MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
GAB CMT EX – CIE
ESCOLA DE INTELIGÊNCIA MILITAR DO EXÉRCITO

CURSO INTELIGÊNCIA CIBERNÉTICA PARA OFICIAIS

TRABALHO DE CONCLUSÃO DE CURSO (TCC)

O USO DE DISPOSITIVOS IOT EM OPERAÇÕES DE COOPERAÇÃO E COORDENAÇÃO COM AGÊNCIAS: UMA ANÁLISE DA ATUAÇÃO DO OPERADOR DE INTELIGÊNCIA CIBERNÉTICA EM PROL DA CONTRAINTELIGÊNCIA

Brasília
2023

1° Ten **NATHAN** FERREIRA DE OLIVEIRA

O USO DE DISPOSITIVOS IOT EM OPERAÇÕES DE COOPERAÇÃO E COORDENAÇÃO COM AGÊNCIAS: UMA ANÁLISE DA ATUAÇÃO DO OPERADOR DE INTELIGÊNCIA CIBERNÉTICA EM PROL DA CONTRAINTELIGÊNCIA

Trabalho de Conclusão de Curso apresentado à Escola de Inteligência Militar do Exército, como requisito para a obtenção do Grau de Pós-graduação *Lato Sensu* de **Especialização em Inteligência Cibernética.**

Orientador: Maj **DIONÍZIO** SANTOS RODRIGUES DOS ANJOS

Brasília

2023

CATALOGAÇÃO NA FONTE
BIBLIOTECA CEL FORRER GARCIA

O48u Oliveira, Nathan Ferreira de

O uso de dispositivos IoT em operações de cooperação e coordenação com agências: uma análise da atuação do operador de inteligência cibernética em prol da contrainteligência/ Nathan Ferreira de Oliveira – 2023.
24 f.

Orientador: Dionízio Santos Rodrigues dos Anjos
Trabalho de Conclusão de Curso (Especialização em Inteligência Cibernética) - Escola de Inteligência Militar do Exército (EsIMEx), Brasília – DF, 2023.

1. Inteligência Cibernética 2. Dispositivos IoT 3. Segurança Cibernética
4. Contrainteligência I. Título.

1° Ten **NATHAN** FERREIRA DE OLIVEIRA

O USO DE DISPOSITIVOS IOT EM OPERAÇÕES DE COOPERAÇÃO E COORDENAÇÃO COM AGÊNCIAS: UMA ANÁLISE DA ATUAÇÃO DO OPERADOR DE INTELIGÊNCIA CIBERNÉTICA EM PROL DA CONTRAINTELIGÊNCIA

Trabalho de Conclusão de Curso apresentado à Escola de Inteligência Militar do Exército, como requisito para a obtenção do Grau de Pós-graduação *Lato Sensu* de **Especialização em Inteligência Cibernética.**

Aprovado em: 31 de agosto de 2023.

COMISSÃO DE AVALIAÇÃO:

_____

DIONÍZIO SANTOS RODRIGUES DOS ANJOS– Maj **-** Presidente
Escola de Inteligência Militar do Exército

_____

RICARDO CÉLIO CHAGAS **BEZERRA FILHO** - Maj
Escola de Inteligência Militar do Exército

RESUMO

O uso de dispositivos IoT é comum em todas as classes da sociedade. No meio militar sua utilização, apesar de facilitar a realização de diversas atividades importantes, introduz novos riscos para a segurança cibernética, em especial para a segurança da informação em Meios de Tecnologia da Informação e Comunicações (MTIC). Em Operações de Cooperação e Coordenação com Agências (OCCA) esses riscos aumentam ainda mais, isso por conta da diferença no modo de agir das agências no que diz respeito ao tratamento e salvaguarda das informações nas operações. Os operadores de inteligência cibernética são militares especializados nas duas áreas que englobam os novos riscos apresentados: cibernética e inteligência, nesse caso com foco no ramo de contrainteligência. Por esse motivo, e como meio de mitigar esses riscos, este trabalho teve por objetivo geral analisar como o operador de inteligência cibernética pode auxiliar na proteção dos sistemas e informações contra possíveis vulnerabilidades de segurança presentes nos dispositivos IoT dos integrantes das operações de cooperação e coordenação com agências.Para isso o estudo realizou uma pesquisa descritiva, por meio de revisão bibliográfica com abordagem qualitativa e natureza aplicada, o que permitiu a identificação dos principais dispositivos IoT e suas principais vulnerabilidades, bem como a apresentação do funcionamento das operações de cooperação e coordenação com agências, e descreveu as capacidades dos operadores de inteligência cibernética, o que forneceu os subsídios necessários que resultaram no estabelecimento de um compilado de ações a serem propostas e executadas, caso autorizadas, pelo operador envolvido nessas operações, o que significa que os operadores agora possuem um direcionamento quando se depararem com essas situações, que podem facilitar seu assessoramento e aumentar o nível de segurança na operação, colaborando com a contrainteligência. O estudo limitou-se a trabalhar apenas no escopo das OCCA e com a segurança das informações em MTIC, dos próprios MTIC e das redes envolvidas nas operações.

Palavras-chave: Inteligência Cibernética; Dispositivos IoT; Operações de Cooperação e Coordenação com agências; Segurança Cibernética; Contrainteligência.

ABSTRACT

The use of IoT devices is common across all classes of society. In the military environment, its use, despite facilitating the performance of several important activities, introduces new risks to cybersecurity, especially for information security in Information Technology and Communications Means (ITCM). In Operations of Cooperation and Coordination with Agencies (OCCA) these risks increase even more, due to the difference in the way agencies act with regard to the treatment and safeguarding of information in operations. Cyber intelligence operators are military personnel specialized in the two areas that encompass the new risks presented: cybernetics and intelligence, in this case with a focus on the counterintelligence branch. For this reason, and as a means of mitigating these risks, the general objective of this work was to analyze how the cyber intelligence operator can help to protect systems and information against possible security vulnerabilities present in IoT devices of members of operations of cooperation and coordination with agencies. For this, the study carried out a descriptive research, through a bibliographical review with a qualitative approach and applied nature, which allowed the identification of the main IoT devices and their main vulnerabilities, as well as the presentation of the behavior of operations of cooperation and coordination with agencies, and described the capabilities of cyber intelligence operators, which provided the necessary subsidies that resulted in the establishment of a compilation of actions to be proposed and executed, if authorized, by the operator involved in these operations, which means that the operators now have a direction when faced with these situations, which can facilitate their advice and increase the level of security in the operation, collaborating with counterintelligence. The study was limited to working only within the scope of the OCCA and with the security of information in the ITCM, the ITCM themselves and the networks involved in the operations.

Keywords: Cyber Intelligence. IoT devices. Operations of Cooperation and Coordination with agencies. Cyber Security. Counter-intelligence.

SUMÁRIO

1 INTRODUÇÃO

Analisando a tecnologia IoT, pode-se enxergá-la como as duas faces de uma moeda. De um lado tornou a vida mais fácil, sem esforço e menos restrita, do outro as intrusões nesses ambientes, principalmente com intuito de obter de dados pessoais, cresce rapidamente (SHARMA, 2018).

Dentro do Exército Brasileiro, a obtenção de dados é uma das fases do ciclo da inteligência que garante que a função de combate inteligência cumpra o objetivo de satisfazer as necessidades de conhecimento do comando (BRASIL, 2015a).

Quando no espectro cibernético, é responsabilidade da Inteligência Cibernética (CYBINT) realizar a obtenção desses dados, protegidos ou não. Convém ressaltar que se caracteriza como espaço virtual aquele que contém dispositivos computacionais inseridos na rede, por onde passam, trafegam ou são processadas informações digitais (BRASIL, 2015b).

O ramo da contrainteligência é o ramo da Inteligência responsável por impedir que ações hostis de qualquer natureza comprometam dados, informações, conhecimentos e sistemas a eles relacionados (BRASIL, 2019).

> A Contrainteligência é, também, uma das atividades da Função de Combate Proteção. Nesse sentido, todas as considerações constantes deste manual querem sejam de guerra ou não guerra, devem ser observadas durante as operações militares (BRASIL, 2019).

No contexto das operações militares, o trabalho delimitou seu tema nas operações de cooperação e coordenação com agências. Essas operações são executadas em apoio aos órgãos ou instituições governamentais ou não, militares ou civis, públicos ou privados, nacionais ou internacionais (BRASIL, 2017).

Neste tipo de operação, o emprego da tropa é limitado no espaço e tempo, a liberdade de ação do comandante é regida pela norma legal que autorizou o emprego da tropa (BRASIL, 2017).

Relacionando os conceitos apresentados, tem-se por objetivo do trabalho analisar como o operador de inteligência cibernética pode auxiliar na proteção dos sistemas e informações contrapossíveis vulnerabilidades de segurança presentes nos dispositivos IoT dos integrantes das operações de cooperação e coordenação com agências.

Com intuito de atingir o objetivo do trabalho, 4 (quatro) objetivos específicos foram definidos:

- Descrever o que são os dispositivos IoT;
- Elencar os principais problemas de segurança para as operações de cooperação e coordenação com agências que podem surgir com a utilização de dispositivos IoT por parte dos integrantes da operação;
- Descrever o que são as operações de cooperação e coordenação com agências; e
- Analisar as capacidades de atuação do operador de inteligência cibernética inseridos nessas operações.

Para isso será utilizado o método de pesquisa descritiva, com a finalidade de analisar as possibilidades de ação do operador de inteligência cibernética dentro do contexto dos riscos de segurança advindos do uso de dispositivos IOT e das operações de cooperação e coordenação com agências. Esse estudo será realizado por meio de revisão bibliográfica composta de artigos, manuais e dissertações que englobam os temas necessários para atingir os objetivos da pesquisa.

O trabalho fará uso de abordagem qualitativa, com foco na coleta de dados de estudos documentais, buscando entender como o cuidado com os riscos dos dispositivos IOT pode se relacionar com a atividade desempenhada pelos operadores de inteligência cibernética e com as operações de cooperação e coordenação com agências.

A natureza da pesquisa é essencialmente aplicada, onde será realizada a técnica de análise documental sobre os dados coletados, buscando confrontá-los com objetivo de desenvolver um modus operandi para os militares com o curso de inteligência cibernética que participarem de operações de cooperação e coordenação com agências que se encontrem expostas as vulnerabilidades oriundas dos dispositivos IOT.

Em síntese, o estudo será composto pela introdução, que resume sucintamente o trabalho e a metodologia empregada; pelo desenvolvimento, que abordará respectivamente em seus três capítulos os dispositivos IoT, as operações de cooperação e coordenação com agências e as capacidades dos operadores de Inteligência Cibernética; e por uma conclusão onde será apresentada uma proposta

de modus operandi para o operador de Inteligência Cibernética com intuito de auxiliar o ramo de contrainteligência e padronizar ações mitigadoras mínimas possíveis de serem empregadas genericamente nessas operações.

2 DISPOSITIVOS IoT

Os dispositivos IoT são objetos físicos incorporados a sensores, softwares e outras tecnologias com a possibilidade de conectar e trocar dados com outros dispositivos e sistemas pela internet, abrangem uma grande diversidade de dispositivos que vão de objetos domésticos a ferramentas industriais (ORACLE, 2023).

Para que se compreenda melhor os dispositivos IoT e suas possíveis vulnerabilidades, faz-se necessário uma breve introdução ao conceito da tecnologia IoT, seu funcionamento e os principais dispositivos encontrados.

2.1 O que é a internet das coisas (IoT)?

> Internet das Coisas (IoT) é uma tecnologia relativamente nova que tem despertado a atenção dos sistemas de informação acadêmicos e empresariais nos últimos anos. A Internet das Coisas estabelece uma rede que permite que dispositivos inteligentes em um sistema de informação organizacional se conectem uns aos outros e troquem dados com o armazenamento central (GAURAV et al., 2023)

Figura 1 – Internet das coisas

Fonte: BABOS (2020).

“A Internet das Coisas permite que pessoas e coisas estejam conectadas a qualquer hora, em qualquer lugar, com qualquer coisa, com qualquer outra pessoa e idealmente usando qualquer caminho/rede e qualquer serviço” (GUILLEMIN; FRIESS, 2009 *apud* PINHEIRO, 2018, p. 25).

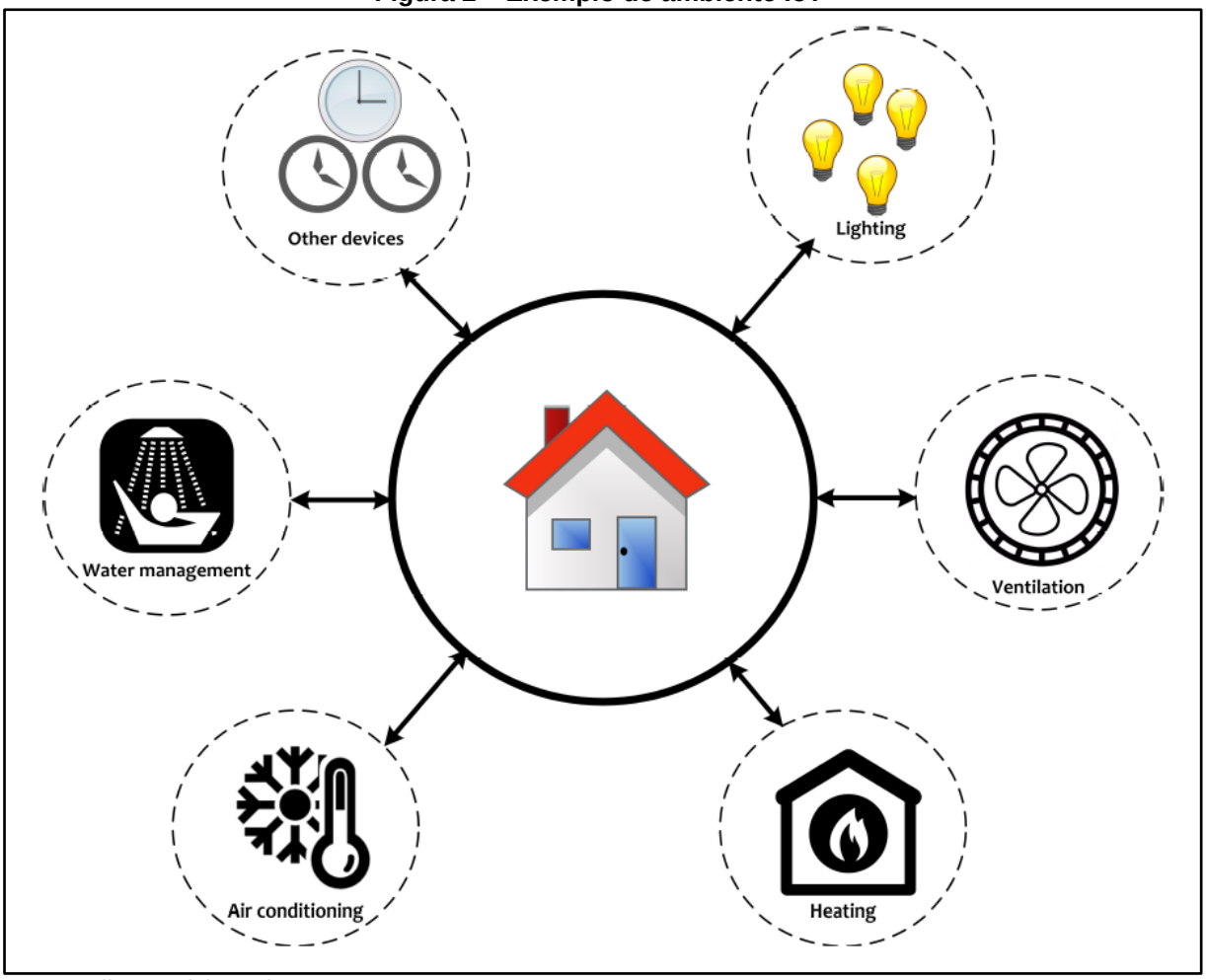
Apesar de o termo IoT ser relativamente recente, já na década de 1970 o conceito de conectar computadores e redes para monitorar e controlar dispositivos era utilizado no monitoramento remoto de medidores de rede elétrica por meio das linhas telefônicas. Na década de 1990, os avanços tecnológicos nas redes sem fio permitiram o início da utilização da tecnologia *Machine to Machine* (M2M) (ROSE *et al.*, 2015).

A comunicação M2M é uma tecnologia que permite que um grande número de dispositivos inteligentes possam se comunicar e tomar decisões colaborativas sem intervenção humana, de maneira autônoma, com a finalidade de alcançar melhor eficiência no gerenciamento de tempo e custo (Chen; Li; 2012 *apud* VERMA *et al.*, 2016)

Segundo Waher (2015) a capacidade da internet das coisas de realizar aprendizagem *Machine to Machine* e a possibilidade de integrar todos os dispositivos que integram o ambiente simultaneamente faz com que a IoT possa ser considerada como o futuro da internet.

Existem quatro modelos mais comuns de comunicação utilizados nas conexões IoT: dispositivo para dispositivo, dispositivo para nuvem, dispositivo para gateway e compartilhamento de dados de *back-end*. A diversidade de maneiras que os IoT podem realizar suas conexões destacam a flexibilidade desses sistemas (ROSE *et al.*, 2015).

Figura 2 – Exemplo de ambiente IoT



Fonte: Ali; Awad (2018).

No campo político, a IoT pode reduzir o tempo e o custo das atividades humanasrelacionadas à gestão de serviços públicos. A inovação da IoT em serviços públicos ajudaráa administração pública a substituir as estruturas tradicionais pela orquestração de serviços IoT em busca da resolução de problemas importantes (WIRTZ *et al.*, 2019 *apud* HU *et al.*, 2022).

2.2 Principais dispositivos IoT

Segundo Hosain (2018), os dispositivos mais populares de uso geral se dividem em três categorias. A primeira é a casa conectada, onde estão incluídos os termostatos inteligentes, lâmpadas inteligentes, fechaduras inteligentes, câmeras inteligentes, entre outros dispositivos conectados. A segunda categoria é a dos vestíveis (do inglês, *wearables*) que englobam os *smartwatches*, rastreadores de

atividades fitness e óculos inteligentes. Já a terceira categoria é a do carro conectado, onde se encontram os controles remotos do carro, navegação de viagem e diagnósticos inteligentes.

Em contrapartida, a Simplilearn (2020) divide os dispositivos IoT em dispositivos sensores e dispositivos gerais. Os dispositivos sensores são aqueles que têm por função realizar algum tipo de medição através de um sensor, eles enquadram os sensores de umidade, sensores de luz, sensores de calor, entre outros. Já os dispositivos gerais são onde se enquadram aparelhos de uso geral que com a evolução da tecnologia foram automatizados através da conexão com a internet, estão inclusos na categoria os *smartwatches*, geladeiras, televisões e todos os dispositivos inteligentes que integram uma casa e não possuem funções sensor.

2.3 Segurança dos dispositivos IoT

É difícil para os desenvolvedores incorporarem *softwares* de segurança nos dispositivos IoT, por conta das restrições de *hardware* que possuem. Por esse motivo, proteger o tráfego gerado por esses dispositivos torna-se a opção mais viável (XIN et al., 2022).

Na tentativa de minimizar esse problema com o menor impacto no *hardware* desses dispositivos, Jammula et al. (2022) propuseram a utilização do método criptografia leve (do inglês *lightweight cryptography*, ou LWC) em conjunto com a criptografia baseada em atributo (do inglês *Attribute-based encryption*, ou ABE). Em suas pesquisas concluíram que o método LWC-ABE se provou flexível e útil na eliminação de ataques gerados no ambiente IoT, ao mesmo tempo que reduziu os recursos necessários em hardware, como o consumo de energia.

Já quanto a ataques de negação de serviço (DoS, do inglês Denial of Service) Syed et al. (2020) propuseram um sistema de detecção de ataques DoS que trabalham com o protocolo de Transporte de telemetria de enfileiramento de mensagens(MQTT, do inglês *Message Queuing Telemetry Transport*) que é um protocolo de camada de aplicativo adequado para comunicações M2M que tem por função permitir que um dispositivo intermediário roteie mensagens apenas para os dispositivos que tenham acesso e/ou necessitem dela.

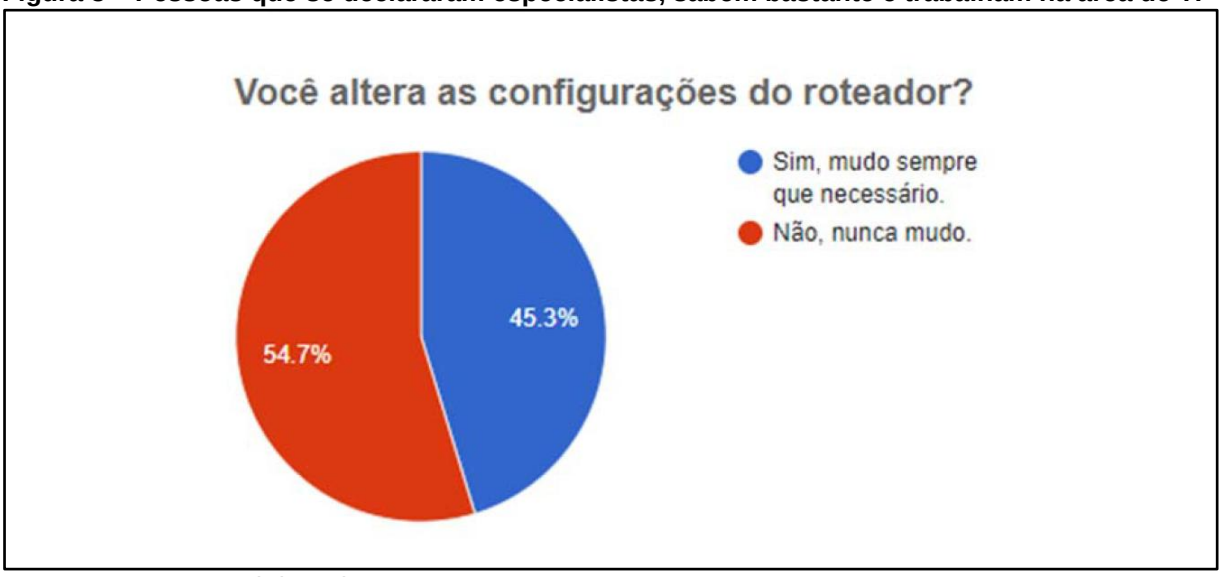
Devido ao objetivo e as características desse protocolo, este costuma ser o principal vetor de ataques de negação de serviço, por isso desenvolveram um *framework* que analisa o tráfego de dados do dispositivo IoT e foi capaz de identificar quando o tráfego deixa de ser normal e passa a ser um possível caso de DoS (SYED *et al.*, 2020).

Estudos sobre o cuidado com a privacidade dos dados pessoais também foram realizados e concluíram que:

> Confirmamos que a preocupação com a privacidade foi um antecedente significativo na determinação da intenção de divulgação de informações, mesmo no ambiente IoT em que a coleta e o uso de informações pessoais são indispensáveis. No entanto, a confiança no prestador de serviços funcionou como a variável mais importante, o que também foi confirmado em pesquisas recentes (SAH; JUN, 2023, tradução nossa).

Ambientes com dispositivos IoT podem facilmente ter seus dados coletados e consequentemente serem invadidos. Câmeras e alarmes podem ser desativados via Wi-Fi. Os roteadores podem ser considerados vetores de entrada, por isso sua segurança deve ser sempre verificada, já que através dele podem ocorrer roubos de informações e exposição de privacidade, entretanto não é isso que foi verificado no estudo, conforme verificado na figura abaixo(PEREIRA *et al.*, 2022).

Figura 3 – Pessoas que se declararam especialistas, sabem bastante e trabalham na área de TI



Fonte: PEREIRA *et al*. (2022)

Além dos sistemas de segurança que vem sendo desenvolvidos, esforços também vêm sendo feitos para regularizar juridicamente as mudanças geradas pela

IoT e seus dispositivos. Nesse contexto, Chiara (2022) desenvolveu um estudo analisando em que nível a legislação existente na União Europeia (UE) abrange os múltiplos desafios na proteção da IoT.

Este estudo concluiu que a complexidade do ambiente IoT em conjunto com o receio de sufocar o mercado por parte dos países integrantes da União Europeia, fizeram com que as regulamentações de segurança nesses ambientes a princípio fossem de cunho voluntário, entretanto a expansão das superfícies de ataque e a complexidade com que as ameaças cibernéticas vêm evoluindo fizeram com que o bloco começasse a reagir, mesmo que por enquanto ainda seja de maneira insipiente (CHIARA, 2022).

Com base nos dados apresentados, quando se analisa os dispositivos IoT em um contexto militar pode-se afirmar que estes são possíveis fontes de vazamento de informações, portanto é essencial que durante as operações esses dispositivos sejam monitorados e controlados, em especial nas operações de coordenação e cooperação com agências que incluem elementos de outras Forças, órgãos e instituições que possuem maneiras de agir e/ou níveis de preocupação com contrainteligência diferentes do que se possui no Exército.

Por esse motivo faz-se necessário que se traga para este estudo a definição, as características e as particularidades das operações de cooperação e coordenação com agências.

3 OPERAÇÕES DE COOPERAÇÃO E COORDENAÇÃO COM AGÊNCIA (OCCA)

As operações de Cooperação e Coordenação com Agências (OCCA) são definidas como:

> São operações executadas por elementos do EB em apoio aos órgãos ou instituições (governamentais ou não, militares ou civis, públicos ou privados, nacionais ou internacionais), definidos genericamente como agências. Destinam-se a conciliar interesses e coordenar esforços para a consecução de objetivos ou propósitos convergentes que atendam ao bem comum. Buscam evitar a duplicidade de ações, a dispersão de recursos e a divergência de soluções, levando os envolvidos a atuarem com eficiência, eficácia, efetividade e menores custos (BRASIL, 2017).

Nas últimas décadas a doutrina de emprego da Força terrestre evoluiu constantemente no que diz respeito a atuação integrada do Exército com as agências. Muito desta evolução advém do emprego de tropa em apoio à segurança pública a partir da ECO 92, aliado a participação de contingentes militares em operações de paz multidimensionais. Esses eventos proporcionaram o aproveitamento de lições aprendidas e formou a base doutrinária necessária para as operações de cooperação e coordenação com agências (TEIXEIRA, 2021).

A dinâmica do conflito moderno fez com que os Estados se desafiassem em busca de soluções que se adaptem a esse ambiente. Por conta da complexidade das operações, evidenciou-se que a atuação isolada das Forças Armadas já não era suficiente para atingir os objetivos traçados. É nesse ponto que a inserção de outras agências nestas operações se apresentou como uma ferramenta eficaz na resolução do problema (MARTINS, 2021).

Figura 4 – Exemplos de agências envolvidas nas OCCA

Fonte: BRASIL (2017)

As OCCA normalmente ocorrem nas situações de não guerra e se subdividem em 7 tipos de operação:garantia dos poderes constitucionais;garantia da lei e da ordem;atribuições subsidiárias; prevenção e combate ao terrorismo; sob a égide de organismos internacionais; em apoio à política externa em tempo de paz ou crise; e outras operações em situação de não guerra (BRASIL, 2017).

Dentre as características dessas operações destacam-se: a coordenação com outros órgãos governamentais e/ou não governamentais; a combinação de esforços políticos, militares, econômicos, ambientais, humanitários, sociais, científicos e tecnológicos; o fato de que não há subordinação entre as agências e, sim, cooperação e coordenação;e a influência de atores não oficiais e de indivíduos sobre as operações (BRASIL, 2017).

No contexto internacional a necessidade de atualização de doutrina e abandono da antiga mentalidade de guerra linear também é notável. Os Estados Unidos da América publicaram o *Pamphlet 525-92* que trouxe novos conceitos a

respeito desse novo terreno onde os exércitos têm operado e na identificação de ameaças. Nesse novo cenário foi incluída às operações básicas das forças terrestres de todo o mundo as OCCA, com as ressalvas jurídicas específicas de cada país (TEIXEIRA, 2021).

Em 2016 a Colômbia criou a Doutrina Damasco, que reformulou sua doutrina militar e reforçou a necessidade de sincronização entre as forças, agências e instituições governamentais, enfatizando a tendência de aumento dessas operações dentro do país (TEIXEIRA, 2021).

As informações obtidas mostram que a integração entre as forças armadas e as agências vem aumentando não apenas no Brasil, mas em todo o mundo. Apesar de benéfica para o cumprimento dos objetivos, novos riscos podem surgir com a inclusão de integrantes com mentalidades diferentes relativas à contrainteligência, em particular no que diz respeito a dispositivos IoT.

Nesse contexto, como medida mitigadora desses riscos, é importante a atuação do operador de inteligência cibernética em prol da contrainteligência. Para que se defina como devem atuar, faz-se necessária a apresentação das capacidades que esses militares possuem.

4 CAPACIDADES DO OPERADOR DE INTELIGÊNCIA CIBERNÉTICA

A Inteligência Cibernética é definida como:

> A Inteligência Cibernética (Cyber Intelligence - CYBINT) é a Inteligência elaborada a partir de dados, protegidos ou não, obtidos no espaço cibernético. Este, por sua vez, é caracterizado como o espaço virtual composto por dispositivos computacionais conectados em rede, onde informações digitais trafegam, são processadas ou armazenadas (BRASIL, 2015b).

Os operadores de inteligência cibernética necessitam possuir diversas capacidades no que diz respeito a análise e levantamento de riscos e vulnerabilidades, aqui serão apresentadas as mais relevantes para o cumprimento dos objetivos propostos no trabalho.

Segundo MOTA *et al.* (2014), o operador pode: “realizar pesquisas e avaliar a Inteligência Cibernética de todas as fontes para desenvolver uma análise aprofundada e uma avaliação sobre as ameaças às redes críticas e infraestruturas críticas”.

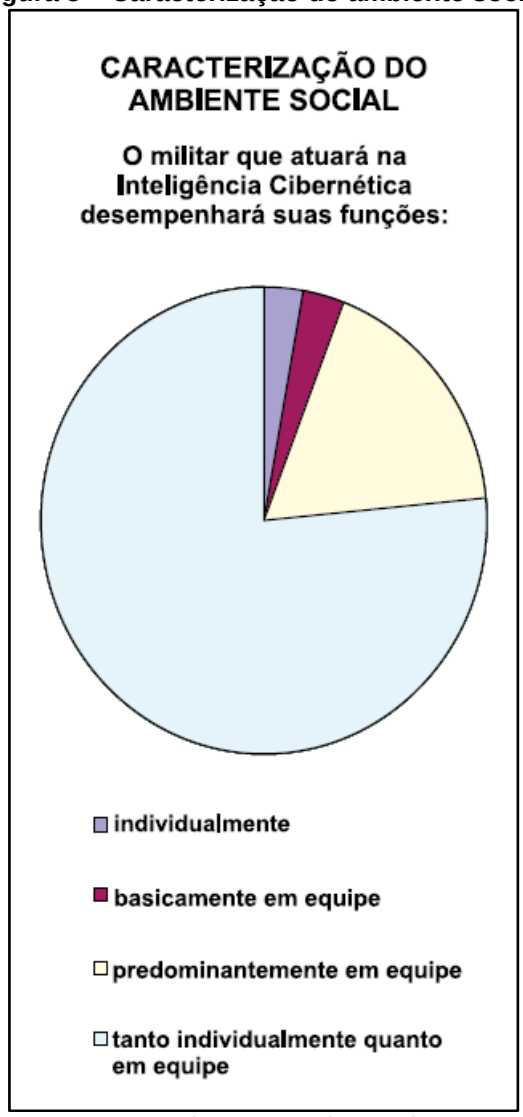
O militar pode trabalhar junto com outros profissionais técnicos, forenses e de gestão de incidentes, buscando uma melhor compreensão das intenções, objetivos e atividades de atores em ameaças cibernéticas (MOTA *et al.*, 2014).

Possui a capacidade de analisar eventos de rede e determinar o impacto sobre as operações atuais de um possível vazamento, bem com realizar pesquisas em todas as fontes para determinar a possível intenção do inimigo (MOTA *et al.*, 2014).

Pode confeccionar análises de perfis de ameaças cibernéticas em eventos atuais, com base em pesquisas em fontes de informações classificadas e abertas (MOTA et al., 2014).

No geral os operadores desempenham suas funções tanto em equipe quanto individualmente, conforme identificado na figura abaixo:

Figura 5 – Caracterização do ambiente social



Fonte: (MOTA *et al*., 2014)

Com isso, verifica-se que o operador de inteligência cibernética deve ser versátil, flexível e possuir nível de conhecimento elevado em sua área de atuação, tais capacidades fornecem as condições necessárias para que executem diversas ações em prol da contrainteligência no que se relaciona com o problema de estudo.

5 CONCLUSÃO

Com base na revisão bibliográfica apresentada, e para que se cumpra o objetivo deste trabalho, foi desenvolvido um compilado de ações que podem ser propostas e, caso autorizadas, executadas pelos operadores de inteligência cibernética visando reduzir o risco à segurança da informação que advém do uso de dispositivos IoT em OCCA.

Para esse desenvolvimento levou-se em consideração todos os dados levantados no trabalho, desde o funcionamento dos dispositivos IoT, seus principais representantes e suas vulnerabilidades mais comuns, passando pelo entendimento do funcionamento das OCCA e culminando com as capacidades apresentadas pelos operadores de inteligência cibernética.

É importante ressaltar que as ações que serão apresentadas não esgotam as possibilidades de atuação do operador, servindo, de maneira geral, como base para incrementar a segurança das informações sujeitas a vazamentos por meio de possíveis dispositivos IoT não seguros. Essas ações podem e devem ser complementadas e/ou alteradas de acordo com a criatividade do operador, necessidade e particularidade da operação.

Com base nas possíveis vulnerabilidades de segurança apresentadas no desenvolvimento, foram definidas como ações sugeridas para evitá-las:

- Propor confecção de documento com regras de restrições de uso de dispositivos IoT durante a operação.
- Propor o estabelecimento política de bloqueio de acesso à rede para dispositivos que não possuam o MAC cadastrado junto ao responsável pela rede.
- Propor a programação de script de escaneamento de rede periódico para analisar possíveis dispositivos não autorizados.
- Propor a criação e escala diária para a realização da análise do tráfego de rede na(s) rede(s) da operação.
- Propor estabelecimento de barreiras de segurança como revistas antes da entrada em locais de realização de *briefings*, videoconferências e reuniões, com intuito de evitar a entrada de dispositivos IoT com capacidade de gravação de áudio e vídeo.

- Propor a proibição de instalação e utilização de câmeras IoT, exceto se autorizados por autoridade competente.
- Propor o bloqueio de portas USB dos computadores e notebooks da operação, utilizar servidor de compartilhamento de arquivos em uma rede interna segregada da internet para transferência de documentos classificados.
- Propor utilização de detector de metais, quando possível, para acesso as dependências utilizadas na operação.
- Propor a implantação de *Intrusion Detection System* (IDS) e *Intrusion Prevention System* (IPS) nas redes da operação, se possível, visando prevenir o vazamento de informações pela rede, bem como a possibilidade de analisar os logs do que foi vazado caso o problema venha a ocorrer.
- Propor a não utilização de redes Wi-Fi, sempre que possível, nas operações.
- Documentar e relatar toda e qualquer alteração ou descumprimento de qualquer uma das medidas.

Estas ações trazem à tona a resposta ao problema de pesquisa apresentado, indicando de maneira prática ações que quando executadas pelos operadores de inteligência cibernética fornecem um aumento significativo de segurança aos sistemas e informações nas OCCA.

De maneira geral, entende-se que os dispositivos IoT já são uma realidade em todos os postos e graduações dentro das Forças Armadas, bem como em todas as funções dentro das agências, por esse motivo em que pese a facilidade advinda dos dispositivos, o aumento da carga sobre a contrainteligência, em especial no que diz respeito à segurança da informação aumenta consideravelmente, exigindo de todos os integrantes consciência e cuidado no tratamento de dados relevantes.

REFERÊNCIAS

ALI, Bako; AWAD, Ali Ismail. Cyber and physical security vulnerability assessment for IoT-based smart homes. **Sensors (Switzerland)**, v. 18, n. 3, p. 1–17, 2018.

BABOS, Flávio. **O Que é Internet das Coisas e 13 Exemplos da Tecnologia**. 2020. Disponível em: https://flaviobabos.com.br/internet-das-coisas/. Acesso em: 12 abr. 2023.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **Contrainteligência**. Manual de campanha EB70-MC-10.220. 1. ed. Brasília, DF, 2019.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **Operações**. Manual de campanha EB70-MC-10.223. 5. ed. Brasília, DF, 2017.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **Planejamento e Emprego da Inteligência Militar**. Manual de Campanha EB70-MC-10.307. 1. Ed. Brasília, DF, 2016.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. **Inteligência**. Manual de campanha EB20-MC-10.207. 1. ed. Brasília, DF, 2015a.

BRASIL. Exército Brasileiro. Estado-Maior. Port Normativa nº 229/MD, de 28 de janeiro de 2013. MD33-M-12: **Operações Interagências**. Brasília, DF, 2012.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. **Inteligência Militar Terrestre**. Manual de fundamentos EB20-MF-10.107. 2. ed. Brasília, DF, 2015b.

CHIARA, Pier Giorgio. The IoT and the new EU cybersecurity regulatory landscape. **International Review of Law, Computers and Technology**, v. 36, n. 2, p. 118–137, 2022. Disponível em: https://doi.org/10.1080/13600869.2022.2060468. Acesso em: 13 abr. 2023.

GAURAV, Akshat; GUPTA, Brij B.; PANIGRAHI, Prabin Kumar. A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. **Enterprise Information Systems**, v. 17, n. 3, 2023. Disponível em: https://doi.org/10.1080/17517575.2021.2023764. Acesso em: 13 abr. 2023.

HOSAIN, Syed. THE INTERNET OF THINGS FOR BUSINESS. **Aeris**, v. 3, p. 212, 2018. Disponível em: http://info.aeris.com/iotguide2016?__hstc=36218495.c514c06aee8637610d59af873e2ffa76.1478190164697.1478190164697.1478190164697.1&__hssc=36218495.1.1478190164698&__hsfp=1175851494&hsCtaTracking=e17cea34-0773-4513-b717-88d56a584e86%7C44281ef5-e277-4cb9-9b65-. Acesso em: 13 abr. 2023.

HU, Guangwei; CHOHAN, Sohail Raza; LIU, Jianxia. Does IoT service orchestration in public services enrich the citizens' perceived value of digital society? **Asian**

Journal of Technology Innovation, v. 30, n. 1, p. 217–243, 2022. Disponível em: https://doi.org/10.1080/19761597.2020.1865824. Acesso em: 13 abr. 2023.

JAMMULA, Mounika; VAKAMULLA, Venkata Mani; KONDOJU, Sai Krishna. Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system. **Connection Science**, v. 34, n. 1, p. 2431–2447, 2022. Disponível em: https://doi.org/10.1080/09540091.2022.2124957. Acesso em: 13 abr. 2023.

MARTINS, Victor. **Operação de cooperação e coordenação com agências:** descrição do modelo pitcic para a obtenção da consciência situacional do comandante tático. 2021. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) - Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2021.

MOTA, Marcel; REZENDE, Claubert; GONÇALVES, Marco Aurélio. O Perfil do Militar de Inteligência Cibernética. **A Lucerna**, p. 17–34, 2014.

ORACLE. **O que é IoT?** Disponível em: https://www.oracle.com/br/internet-of-things/what-is-IoT/#:~:text=A%20Internet%20das%20Coisas%20(IoT)%20descreve%20a%20rede%20de%20objetos,comuns%20a%20ferramentas%20industriais%20sofisticadas.. Acesso em: 10 abr. 2023.

PEREIRA, Jheniffer; SENO, Gabriel; OLIVEIRA, Rogério. **Segurança E Privacidade Na Internet Das Coisas**. p. 14, 2022.

PINHEIRO, Alexander. **A influência da internet das coisas para a guerra cibernética**. 2018. Trabalho de Conclusão de Curso (Bacharel em Ciências Militares) - Academia Militar das Agulhas Negras, Rio de Janeiro, 2018. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/4575. Acesso em: 20 abr. 2023.

ROSE, Karen; ELDRIDGE, Scott; CHAPIN, Lyman. **T**he Internet of Things (IoT): An Overview. **Int. Journal of Engineering Research and Applications**, v. 5, n. 12, p. 71–82, 2015. Disponível em:https://crsreports.congress.gov. Acesso em: 20 abr. 2023.

SAH, Jeeyeon; JUN, Sangmin. The Role of Consumers' Privacy Awareness in the Privacy Calculus for IoT Services. **International Journal of Human–Computer Interaction**, v. 0, n. 0, p. 1–12, 2023. Disponível em: https://doi.org/10.1080/10447318.2023.2184102. Acesso em: 20 abr. 2023.

SHARMA, Deeksha. **Internet of Things:** An umbrella of technologically progressive and cynical outlooks. 1. ed. [S.l: s.n.], 2018. v. 1.

SIMPLILEARN. **What is IoT ?** Disponível em: https://www.youtube.com/watch?v=6mBO2vqLv38. Acesso em: 20 abr. 2023.

SYED, Naeem Firdous et al. Denial of service attack detection through machine learning for the IoT. **Journal of Information and Telecommunication**, v. 4, n. 4, p.

482–503, 2020. Disponível em: https://doi.org/10.1080/24751839.2020.1767484. Acesso em: 20 abr. 2023

TEIXEIRA, Carlos. Operações de Cooperação e Coordenação com Agências e Operações de Guerra Integrando a doutrina. **Revista Exército Brasileiro**, v. 157, p. 3–11, 2021.

VERMA, Pawan Kumar et al. Machine-to-Machine (M2M) communications: A survey. **Journal of Network and Computer Applications**, v. 66, p. 83–105, 1 Mai 2016.

WAHER, Peter. **Learning Internet of Things**. 1. ed. [S.l.]: Packt Publishing, 2015.

XIN, Liu et al. TCN enhanced novel malicious traffic detection for IoT devices. **Connection Science**, v. 34, n. 1, p. 1322–1341, 2022. Disponível em: https://doi.org/10.1080/09540091.2022.2067124.Acesso em: 20 abr. 2023.