fim ajudar o processo de tomada de decisão para melhor detecção e resposta a intrusões, os analistas da empresa Lockheed Martin, fabricante de produtos aeroespaciais como o caça F-22, desenvolveram o *CKC.*

Esse *framework* consiste em categorizar os ataques cibernéticos em sete estágios interdependentes, por meio dos quais o defensor pode melhor identificar e mitigar o ataque durante cada uma de suas fases.[13]

O apelo do *CKC* baseia-se no fato de que mesmo se os atacantes implementarem uma ação que explore vulnerabilidades inéditas (dia zero), mas vierem a reutilizar ferramentas ou infraestruturas que sejam suscetíveis de

[13] MARTIN, Lockheed. **The Cyber Kill Chain**. Disponível em: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>, acessado em 01 de maio de 2018.

identificação em alguma outra fase do *framework*, isso levará à mitigação do ataque (HUTCHINS, 2010).

Essa resiliência estabelecida força os atacantes a realizarem aprimoramentos mais complexos para atingir seus objetivos e elevando o custo de campanhas bem-sucedidas.

No Exército Brasileiro essa metodologia vem sendo estudada e foi alvo de apresentação por Laios Felipe Barbosa, Capitão do Exército servindo no CITEx, que durante o Brazil Cyber Defence 2018, realizado em Brasília-DF, abordou o assunto como parte de sua apresentação sobre Defesa Contra Ataques Avançados, Preparação e Emprego de Equipes de Segurança da Informação e Comunicações (SIC).[14]

A disseminação desse framework já pode ser percebida por meio dos dados levantados visto que a maioria dos militares consultados já realizaram algum contato pretérito com o *CKC*.

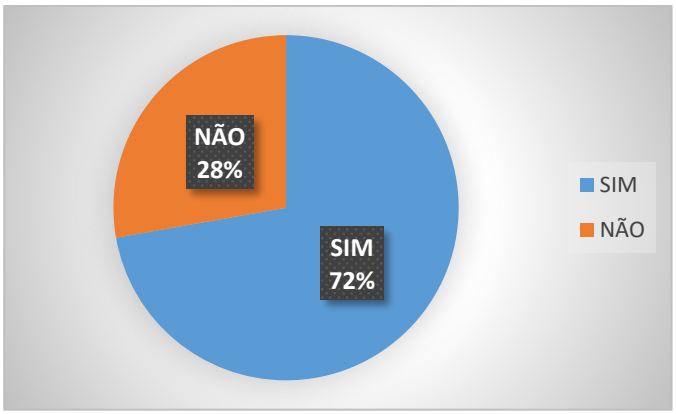

GRÁFICO 2 – Opinião da amostra, em valores relativos, sobre o militar ter conhecimento pretérito mínimo sobre *CKC*.
Fonte: O autor

Dando continuidade a pesquisa foram disponibilizadas fontes de consulta aos militares a fim de gerar algum nivelamento de conhecimento introdutório a respeito do assunto. Em seguida, a amostra foi questionada quanto às atividades de Guerra Cibernética (G Ciber) que poderiam se beneficiar do método (BRASIL, 2017).

[14] BARBOSA, Laios Felipe. **Defesa contra ataques avançados:** preparação e emprego de equipes de SIC. In: SEMINÁRIO INTERNACIONAL DE DEFESA CIBERNÉTICA, 2018, Brasília, DF.

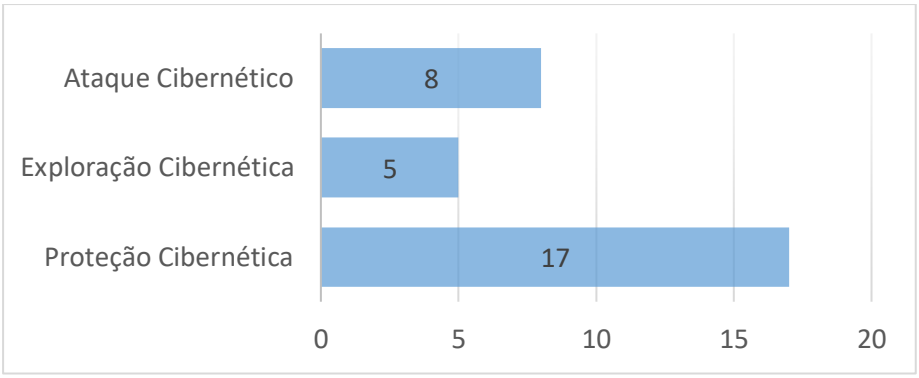

GRÁFICO 3 – Opinião da amostra, em valores absolutos, sobre as atividades de G Ciber que poderiam se beneficiar do *CKC*.
Fonte: O autor

Neste levantamento os consultados poderiam selecionar quantas opções quisessem sem possibilidade de classificação por prioridade.

Percebe-se que a atividade de Proteção Cibernética foi escolhida por 17 dos 18 participantes (94,44%).

Também é possível constatar que os votos recebidos por Ataque e Exploração Cibernética evidenciam que o *CKC* pode beneficiar todas as atividades de G Ciber, sendo a atividade de Proteção Cibernética, aparentemente, a mais privilegiada.

Esses dados corroboram com as propostas da Lockheed Martin (2011) e de Barbosa (2018) sobre a contribuição da ferramenta.

Tendo os conhecimentos colhidos até aqui como base é possível iniciar indagações que englobem também a influencia desses dados em atividades práticas envolvendo equipes de resposta a incidentes de rede e busca de vulnerabilidades, equipes essas que desempenham atividades semelhantes às que o Dst Cj Def Ciber realizou durante os JOP Rio 2016.

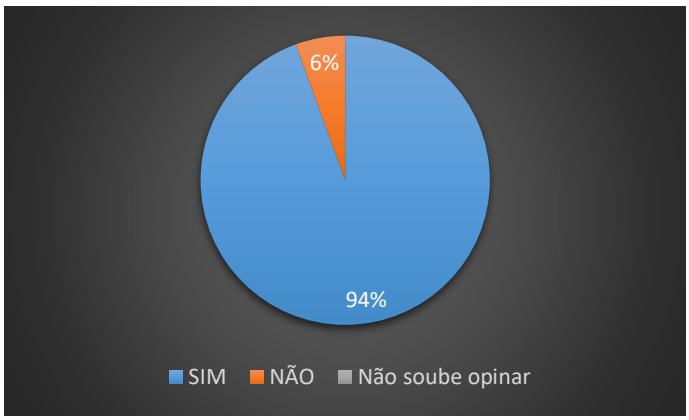

GRÁFICO 4 – Opinião da amostra, em valores relativos, sobre a aplicação dos conceitos de *CKC* em favor do aprimoramento do trabalho de planejamento e emprego do Destacamento Conjunto de Defesa Cibernética.
Fonte: O autor

O Gráfico 4 traduz que, na opinião da amostra, o trabalho de planejamento e emprego do Dst Cj Def Ciber pode ser beneficiado pela aplicação dos conceitos de *CKC*. Com isso é possível subir mais um patamar em direção a enumeração de medidas para identificação de *APT* utilizando os conceitos propostos.

Importante destacar que isso só é possível devido à natureza da amostra, composta 100% por militares que detém conhecimento técnico, experimentados em atividades de G Ciber em sua maioria oficiais superiores (72%).

Quando consultados a respeito da prioridade dos aspectos passíveis de aprimoramento por meio do *CKC,* esses militares optaram pela identificação de ataques com base em processos como sendo o principal aspecto. Contudo, a criação de um procedimento padrão a ser adotado como conduta mínima a ser observada pelo Dst Cj Def CIber aparece com vantagem quando o somados os votos das prioridades 1 e 2.

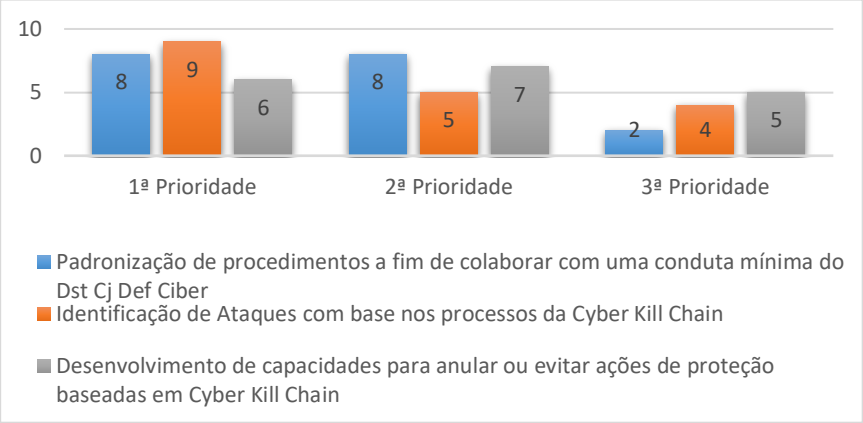

GRÁFICO 5 – Opinião da amostra, em valores absolutos, sobre a prioridade dos aspectos avaliados como passíveis de aprimoramento por meio do CKC.
Fonte: O autor

Em seguida foi proporcionado aos militares apresentar outros aspectos que julgassem de interesse. As respostas obtidas reforçavam a ideia de que a abordagem do *CKC* seria melhor aproveitada em operações de grande vulto como os JOP Rio 2016, que poderia contribuir com a capacidade de consciência situacional de proteção cibernética e que existem várias outras ferramentas que devem ser aplicadas concomitantemente.

Não obstante, foi destacado que o mais importante não seria nenhuma aplicação, metodologia ou software, mas sim a expertise dos analistas cibernéticos a fim de conduzirem as ações de acordo com as características de cada incidente, ataque ou evento.

Essa assertiva pode ser ratificada pelos resultados colhidos a respeito dos desafios de implementação do *CKC* para as Forças Armadas.

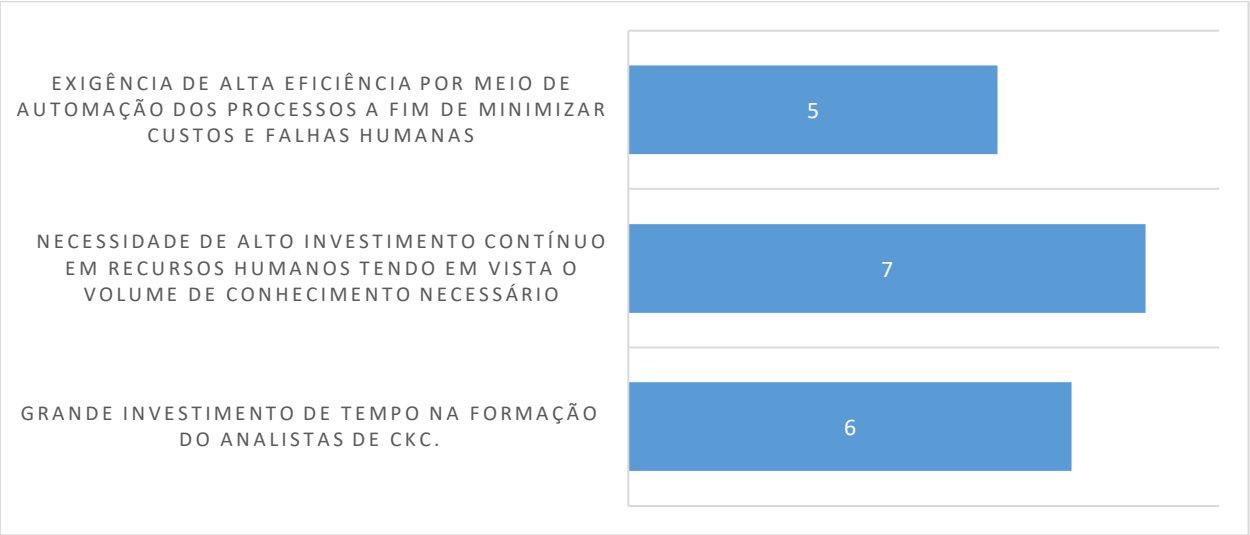

GRÁFICO 6 – Opinião da amostra, em valores absolutos, sobre quais aspectos podem representar desafios consideráveis na implementação do *CKC* visto o contexto nacional das Forças Armadas

Fonte: O autor

Quanto a este quesito, a opção alusiva à eficiência de processos foi a menos votada enquanto as outras duas opções versando sobre investimento contínuo e formação de recursos humanos apresentaram valoração superior.

Neste item, foi aberto um espaço para “outras opções”, no qual destacaram-se comentários a cerca da:

a) amplitude de aplicabilidade necessária abranger ao menos uma Força Armada (FA) de cada vez;

b) necessidade de sensibilizar as autoridades; e

c) alteração da cultura das equipes de tratamento de incidentes de rede, inclusive a das organizações enquadrantes, que geralmente estão acostumadas a trabalhar com modelos baseados em reatividade.

É necessário esclarecer que essas afirmações são coerentes com o modelo em estudo e ressaltam a importância da maturidade institucional necessária para sua melhor implementação.

Diante do exposto pode-se depreender que existe uma demanda legítima pela implementação do *CKC* em favor do Dst Cj Def Ciber assim como o reconhecimento da influência decisiva do *CKC* na produção de doutrina por meio de manuais técnicos de G Ciber de acordo com o Gráfico 7.

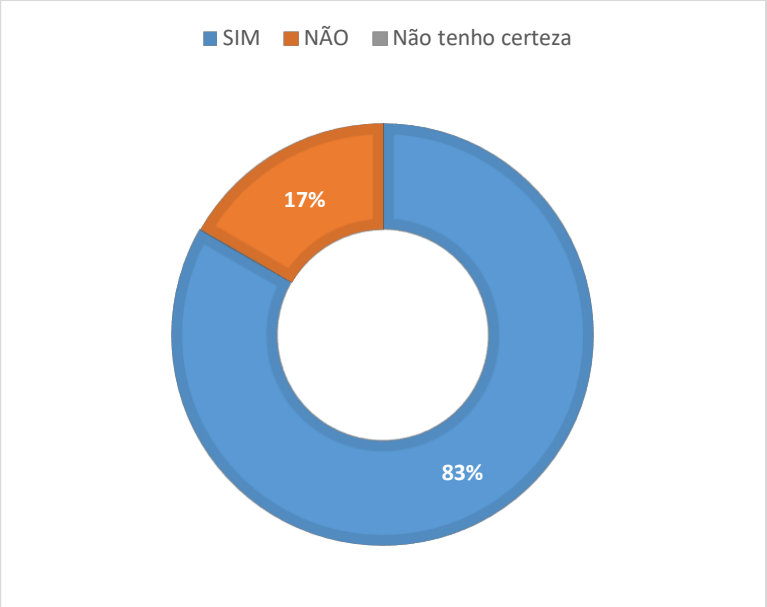

GRÁFICO 7 – Opinião da amostra, em valores relativos, sobre a influência decisiva do *CKC* na produção de doutrina por meio de manuais técnicos de G Ciber.

Fonte: O autor

Por fim foi realizado uma pergunta aberta a respeito da visão de cada um dos consultados sobre como o *CKC* pode colaborar para concepção de alguma parte desses manuais técnicos.

Isso possibilitou verificar criticamente a visão da amostra e extrair conclusões úteis, das quais ressaltam-se:

a) a amostra apresentou demanda por definição de procedimentos claros e obrigatórios que subsidiassem a tomada de decisão contemplando a análise simultânea dos muitos processos contínuos fundamentais à Proteção Cibernética;

b) outra demanda foi a necessidade de personalizar a aplicação do *CKC* para a realidade das FA; e

c) por último foi observado a potencialidade do modelo *CKC* em favorecer, de maneira amigável, o registro de dados que poderiam ser usados posteriormente para atualização de procedimentos os quais, ao longo do tempo, poderiam impactar a doutrina.

Da análise das considerações dos militares é possível extrair características mínimas necessárias a fim de propor um modelo de medidas para identificação de *APT* que atenda ao Dst Cj Def Ciber.

Grupo \ Sugestões	**Como o *CKC* pode colaborar para concepção de alguma parte dos manuais técnicos.**
AMOSTRA	**1)** Por já estar organizado pode contribuir sendo um guia, ou espinha dorsal, dos diversos processos de tomada de decisão, indicando como reagir em pouco tempo.
	2) Procedimentos de como lidar com ameaças cibernéticas
	3) Elencando estatísticas e identificações de falhas já ocorridas no passado, de forma preventiva, não facultativa.
	5) A metodologia contemplada pelo CKC pode ser de grande valia para as atividades de Ptc Ciber, sendo devidamente adaptada às capacidades e demandas do Dst Cj Def Ciber conforme previsto no manual.
	6) A CKC pode ser aproveitada como fonte de conhecimento a respeito de técnicas usadas pela comunidade hacker para ações no espaço cibernético.
	7) Com a capacidade de levantamento de dados é possível melhorar os manuais técnicos devido a melhor visão dos tipos de exploração e maneiras de contenção.
	8) Na prevenção de ataques, incluindo pops.
	9) A definição do CKC em si já traz contribuição, restando personalizar sua aplicação para a realidade das FA.
	10) Com a definição de parâmetros obrigatórios ou padrões de proteção.

QUADRO 2 – Considerações dos militares (resposta opcional)
Fonte: O autor

Essas características foram sintetizadas, por meio de grupo focal, da seguinte forma: geração de consciência situacional por meio de banco de dados com registro contínuo de informação contendo falhas históricas e elencando estatísticas das ferramentas; tudo organizado segundo o *CKC* para subsidiar uma tomada de decisão no mais curto prazo e utilizando um correlacionador de eventos a fim de sugerir possíveis linhas de ação com base em problemas anteriores.

O grupo focal concluiu, observando as características sugeridas, que o modelo tradicional[15] de segurança não atende sozinho às demandas solicitadas visto a integração entre as equipes e o compartilhamento de dados de ameaças identificadas dependerem sobretudo de processos humanos.

Dessa forma, segundo o grupo focal, é interessante que recursos mais automatizados sejam empregados, como por exemplo as *Threat Intelligence Platforms* (*TIP*)[16], ou qualquer outra solução que favoreça um processo automatizado de aplicação do *CKC*.

[15] Solução envolvendo equipes de segurança utilizando processos e ferramentas para resposta de incidentes, proteção de rede e analise de ameaças.
[16] Tecnologia em ascensão baseado em quatro fundamentos: agregação de inteligência de múltiplas fontes; curadoria, normalização, enriquecimento e classificação de risco dos dados; integrações com sistemas de segurança existentes; e Análise e compartilhamento de inteligência de ameaças.

4 CONSIDERAÇÕES FINAIS

Como forma de propor medidas que favoreçam a identificação de *APT* sob a ótica do *CKC*, o Quadro 3 apresenta uma proposta simples, porém elucidativa, de como proporcionar consciência situacional acerca de uma infraestrutura de rede, favorecendo assim a identificação de *APT* (MARTIN, 2015).

VERBO / FASE	Coletar	Buscar	Interromper	Negar	Degradar	Corromper	Destruir
Reconhecimento (Reconnaissance)	-	SIEM	Treinamento de recursos humanos Auditorias	Honeypot	-	-	-
Preparação (Weaponization)	Análise de Logs Black list (IP)	Análise de Logs Firewall NIPS Black list (IP)	Auditorias Firewall ACL	Sistema de Firewall Firewall ACL	Atualização de regras de Firewall Firewall ACL	-	-
Entrega (Delivery)	Análise de Logs HIDS Política de sistemas atualizados Gerenciamento de segurança contra engenharia social	HIDS Política de sistemas atualizados Gerenciamento de segurança contra engenharia social	Firewall ACL	Firewall ACL	-	HIDS Política de sistemas atualizados Gerenciamento de segurança contra engenharia social	HIDS Política de sistemas atualizados Gerenciamento de segurança contra engenharia social
Exploração (Explotation)	NIPS HIPS	-	NIPS	IPS NIPS	IPS NIPS	HIPS	HIPS
Instalação (Installation)	Forense NIPS HIPS	IDS	IPS NIPS SIEM	Anti-vírus NIPS	NIPS SIEM	HIPS	HIPS
C^2 (Command & Control)	HIPS SIEM	HIPS SIEM	Anti-vírus NIPS Firewall ACL	Sistema de Firewall NIPS Firewall ACL	NIPS Firewall ACL	HIPS SIEM	HIPS SIEM
Ação no Objetivo (Actions on Objective)	IDS File Integrity Monitoring (FIM)	IDS FIM	Anti-vírus	Sistema de firewall	-	Inteligência de ameaças FIM	Inteligência de ameaças FIM

QUADRO 3 – Contramedidas
Fonte: O autor

Esse quadro é uma adaptação, concebida pelo grupo focal, para a doutrina brasileira baseado no trabalho realizado por Hutchins (2010, p.5) que relacionou as fases do *CKC* com algumas das ações previstas na doutrina de Operações de Informação do Departamento de Defesa americano.[17]

Relacionando as sete fases do *CKC* (coluna da esquerda) com os verbos das

[17] U.S. DEPARTMENT OF DEFENCE. **Joint Publication 3-13 Information Operations**. 2006. Disponível em: <https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf>, acessado em 29 de agosto de 2018.

capacidades operativas da G Ciber brasileira, Exploração e Ataque Cibernético, é possível alocar a maioria dos recursos que o defensor dispõe, verificar quais ações esses recursos são capazes de identificar/mitigar e por fim classificar em qual fase do *CKC* esse evento provavelmente ira ocorrer.

As lacunas que permanecerem vazias indicam brechas que podem ser exploradas por campanhas maliciosas.

Quanto mais avançado a lacuna estiver no modelo do *CKC*, mais próximo ao seu objetivo o atacante estará e maior será a criticidade do evento. Utilizando esses critérios, os esforços e investimentos podem ser melhor priorizados na busca pela manutenção da resiliência.

Um exemplo disso é que uma lacuna na fase de Comando e Controle (C2) é muito mais crítica que uma lacuna na fase de Exploração e desta forma deve ser priorizado adequadamente.

Diante do supracitado e como forma de propor uma futura melhoria para o emprego desse quadro, podem ser criados parâmetros para uma *TIP* com a finalidade de fornecer esse tipo de quadro como saída (resultado do cruzamento de parâmetros), além de associar tentativas de invasão e eventos de segurança futuros a fim de ajudar a identificar qual lacuna estaria sendo mais assediada pelas campanhas de ataque recentes.

Importante salientar que nem todas as lacunas precisam ser preenchidas para todas as redes, no entanto, com a ajuda de uma *TIP*, as demandas existentes podem ser melhor mapeadas e levar ao desenvolvimento de ferramentas que preencham determinadas lacunas aparentemente sem solução (HUTCHINS, 2010).

Com base no exposto é possível chegar a seguinte conclusão sobre a problemática da pesquisa: o *CKC* é uma opção interessante a ser explorada em favor do Dst Cj Def Ciber como fonte de aprimoramento para as medidas de proteção cibernética que visam identificar *APT*. Isso pode ser realizado atuando nas diversas tarefas da G Ciber por meio dos manuais técnicos e no desenvolvimento de ferramentas, de preferência automatizadas, como as *TIP.*

REFERÊNCIAS

BARBOSA, Laios Felipe. **Defesa contra ataques avançados:** preparação e emprego de equipes de SIC. In: SEMINÁRIO INTERNACIONAL DE DEFESA CIBERNÉTICA, 2018, Brasília, DF.

BRASIL. Exército. Estado-Maior. **EB20-C-07.001:** Catálogo Capacidades do Exército. Brasília, DF, 2015.

_____._____. **EB70-MC-10.232:** Guerra Cibernética. 1ª Edição. Brasília, DF, 2017.

_____. Ministério da Defesa. **MD31-M-07:** Doutrina Militar de Defesa Cibernética. 1ª Edição. Brasília, DF, 2014.

CARVALHAIS, André Melo Dutra. **Introdução à Guerra Cibernética:** a necessidade de um despertar brasileiro para o assunto. São José dos Campos, SP, 2007. Disponível em: <http://www.sige.ita.br/anais/IXSIGE/Artigos/GE_39.pdf>, acessado em 16 de outubro de 2017.

DA CUNHA, Caio Tavares. **CDS Deodoro**: Relatório de Missão Jogos Olímpicos e Paralímpicos Rio - 2016. Rio de Janeiro, 2016. 19p.

HUTCHINS, Eric; CLOPPERT, Michael; AMIN, Rohan. **Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains**. 2010. Disponível em: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>, acessado em 01 de maio de 2018.

CAVELTY, Myrian Dunn. **Critical information infraestructure:** vulnerabilities, threats and responses. 2007.

EXÉRCITO BRASILEIRO. Escola de Aperfeiçoamento de Oficiais. **MTAD 2017:** Manual para apresentação de trabalhos acadêmicos e dissertações**.** 4ª Edição. Rio de Janeiro-RJ, 2017.

FIREEYE. **M-Trends 2018.** 2018**.** Disponível em: <https://www.fireeye.com/content/ dam/collateral /en/mtrends-2018.pdf>, acessado em 01 de maio de 2018.

MARTIN, Lockheed. **The Cyber Kill Chain**. 2015. Disponível em: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>, acessado em 01 de maio de 2018.

_____. **Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform**. 2015. Disponível em: <https://www.lockheedmartin.com/content/dam/Lockheedmartin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf>, acessado em 01 de maio de 2018.

PORTAL G1. **Ciberataques em Larga Escala Atingem Empresas no Mundo e Afetam Brasil** Disponível em: <https://www.g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sãoalvo-cyber-ataques-em-larga-escala.ghtml>, acessado em: 01 de maio de 2018.

SPITZNER, Lance. **Applying Security Awareness to the Cyber Kill Chain.** 12 de fevereiro de 2018. Disponível em <https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain>, acessado em 01 de maio de 2018.

U.S. DEPARTMENT OF DEFENCE. **Joint Publication 3-13 Information Operations**. 2006. Disponível em: <https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf>, acessado em 29 de agosto de 2018.

THE ECONOMIST. **War in the fifth domain**. 2010. Disponível em < http://www.economist.com/node/16478792>, acessado em: 08 de novembro de 2017.