

**ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1811)
CURSO DE CIÊNCIAS MILITARES**

Danielson Campos dos Santos Filho

**UTILIZAÇÃO DO PYMISP PARA APLICAÇÃO DE REGRAS DE SEGURANÇA
EM EQUIPAMENTOS DE SEGURANÇA CIBERNÉTICA EMPREGADOS EM
EXERCÍCIOS NO TERRENO**

**Resende
2022**

Danielson Campos Filho



**APÊNDICE III (TERMO DE AUTORIZAÇÃO DE USO
DE DIREITOS AUTORAIS DE NATUREZA
PROFISSIONAL) AO ANEXO B (NITCC) ÀS
DIRETRIZES PARA A GOVERNANÇA DA PESQUISA
ACADÊMICA E DA DOCTRINA NA AMAN**

**AMAN
2022**

**TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA
PROFISSIONAL**

**TÍTULO DO TRABALHO: UTILIZAÇÃO DO PYMISP PARA APLICAÇÃO DE
REGRAS DE SEGURANÇA EM EQUIPAMENTOS DE SEGURANÇA
CIBERNÉTICA EMPREGADOS EM EXERCÍCIOS NO TERRENO**

AUTOR: DANIELSON CAMPOS DOS SANTOS FILHO

Este trabalho, nos termos da legislação que resguarda os direitos autorais, é considerado de minha propriedade.

Autorizo a Academia Militar das Agulhas Negras a utilizar meu trabalho para uso específico no aperfeiçoamento e evolução da Força Terrestre, bem como a divulgá-lo por publicação em revista técnica da Escola ou outro veículo de comunicação do Exército.

A Academia Militar das Agulhas Negras poderá fornecer cópia do trabalho mediante ressarcimento das despesas de postagem e reprodução. Caso seja de natureza sigilosa, a cópia somente será fornecida se o pedido for encaminhado por meio de uma organização militar, fazendo-se a necessária anotação do destino no Livro de Registro existente na Biblioteca.

É permitida a transcrição parcial de trechos do trabalho para comentários e citações desde que sejam transcritos os dados bibliográficos deles, de acordo com a legislação sobre direitos autorais.

A divulgação do trabalho, em outros meios não pertencentes ao Exército, somente pode ser feita com a autorização do autor ou da Direção de Ensino da Academia Militar das Agulhas Negras.

Resende, 18 de Abril de 2022.


Cad Danielson Campos dos Santos Filho

**UTILIZAÇÃO DO PYMISP PARA APLICAÇÃO DE REGRAS DE SEGURANÇA
EM EQUIPAMENTOS DE SEGURANÇA CIBERNÉTICA EMPREGADOS EM
EXERCÍCIOS NO TERRENO**

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Orientador: Miquelângelo de Souza Dias

Resende
2022
Danielson
Campos dos
Santos Filho

Dados internacionais de catalogação na fonte

S237u SANTOS FILHO, Danielson Campos dos

Utilização do PyMISP para aplicação de regras de segurança em equipamentos de segurança cibernética empregados em exercícios no terreno. / Danielson Campos dos Santos Filho – Resende; 2022. 29 p. : il. color. ; 30 cm.

Orientador: Miquelângelo de Souza Dias

TCC (Graduação em Ciências Militares) - Academia Militar das Agulhas Negras, Resende, 2022.

1.Equipamentos de segurança cibernética.
2.Comando e controle. 3.PyMISP. 4.Inteligência de ameaças. 5. Regras de segurança I. Título.

CDD: 355

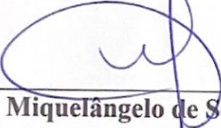
Danielson Campos dos Santos Filho

**UTILIZAÇÃO DO PYMISP PARA APLICAÇÃO DE REGRAS DE SEGURANÇA EM
EQUIPAMENTOS DE SEGURANÇA CIBERNÉTICA EMPREGADOS EM
EXERCÍCIOS NO TERRENO**

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Aprovado em 23 de agosto de 2022:

Banca examinadora:

Nimp  1º Ten Mathews Barla Silva
Miquelângelo de Souza Dias, Capitão
(Presidente/Orientador)

Allanderson Rodrigues Teixeira
Allanderson Rodrigues Teixeira, Tenente-Coronel

Antônio Fernando Pires Patury Júnior
Antônio Fernando Pires Patury Júnior, Tenente-Coronel

Resende
2022

Dedico este trabalho aos meus pais, Danielson e Patrícia, por todo apoio que tive e por sempre acreditarem em mim. Se hoje estou realizando o meu sonho de infância é porque a minha base sempre foi sólida e tenho muito orgulho disso.

AGRADECIMENTOS

Ao meu orientador, Capitão Miquelângelo de Souza Dias, por suas orientações na vida acadêmica, profissional e pessoal, constituindo um exemplo de militar que por inúmeras vezes, durante as retiradas de dúvidas desse trabalho, me auxiliou a pensar de forma mais madura e otimista.

Agradeço primeiramente a Deus, por ter colocado no meu caminho oportunidades e pessoas que me prestaram todo tipo de apoio desde que decidi ingressar na Academia Militar das Agulhas Negras, e pudesse estar concluindo o meu maior sonho, o de tornar-me Oficial do Exército Brasileiro.

Agradeço também a minha família, em especial aos meus pais, por lutarem por mim em todos os momentos, me apoiando, me orientando e me corrigindo em todos os momentos.

Estendo esses agradecimentos à minha namorada, Caroline Benites Neves, que me ajudou a lidar com todas as minhas dificuldades da vida castrense, sendo mais do que namorada, sendo a minha família e a minha melhor amiga. À Família de Erivan e Karina por todo carinho e atenção que me deram durante quatro anos de formação.

Por fim, meu orientador, por todo o esforço e dedicação em auxiliar-me no desenvolvimento deste trabalho, sempre estando disponível para ajudar, tirar dúvidas e contribuir para que esse Trabalho de Conclusão de Curso tivesse êxito.

RESUMO

UTILIZAÇÃO DO PYMISP PARA APLICAÇÃO DE REGRAS DE SEGURANÇA EM EQUIPAMENTOS DE SEGURANÇA CIBERNÉTICA EMPREGADO EM EXERCÍCIOS NO TERRENO

AUTOR: Danielson Campos dos Santos Filho

ORIENTADOR: Miquelângelo de Souza
Dias

Com o crescimento do ambiente cibernético, inúmeras ferramentas foram criadas para testar a vulnerabilidade dos sistemas de informação, bem como extrair informações ou interferir na Confidencialidade, Integridade, Disponibilidade e Autenticidade dos diversos equipamentos de segurança cibernética. Na Academia Militar das Agulhas Negras, durante o fim do calendário acadêmico ocorre a Manobra Escolar, (“Manobrão”) que tem como objetivo a aplicação prática dos conhecimentos adquiridos ao longo do ano letivo no Sistema de Educação e Cultura do Exército, e representa a maior atividade de preparo executada no campo pela Força Terrestre. Durante esse exercício, é necessário interligar as informações provenientes de sensores, equipamento IoBT (*Internet of Battlefield Things*), e atuadores, a tropa, importantes para o Comando e Controle da tropa, através dos Centros de Coordenação de Operações que auxiliam no desenvolvimento das atividades e na proteção dos dados relevantes. Por isso, faz-se necessário o presente estudo para explorar as aplicações de métodos de gerenciamento de segurança para dispositivos em rede, através de inteligência de ameaças PyMISP/MISP para aplicar regras de segurança e para garantir a proteção de dados e dispositivos contra agentes maliciosos que possam influenciar no desenvolvimento das atividades ou obter informações sigilosas do exercício militar. Além disso, para contribuir com o compartilhamento de ameaças entre as diversas unidades a fim de mitigar os efeitos de um possível agente atacante. Por fim, foram coletados 82.169 Hosts maliciosos que se tornam regras de segurança cibernética

Palavras-chave: Equipamentos de segurança cibernética. Manobrão. Comando e Controle. PYMISP. Inteligência de ameaças. Regras de segurança.

ABSTRACT

USE OF PYMISP TO APPLY SAFETY RULES IN CYBER SECURITY EQUIPMENT USED IN BOOT CAMP

AUTHOR: Danielson Campos dos Santos Filho

ADVISOR: Miquelângelo de Souza Dias

With the growth of the cyber environment, numerous tools have been created to test the vulnerability of information systems, as well as extract information or interfere with the Confidentiality, Integrity, Availability and Authenticity of the various cybersecurity equipment. At the Academia Militar das Agulhas Negras, during the end of the academic calendar, the School Maneuver takes place, (“Manobra”), which aims at the practical application of the knowledge acquired throughout the academic year in the Education and Culture System of the Army and represents the greater preparation activity performed in the field by the Land Force. During this exercise, it is necessary to link information from sensors, IoBT equipment (Internet of Battlefield Things), and actuators, to the troop, which are important for the Command and Control of the troop, through the Operations Coordination Centers that assist in the development of activities. and the protection of relevant data. Therefore, the present study is necessary to explore the applications of security management methods for networked devices, through PyMISP/MISP threat intelligence to apply security rules and to ensure the protection of data and devices against malicious agents. that may influence the development of activities or obtain confidential information from the military exercise. In addition, to contribute to the sharing of threats between the different units in order to mitigate the effects of a possible attacking agent. Finally, 82,169 malicious hosts that become cybersecurity rules were collected.

Keywords: Cyber security Equipment. Manobra. Command and Control. PyMISP. Threat intelligence. Security rules.

LISTA DE FIGURAS

Figura 1 – Usando o PyMISP.....	15
Figura 2 – Usando o PyMISP.....	15
Figura 3 – Usando o PyMISP.....	15
Figura 4 – Usando o PyMISP.....	16
Figura 5 – Usando o PyMISP.....	16
Figura 6 – Login do MISP.....	18
Figura 7 – Feeds de alimentação.....	19
Figura 8 – Eventos.....	20
Figura 9 – Remoção de aviso de segurança e importação da StringIO.....	20
Figura 10 – Listando as vulnerabilidades.....	21
Figura 11 – Relative_path.....	21
Figura 12 – Relative_path.....	22
Figura 13 – Identificando ameaças através dos dados coletados.....	22
Figura 14 – Hosts maliciosos identificados.....	23

SUMÁRIO

1	INTRODUÇÃO.....	9
1.1	OBJETIVOS.....	10
1.1.1	Objetivo geral.....	10
1.1.2	Objetivos específicos.....	10
2	REFERENCIAL TEÓRICO.....	11
2.1	CIBERNÉTICA.....	11
2.1.1	Guerra Cibernética.....	11
2.2	FERRAMENTAS UTILIZADAS EM OPERAÇÕES MILITARES.....	12
2.2.1	MISP (Malware Information Sharing Platform).....	12
2.2.2	PyMISP.....	12
2.2.3	API REST.....	13
2.2.4	Docker/Contêineres.....	13
2.2.5	Anaconda Navigator/Jupyter.....	14
2.2.6	Firewall.....	14
2.3	UTILIZAÇÃO DO PYMISP.....	15
3	REFERENCIAL METODOLÓGICO.....	17
3.1	TIPO DE PESQUISA.....	17
3.2	MÉTODOS.....	17
4	RESULTADOS E DISCUSSÃO.....	18
4.1	INFORMAÇÕES COLETADAS PELO MISP.....	18
4.2	UTILIZANDO INFORMAÇÕES COLETADAS NO MISP/PyMISP.....	20
4.3	DISCUSSÃO.....	24
5	CONSIDERAÇÕES FINAIS.....	25
	REFERÊNCIAS.....	26

1 INTRODUÇÃO

O avanço da Guerra Cibernética vem influenciando cada vez mais os relacionamentos entre Estados e Nações. Atualmente, o ambiente cibernético vem se concretizando como o mais novo domínio de guerra, além do Espaço Terrestre, Marítimo, Aéreo e Espacial (Geespacial) (SILVA, 2014).

Neste sentido a Guerra Cibernética envolve ações ofensivas, defensivas e/ou exploratórias, no espaço cibernético, que tem por objetivo negar ou neutralizar o inimigo para que este não a utilize em benefício próprio, garantindo a confidencialidade, integridade, disponibilidade e autenticidade das informações existentes em computadores, redes e sistemas informacionais tanto das Forças Armadas quanto das instituições civis do País (SILVA, 2014).

O maior objetivo das Forças Armadas no espaço cibernético vem consistindo em garantir a proteção da informação, que é o produto mais sensível desse domínio. Por isso os sistemas de Comando, Controle, Comunicações e Informação (C³I), computadores, equipamentos de segurança cibernética e sistemas, que contribuem para a decisão, vem se integrando cada vez mais nesse novo ambiente (SILVA, 2014).

Dessa forma, esse espaço se tornou fundamental nos contextos civil e militar em decorrência da grande importância estratégica e militar que trazem os computadores e suas redes, contribuindo de forma significativa para a disseminação de ordens ou informações. Essas informações, que trafegam nessas redes, vêm propiciando a interligação de aeronaves, embarcações, bases locais de apoio e centros estratégicos de controle dispersos territorialmente. E descobrir vulnerabilidades que possam viabilizar a obtenção dessas informações para utilizá-los em proveito próprio consiste no objetivo da denominada “Guerra Cibernética” (SILVA, 2014).

Portanto, dada os antecedentes dos conflitos militares e as proporções do combate moderno onde a complexidade e incerteza estão presentes e que o detentor do poder informacional garante efetivo poder ofensivo e defensivo, cabe às Forças Armadas garantir a sua própria segurança de forma rápida e decisiva.

Desse modo, as áreas de concentração que envolvem o presente estudo são de cunho cibernético e a importância para as operações militares onde as informações, a escassez de tempo para tomada de decisão e proteção de dados tomam proporções maiores. Dentre as diversas ferramentas de proteção cibernética, o presente estudo visa abordar a relevância da utilização do MISP/PyMISP como forma de aplicar regras de segurança cibernética em firewall, equipamento de segurança cibernético que será o objeto de estudo.

1.1 OBJETIVOS

1.1.1 Objetivo geral

O objetivo geral da pesquisa visa apresentar o MISP/PyMISP como principal ferramenta para compartilhamento de inteligência de ameaças e aplicar regras de segurança cibernética, como forma de garantir a confidencialidade, integridade, disponibilidade e autenticidade em equipamentos de segurança cibernética.

Nesse contexto, a pesquisa tem por finalidade abordar a explorar as aplicações de um método interdisciplinar de gerenciamento de segurança para equipamentos de segurança cibernética em operações militares, para o presente estudo será utilizado o firewall, através da ferramenta de compartilhamento de inteligência de ameaças MISP/PyMISP e aplicando regras de segurança. Assim, auxiliando na proteção de dados e informações contra ataques e agentes maliciosos de modo que influencie na redução de vulnerabilidade nas redes das Forças Armadas.

1.1.2 Objetivos específicos

Apresentar as informações coletadas pelo MISP evidenciando a sua importância para o presente estudo.

Apresentar como as informações coletadas podem ser utilizadas no MISP/PYMISP. Apresentar a aplicação de regras de segurança em firewall.

Salientar a importância do MISP/PYMISP para a segurança e guerra cibernética na prevenção de ameaças, apresentando dados que confirmem a sua eficiência.

2 REFERENCIAL TEÓRICO

2.1 CIBERNÉTICA

2.1.1 Guerra Cibernética

O Departamento de Defesa dos EUA (em inglês, *Department of Defense* - DoD) define Espaço Cibernético como “um domínio global dentro do ambiente de informações que consistem das redes interdependentes de infra-estruturas de Tecnologia da Informação (TI), incluindo a Internet, redes de telecomunicações, sistemas de computador, processadores e controladores embutidos” (SILVA, 2014).

No Brasil, o Ministério da Defesa (MD) define Guerra Cibernética como “o conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores”. Essas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil (BRASIL, 2007c, p. 123).

Entretanto, não há consenso entre os diversos autores sobre a definição do termo “Guerra Cibernética”. Para nosso estudo, além da definição proposta pelo ministério da defesa, buscamos a definição proposta por Parks e Duggan em 2001.

É o subconjunto da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes. Existem diversos mundos cibernéticos, mas o mais relevante para a Guerra Cibernética é a Internet e as redes a ela relacionadas, as quais compartilham mídia com a Internet. A definição militar mais próxima para o nosso termo, guerra cibernética, é uma combinação de ataque a redes de computadores e defesa de redes de computadores, e possivelmente, operações especiais de informação. Nós definimos guerra cinética como sendo a guerra praticada no “mundo real”. Todos os blindados e navios e aviões e soldados tradicionais são os protagonistas da guerra cibernética. (tradução do autor).

Para Dutra (2001) as pesquisas que são responsáveis por desenvolver as ferramentas, técnicas e conhecimentos voltados para a Segurança da Informação possuem aplicações em Guerra Cibernética. Por esse motivo, a principal diferença entre elas está na intenção do autor.

2.2 FERRAMENTAS UTILIZADAS EM OPERAÇÕES MILITARES

2.2.1 MISP (Malware Information Sharing Platform)

O MISP (*Malware Information Sharing Platform*) é uma plataforma que consiste em compartilhar, armazenar e correlacionar indicadores de compromissos de ataques direcionados, mas também inteligência de ameaças, como informações de autores de ameaças e informações de fraude financeira (CIRCL.lu, 2021).

A Plataforma de Inteligência e Compartilhamento de Ameaças de Código Aberto permite que as organizações compartilhem informações como inteligência de ameaças, indicadores, informações sobre autores de ameaças ou qualquer tipo de ameaça que possa ser estruturada no MISP. Os usuários do MISP se beneficiam do conhecimento colaborativo sobre *Malware* ou ameaças existentes. O objetivo desta plataforma confiável é ajudar a melhorar as contramedidas usadas contra ataques direcionados e configurar ações preventivas e detecção (CIRCL.lu, 2021).

A Plataforma de Compartilhamento de Informações de Malware é acessível a partir de diferentes interfaces, como uma interface web (para analistas ou manipuladores de incidentes) ou através de uma **API REST** (para sistemas empurrando e puxando IOCs). O objetivo inerente do MISP é ser uma plataforma robusta que garanta uma operação suave de revelar, amadurecer e explorar as informações de ameaças (CIRCL.lu, 2021).

2.2.2 PyMISP

PMISP é uma biblioteca Python utilizada para acessar plataformas MISP através de sua **API REST**. Permitindo buscar eventos, adicionar ou atualizar eventos ou atributos, adicionar ou atualizar amostras ou pesquisar atributos.

Entretanto, é preciso ter acesso à Auth Key na MISP Instance para usar o PyMISP. Segundo a CIRCL.lu (2021), o PYMISP possui as capacidades de:

- Adicionar, obter, atualizar, publicar, excluir eventos;
- Adicionar ou remover tags;
- Adicionar atributos de arquivo: hashes, chave de registro, padrões, tubo, mutex;
- Adicionar atributos de rede: dest/src IP, hostname, domínio, url, UA, entre outros;
- Adicionar atributos de e-mail: fonte, destino, assunto, anexo, entre outros;

- Amostras de upload/download; e
- Atualizar avistamentos.

2.2.3 API REST

Segundo o site Redhat.com (2021) a API REST ou API RESTful, funciona como uma interface de programação de aplicações (API ou API *web*) que está em congruência com as restrições do estilo de arquitetura REST, permitindo a interação com serviços web RESTful. REST é a sigla em inglês para transferência representacional de estado.

A API reúne definições e protocolos que são utilizados no desenvolvimento e na integração de aplicações. Por vezes, as APIs são descritas como um contrato entre um provedor e um usuário de informações, que estabelece o conteúdo exigido pelo consumidor (a chamada) e o conteúdo exigido pelo produtor (a resposta) (Redhat.com, 2021).

Por exemplo, o design da API de um serviço meteorológico pode especificar que o usuário forneça um CEP e o produtor responda em duas partes, a primeira contendo a temperatura mais elevada e a segunda com a temperatura mais baixa (Redhat.com, 2021).

Logo, a interação entre um computador ou sistema para recuperação de informações ou execução de uma função, a API irá auxiliar na comunicação requerida pelo usuário a fim de que ele entenda e execute o que foi solicitado.

As APIs funcionam como mediador entre os usuários ou clientes e os recursos ou serviços *web* que eles têm como interesse. As APIs também são essenciais para que as organizações compartilhem recursos e informações e mantenham a segurança, o controle e a obrigatoriedade de autenticação de forma simultânea, permitindo determinar o que pode ser acessado e quem pode ter acesso.

Outra vantagem de usar APIs é que não é necessário saber todos os detalhes sobre o armazenamento em cache, como os recursos são recuperados ou qual é a origem deles (Redhat.com, 2021).

2.2.4 Docker/Contêineres

O Docker é um projeto de software livre para automatizar a implantação de aplicativos como contêineres autossuficientes portáteis que podem ser executados na nuvem ou localmente. O Docker também é uma empresa que promove e evolui essa tecnologia,

trabalhando em colaboração com fornecedores de nuvem, Linux e Windows, incluindo a Microsoft (Docs.microsoft.com, 2022).

Com o Docker, é possível lidar com os contêineres como se fossem máquinas virtuais modulares e extremamente leves. Além disso, os contêineres oferecem maior flexibilidade para criar, implantar, copiar e migrar um contêiner de um ambiente para o outro. Isso otimiza as aplicações na nuvem (Redhat.com, 2022).

O objetivo dos contêineres é criar essa independência: a habilidade de executar diversos processos e aplicações separadamente para utilizar melhor a infraestrutura e, ao mesmo tempo, manter a segurança que você teria em sistemas separados (Redhat.com, 2022).

2.2.5 Anaconda Navigator/Jupyter

Anaconda Navigator é uma interface de usuário gráfico de desktop incluída na Anaconda que permite iniciar aplicativos e gerenciar facilmente pacotes, ambientes e canais conda sem a necessidade de usar comandos de linha de comando (Anaconda.org, 2022), além de ser uma forma de executar os scripts do PyMISP.

Através do Anaconda foi utilizado o JupyterLab que é uma versão mais moderna do Jupyter Notebook e uma de suas vantagens é a possibilidade de utilizar extensões. O Jupyter Notebook é uma interface gráfica que permite a edição de notebooks em um navegador web (Letscode.com.br, 2022).

Esse tipo de documento virtual permite a execução de códigos de uma linguagem de programação juntamente com ferramentas para edição de textos comuns; ou seja, além das rotinas usuais de programação, o usuário pode documentar todo o processo de produção do código. Dessa forma, o notebook permite uma maneira interativa de programar (Letscode.com.br, 2022).

Os notebooks também oferecem uma programação mais dinâmica, oferecendo ao usuário o output imediato do código; não havendo, assim, a necessidade de compilar ou executar todo o documento (Letscode.com.br, 2022).

2.2.6 Firewall

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança (Cisco.com, 2022).

Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.

2.3 UTILIZAÇÃO DO PYMISP

Para ter uma melhor compreensão de como usar o PYMISP, será analisado os exemplos existentes: *add_named_attribute.py*. Este script permite adicionar um atributo a um evento existente, sabendo apenas seu tipo (a categoria é determinada por padrão) (CIRCL.lu, 2021).

Figura 1 – Usando o PyMISP

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

from pymisp import PyMISP
from keys import misp_url, misp_key
import argparse
```

Fonte: CIRCL.LU (2021)

Em primeiro lugar, precisamos importar PyMISP. Em seguida, também precisamos saber tanto a instância com a qual trabalharemos quanto a chave de API a ser usada: Ambos devem ser armazenados no arquivo *keys.py*.

Finalmente importamos a biblioteca *argparse* para que o script possa lidar com argumentos (CIRCL.lu, 2021).

Figura 2 – Usando o PyMISP

```
# For python2 & 3 compat, a bit dirty, but it seems to be the least bad one
try:
    input = raw_input
except NameError:
    pass
```

Fonte: CIRCL.LU (2021)

Apenas algumas linhas para ter certeza de que python 2 e 3 são suportados.

Figura 3 – Usando o PyMISP

```
def init(url, key):
    return PyMISP(url, key, True, 'json', debug=True)
```

Fonte: CIRCL.LU (2021)

Essa função criará um objeto PYMISP que será usado posteriormente para interagir com a instância MISP. Como visto no *api.py*, um objeto PyMISP precisa saber tanto a URL da instância MISP quanto a chave de API a ser usada. Também pode levar dados adicionais e não obrigatórios, como o uso ou não de SSL ou o nome do formato de exportação (CIRCL.lu, 2021).

Figura 4 – Usando o PyMISP

```
if __name__ == '__main__':
    parser = argparse.ArgumentParser(description='Create an event on MISP.')
    parser.add_argument("-e", "--event", type=int, help="The id of the event to
update.")
    parser.add_argument("-t", "--type", help="The type of the added attribute")
    parser.add_argument("-v", "--value", help="The value of the attribute")
    args = parser.parse_args()
```

Fonte: CIRCL.LU (2021)

Em seguida, a função começa preparando os argumentos aguardados:

- evento: O evento que receberá um novo atributo;
- tipo: O tipo do atributo que será adicionado; e
- valor: O valor do novo atributo devido à função criada anteriormente, criamos um objeto PYMISP. Para adicionar o novo argumento, primeiro é necessário buscar o evento no banco de dados do MISP usando a função *get_event* que precisa do *event_id*. Então, após adquirido, é possível usar a função *add_named_attribute* que irá adicionar o argumento.

Dessa forma o novo evento é impresso, podendo verificar se o atributo foi adicionado corretamente, e que uma categoria foi anexada a ele automaticamente (CIRCL.lu, 2021).

Figura 5 – Usando o PyMISP

```
misp = init(misp_url, misp_key)
event = misp.get_event(args.event)
event = misp.add_named_attribute(event, args.type, args.value)
print(event)
```

Fonte: CIRCL.LU (2021)

3 REFERENCIAL METODOLÓGICO

3.1 TIPO DE PESQUISA

O tipo de pesquisa presente neste estudo é o quantitativo-qualitativo. Foi realizado o estudo do uso do MISP/PyMISP para aplicação de regras de segurança em firewall a partir de dados coletados em ambiente virtual simulado para verificar a eficiência do sistema MISP para o compartilhamento de ameaças e a eficiência do PyMISP na aplicação de regras de segurança cibernética para proteção de dados e informações em firewall contra ataques direcionados garantindo a confidencialidade, integridade, disponibilidade e autenticidade dos equipamentos.

Esse estudo foi realizado durante o ano de 2021 e 2022 na Academia Militar das Agulhas Negras.

3.2 MÉTODOS

O método utilizado nesta pesquisa foi o indutivo e o instrumento foi o de observação sistemática. Foi criado um ambiente isolado por meio de um sistema de contêiner com o objetivo de melhor explorar o MISP/PyMISP propiciando a fluidez nos trabalhos. A fim de verificar a operacionalidade e a eficiência desses sistemas foi instalado o Anaconda Navigator e utilizado a aplicação JupyterLab para adicionar linhas de códigos no PyMISP. Pela complexidade e por não fazer parte dos objetivos desse estudo não serão apresentadas as etapas de criação do referido ambiente virtual.

As etapas dessa pesquisa foram seguidas a partir da instalação do docker e a criação de um contêiner com o MISP, Após isso, foi utilizado o JupyterNotebook para instalar a biblioteca PyMISP, dando sequência para a coleta de dados.

4 RESULTADOS E DISCUSSÃO

4.1 INFORMAÇÕES COLETADAS PELO MISP

Com a criação do sistema de contêiner e a configuração do ambiente virtual é apresentada a tela inicial de *login* do MISP.

Figura 6 – Login do MISP



The image shows the login interface for MISP Threat Sharing. At the top, there is a blue logo consisting of a speech bubble with three dots inside, followed by the text 'MISP Threat Sharing' in a bold, sans-serif font. Below this, the word 'Login' is centered. Underneath, there are two input fields: 'Email' and 'Password'. The 'Email' field is currently empty and has a red border around it. The 'Password' field is also empty. Below the password field is a blue button with the word 'Login' written in white.

Fonte: AUTOR (2022)

Após configurar o ambiente de contêiner, o MISP foi acessado remotamente e, sem seguida, foram gerados eventos a partir dos feeds de alimentação, que podem ser utilizados como fonte de correlações para todos os seus eventos e atributos sem a necessidade de importá-los diretamente em seu sistema. O Sistema de alimentação MISP permite a correlação rápida. Além disso, foi habilitado o feed CIRCL OSINT dentro da instância MISP que é gerado com o gerador de alimentação PyMisp (Misp-project.org, 2022).

Os feeds podem estar em três formatos diferentes: formato padronizado MISP, formato CSV e formato freetext; e localizados em diferentes transportes de entrada como URL (Rede) e Local (arquivo) como pode ser observado na figura abaixo.

Figura 7 – Feeds de alimentação

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

Load default feed metadata
 Cache all feeds
 Cache freetext/CSV feeds
 Cache MISP feeds
 Fetch and store all feed data
 Default feeds
 Custom feeds
 All feeds
 Enabled feeds

ID	Enabled	Caching	Name	Format	Provider	Org	Source URL
<input type="checkbox"/> 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CIRCL OSINT Feed	misp	CIRCL		network: https://www.circl.lu/doc/misp/feed-osint
<input type="checkbox"/> 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	The Botvrij.eu Data	misp	Botvrij.eu		network: https://www.botvrij.eu/data/feed-osint
<input type="checkbox"/> 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CIRCL OSINT Feed	misp	CIRCL		network: https://www.circl.lu/doc/misp/feed-osint/
<input type="checkbox"/> 4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	blockrules of rules.emergingthreats.net	csv	rules.emergingthreats.net	CERT-RLP	network: https://rules.emergingthreats.net/blockrules/compromised-ips.txt
<input type="checkbox"/> 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tor exit nodes	csv	TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor ALL nodes" feed.		network: https://www.dan.me.uk/torlist?exit
<input type="checkbox"/> 6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tor ALL nodes	csv	TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor exit nodes" feed.		network: https://www.dan.me.uk/torlist/
<input type="checkbox"/> 7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	cybercrime-tracker.net - all	freetext	cybercrime-tracker.net		network: https://cybercrime-tracker.net/all.php
<input type="checkbox"/> 8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Phishtank online valid phishing	csv	Phishtank		network: https://data.phishtank.com/data/online-valid.csv
<input type="checkbox"/> 9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ip-block-list - snort.org	freetext	https://snort.org		network: https://snort.org/downloads/ip-block-list
<input type="checkbox"/> 10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	diamondfox_panels	freetext	pan-unl42		network: https://raw.githubusercontent.com/pan-unl42/ocs/master/diamondfox/diamondfox_panels.txt
<input type="checkbox"/> 11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	pop3gropers	csv	home.nuug.no		network: https://home.nuug.no/~peter/pop3gropers.txt
<input type="checkbox"/> 12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feodo IP Blocklist	csv	abuse.ch		network: https://feedotracker.abuse.ch/downloads/ipblocklist.csv
<input type="checkbox"/> 13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	OpenPhish url list	freetext	openphish.com		https://openphish.com/feed.txt
<input type="checkbox"/> 14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	firehol_level1	freetext	iplists.firehol.org		network: https://raw.githubusercontent.com/ksaou/blocklist-ipsets/master/firehol_level1.netset
<input type="checkbox"/> 15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IPs from High-Confidence DGA-Based C&Cs Actively Resolving - requires a valid license	csv	osint.bambenekconsulting.com		network: https://osint.bambenekconsulting.com/feeds/c2-ipmasterlist-high.txt
<input type="checkbox"/> 16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Domains from High-Confidence DGA-based C&C Domains Actively	csv	osint.bambenekconsulting.com		network: https://osint.bambenekconsulting.com/feeds/c2-dommasterlist-high.txt

Fonte: AUTOR (2022)

Assim, os eventos MISP são encapsulamentos para informações contextualmente relacionadas representadas como atributo e objeto. É possível construir eventos completos que estendam um evento existente, dando lugar a uma visão combinada de eventos que inclui uma soma total do evento, juntamente com todos os eventos de extensão (Circl.lu, 2022). Na figura a seguir serão apresentados os eventos no MISP.

Figura 8 – Eventos

Events										Enter value to search	Filter
Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution
<input checked="" type="checkbox"/>	CERT-RLP	ORGRNAME	1465			6218	9	admin@admin.test	2021-11-17	blocklist.greensnow.co/feed	Organisation
<input checked="" type="checkbox"/>	CERT-RLP	ORGRNAME	1464		osint:source-type="block-or-filter-list"	36926	9	admin@admin.test	2021-11-17	blocklist.de/lists/all-ot/feed	Organisation
<input checked="" type="checkbox"/>	CERT-RLP	ORGRNAME	1463		osint:source-type="block-or-filter-list"	725	2	admin@admin.test	2021-11-17	blockrules.of.rules.emergingthreats.net/feed	Organisation
<input checked="" type="checkbox"/>	CUDESO	ORGRNAME	1471		tip:white	329		admin@admin.test	2022-01-13	The BlueNoroff cryptocurrency hunt is still on	All
<input checked="" type="checkbox"/>	ICS-CSIRT.io	ORGRNAME	1474		misp-galaxy:financial-fraud="Business Email Compromise" misp-galaxy:mitre-attack-pattern="Business Relationships - T1591.002" misp-galaxy:mitre-attack-pattern="Credentials - T1589.001" misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" tip:white	44		admin@admin.test	2022-01-20	Campaigns abusing corporate trusted infrastructure hunt for corporate credentials on ICS networks	All
<input checked="" type="checkbox"/>	CUDESO	ORGRNAME	1473		tip:white	18		admin@admin.test	2022-01-19	TinyNuke Banking Malware Targets French Entities	All
<input checked="" type="checkbox"/>	CUDESO	ORGRNAME	1472		tip:white	12	1	admin@admin.test	2022-01-16	Destructive malware targeting Ukrainian organizations	All
<input checked="" type="checkbox"/>		ORGRNAME	1468		type:OSINT osint:lifetime="perpetual" osint:certainty="50" tip:white misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" misp-galaxy:target-information="Ukraine" collaborative-intelligence:request="related-samples" collaborative-intelligence:request="sample"	20	1	admin@admin.test	2022-01-16	MSFT - MSTIC - Destructive malware targeting Ukrainian organizations	All
<input checked="" type="checkbox"/>		ORGRNAME	1467		type:OSINT osint:lifetime="perpetual" osint:certainty="50" tip:white misp-galaxy:mitre-enterprise-attack-intrusion-set="MuddyWater - G0069" misp-galaxy:mitre-intrusion-set="MuddyWater - G0069" misp-galaxy:threat-actor="MuddyWater" misp-galaxy:country="Iran"	119		admin@admin.test	2022-01-13	CYBERCOM_Malware_Alert - MuddyWater has been seen using a variety of techniques to maintain access to victim networks.	All
<input checked="" type="checkbox"/>	CUDESO	ORGRNAME	1248		tip:white	79	4	admin@admin.test	2015-09-15	In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia	All
<input checked="" type="checkbox"/>	CUDESO	ORGRNAME	1271		tip:white	8		admin@admin.test	2015-11-16	WitchCoven: Exploiting Web Analytics to Ensnare Victims	All
<input checked="" type="checkbox"/>	CUDESO	ORGRNAME	1279		tip:white	13	1	admin@admin.test	2019-03-22	Operation ShadowHammer	All

Fonte: AUTOR (2022)

4.2 UTILIZANDO INFORMAÇÕES COLETADAS NO MISP/PyMISP

Após a instalação a criação do contêiner com o MISP, foi feita a instalação da biblioteca PyMISP no Jupyter Notebook (Extensão do Anaconda) para executar os scripts do PyMISP para coletar os dados cibernéticos.

Primeiramente, para facilitar o presente estudo será executado um código para remoção das mensagens de segurança. Em seguida, será importado a StringIO que pode ser útil quando for lidar com APIs cuja interface exige objetos file.

Figura 9 – Remoção de aviso de segurança e importação da StringIO

```
In [1]: # Remover mensagem de aviso de segurança
import requests
from requests.packages.urllib3.exceptions import InsecureRequestWarning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

In [2]: from misp import misp
import os
import pandas as pd
from io import StringIO
#from auxiliary import aux
```

Fonte: AUTOR (2022)

Para listar as vulnerabilidades, *Common Vulnerabilities and Exposures* (CVE), a próxima linha de código será responsável por padronizar e facilitar a procura, o acesso e principalmente o compartilhamento desses dados entre os envolvidos.

Figura 10 – Listando as vulnerabilidades

```
In [3]: # CVE com exploit no MISP
relative_path = 'attributes/restSearch'
body = {
    "returnFormat": "json",
    "type": "vulnerability"}

dados = misp.pymisp.direct_call(relative_path, body)
misp_dados = pd.DataFrame(dados['Attribute'])
print('Quantidade de CVE com Exploit disponível: ', len(misp_dados))
misp_dados[['event_id', 'category', 'type', 'value']].head()
```

Quantidade de CVE com Exploit disponível: 145

```
Out[3]:
```

	event_id	category	type	value
0	3	Payload delivery	vulnerability	CVE-2014-0515
1	3	Payload delivery	vulnerability	CVE-2013-7331
2	3	Payload delivery	vulnerability	CVE-2013-2551

Fonte: AUTOR (2022)

Com as vulnerabilidades listadas, foram salvas as informações em “Quantidade de CVE com Exploit disponível” e separados de acordo com o ID dos eventos, sua categoria, o tipo e o respectivo valor.

Figura 11 – Relative_path

```
In [4]: relative_path = 'events/nids/snort/download/'
dados = misp.pymisp.direct_call(relative_path,
                                {"returnFormat": "json", "to_ids": True})
data_pd = pd.json_normalize(dados)
print('Quantidade de linhas de dados = ', len(data_pd))
df = pd.json_normalize(data_pd['Event.Attribute']).loc[0] #Apenas 1 linha de evento

Quantidade de linhas de dados = 1441
```

```
In [5]: df[['category', 'to_ids', 'value']].head()
```

```
Out[5]:
```

	category	to_ids	value
0	Network activity	True	41.190.233.29

Fonte: AUTOR (2022)

Figura 12 – Relative_path

```
In [6]: relative_path = 'attributes/restSearch'
        body = {
            "returnFormat": "json",
            "type": {
                "OR": ["ip-dst", "url"]}
        }
        rules = misp.pymisp.direct_call(relative_path, body)

In [7]: misp_dados = pd.DataFrame(rules['Attribute'])
        print('Hosts maliciosos identificados no MISP = ', len(misp_dados))
        misp_dados[['event_id', 'category', 'type', 'value']].head(50)
```

Fonte: AUTOR (2022)

Figura 13 – Identificando ameaças através dos dados coletados

```
In [7]: misp_dados = pd.DataFrame(rules['Attribute'])
        print('Hosts maliciosos identificados no MISP = ', len(misp_dados))
        misp_dados[['event_id', 'category', 'type', 'value']].head(50)
```

Fonte: AUTOR (2022)

O objetivo das linhas de código acima era listar as vulnerabilidades através dos eventos coletados a fim de padronizar essas informações para identificar possíveis ameaças.

Durante a execução do estudo de caso simulado foram identificados 82.169 hosts maliciosos a partir dos atributos dos eventos que foram listados, o mesmo valor obtido constitui

Figura 14 – Hosts maliciosos identificados

```
Hosts maliciosos identificados no MISP = 82169
```

Out[7]:	event_id	category	type	value
0	2	Network activity	ip-dst	223.25.233.248
1	2	Network activity	ip-dst	196.45.144.12
2	4	Network activity	ip-dst	210.253.101.105
3	4	Network activity	ip-dst	58.64.178.77
4	4	Network activity	ip-dst	211.125.81.203
5	4	Network activity	ip-dst	210.253.96.200
6	4	Network activity	ip-dst	173.255.217.77
7	4	External analysis	ip-dst	210.253.96.200
8	4	External analysis	ip-dst	210.253.99.103
9	4	External analysis	ip-dst	119.205.217.104
10	4	External analysis	ip-dst	96.7.111.133
11	4	External analysis	ip-dst	202.181.133.215
12	4	External analysis	ip-dst	10.0.1.9
13	4	External analysis	ip-dst	121.78.246.174
14	4	External analysis	ip-dst	112.175.143.2
15	4	External analysis	ip-dst	211.125.81.203

Fonte: AUTOR (2022)

A partir desses dados coletados é possível criar regras de segurança cibernética para um firewall que serão utilizados para mitigar ameaças extraídas de bases de Inteligência de Ameaças com hosts maliciosos reais.

4.3 DISCUSSÃO

As informações coletadas pelo MISP foram importantes para o presente estudo porque garantiram que o PyMISP analisasse esses dados e foram observados no ambiente simulado no sistema de contêiner que em um simples experimento o firewall ficou exposto a inúmeros hosts maliciosos que podem comprometer o sistema.

Dessa forma, os dados coletados foram suficientes para criar regras de segurança cibernética para firewall a partir de cada linha de código geradas para mitigar os efeitos colaterais que poderiam ser causados pelos hosts maliciosos encontrados, totalizando 82.169 regras criadas que poderão ser aplicadas em um firewall.

No presente estudo pode-se notar a correlação entre a área de concentração cibernética e de operações militares onde são utilizados inúmeros equipamentos informacionais é possível notar que há uma exposição alta a favor da guerra cibernética inimiga uma vez que não há uma mentalidade ou doutrina no Exército Brasileiro que esteja engajada do mais alto escalão até as pequenas frações.

Através de uma ferramenta de compartilhamento de inteligência de ameaças e aplicação de regras de segurança cibernética através do PyMISP é possível ter bons resultados a serem explorados para garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações que são diariamente despachadas nas ordens de operações, em dados confidenciais, planejamentos e na própria execução.

5 CONSIDERAÇÕES FINAIS

O MISP/PyMISP se configura como uma forma de prevenção efetiva uma vez que é possível compartilhar os eventos de inteligência de ameaças entre diversos órgãos e instituições que trabalham esses dados a fim de aumentar a segurança cibernética garantindo a confidencialidade, integridade, disponibilidade e autenticidade.

O Exército Brasileiro existem diversos setores no ambiente cibernético que precisam ser protegidos e que possuem dados sensíveis às operações que são executadas em todo o território nacional.

É de extrema importância investir em áreas que garantem a proteção cibernética e principalmente permanecer os estudos e ampliando a proteção para todas as áreas incluindo o compartilhamento de dados entre as forças armadas.

Afinal, a cada ano que passa a Guerra Cibernética faz-se presente no campo de batalha. E por ser um ambiente complexo, a doutrina está em constante mudança pois há diversos métodos, meios e vulnerabilidades que possam ser exploradas para prejudicar um alvo importante.

Diante do que foi apresentado, a pesquisa buscou enfatizar que o resultado mais relevante se constitui no fato de que um simples experimento em ambiente controlado é capaz de gerar inúmeros dados maliciosos que podem afetar a integridade de um sistema mal gerenciado e fiscalizado. Negligenciar a proteção de dados em ambientes de incerteza e com vulto informacional pode prejudicar as operações militares podendo vazar dados sigilosos, além de prejudicar a reputação da própria força armada.

Recomendo para o trabalho futuro, indico a aplicação desses estudos durante a Manobra Escolar ou exercícios no terreno. Embora estivesse explícito esse objetivo no escopo, o presente experimento precisou ser adaptado pela falta de recurso, tempo e material a fim de evidenciar a importância de aplicar regras de segurança cibernética em equipamentos de segurança cibernética em operações militares.

REFERÊNCIAS

ANACONDA NAVIGATOR. Disponível em: <<https://anaconda.org/anaconda/anaconda-navigator>>. Acesso em: 13 fev. 2022.

CIRCL.LU. **Glossário MISP**. Disponível em: <<https://www.circl.lu/doc/misp/GLOSSARY.html>>. Acesso em: 29 mar. 2022.

CIRCL.LU. **PYMISP – Biblioteca Python para acessar o MISP**. Disponível em: <<https://www.circl.lu/doc/misp/pymisp/>>. Acesso em: 01 jul. 2021.

CIRCL.LU. **MISP – Plataforma de Inteligência de Ameaças de Código Aberto**. Disponível em: <<https://www.circl.lu/services/misp-malware-information-sharing-platform/>>. Acesso em: 01 jul. 2021.

BRASIL. Ministério da Defesa. **MD35-G-01: Glossário das Forças Armadas**. 2007.

DUTRA, André Melo Carvalhais. **Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto**. Instituto Tecnológico da Aeronáutica. Disponível em: <http://www.sige.ita.br/anais/IXSIGE/Artigos/GE_39.pdf>. Acesso em: 21 jul. 2021.

ESTADOS UNIDOS DA AMÉRICA. Departamento de Defesa (DoD). **Department of Defense Dictionary of Military and Associated Terms**. 2008.

LET'S CODE. **Introdução ao Jupyter Notebook**. 2019. Disponível em: <<https://www.letscode.com.br/blog/introducao-ao-jupyter-notebook>>. Acesso em: 13 fev. 2022.

MALWARE. **Códigos maliciosos**. Disponível em: <<https://cartilha.cert.br/malware/>>. Acesso em: 03 jul. 2021.

MISP. **Feeds Padrão do MISP**. Disponível em: <<https://www.misp-project.org/feeds/>>. Acesso em: 29 mar. 2022.

RED HAT. **API REST**. 2020. Disponível em: <<https://www.redhat.com/pt-br/topics/api/what-is-a-rest-api>>. Acesso em: 01 jul. 2021.

RED HAT. **Docker**. 2018. Disponível em: <<https://www.redhat.com/pt-br/topics/containers/what-is-docker>>. Acesso em: 13 fev. 2022.

SILVA, Júlio Cezar Barreto Leite da. **Guerra Cibernética: A guerra no quinto domínio, conceituação e princípios**. Revista da Escola de Guerra Naval, Rio de Janeiro, v. 20, n. 1, p. 193-211, 2014. Disponível em: <<https://revista.egn.mar.mil.br/index.php/revistadaegn/issue/view/44>>. Acesso em: 13 jul. 2021.

PARKS, Raymon C.; DUGGAN, David P. **Principles of Cyber-warfare**. Proceedings of the IEEE Workshop on Information Assurance, West Point, NY, p 122 – 125, 2001. Trabalho apresentado no Seminário de Segurança da Informação da Academia Militar do Estados Unidos da América, 2001, West Point, NY.