Departamento de Engenharia Informática e de Sistemas
Instituto Superior de Engenharia de Coimbra
Instituto Politécnico de Coimbra

Licenciatura em Engenharia Informática

Curso Engenharia Informática

Ramo de Sistemas de Informação

Unidade Curricular de Ética e Deontologia

Ano Lectivo de 2024/2025

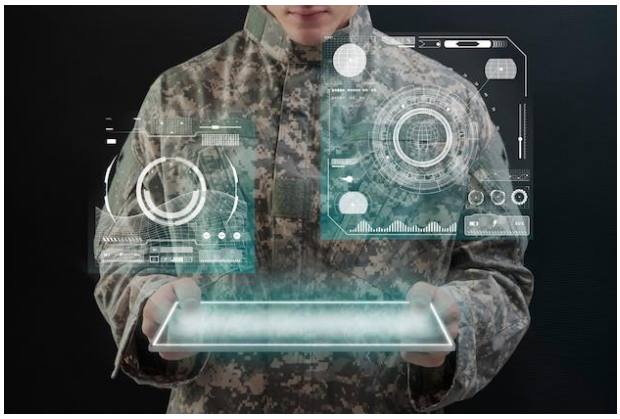
PALESTRA Nº 3

Cyber Threat Intelligence - Implicações táticas e operacionais

Major Rui Filipe Santos

Realizada em 26 de março de 2025

CYBER THREAT INTELLIGENCE: DESAFIOS, ESTRATÉGIAS E COOPERAÇÃO INTERNACIONAL



João Pedro Silveira da Costa

Número de Aluno: 2022143368

Coimbra, 01 de abril de 2025

João Pedro Silveira da Costa

Cyber Threat Intelligence: Desafios, Estratégias e Cooperação Internacional

Ética e Deontologia

Coimbra, 01 de abril de 2025

Índice

RESUMO

O presente relatório versa sobre a palestra proferida pelo Major Rui Filipe Santos, subordinada ao tema da Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence) e às suas repercussões nos planos tático e operacional. Procede-se a uma análise da evolução do ciberespaço enquanto domínio estratégico, das diferenças essenciais entre cibersegurança e ciberdefesa, bem como da estrutura da inteligência cibernética. Adicionalmente, foram debatidos desafios de ordem jurídica, o impacto das tecnologias emergentes, a experiência prática no seio da NATO e a relevância da cooperação internacional. Este relatório tem como objetivo apresentar uma análise crítica e aprofundada dos temas abordados, destacando a crescente importância da ciberdefesa para a segurança global.

Palavras-chave: Ciberdefesa, Inteligência de Ameaças Cibernéticas, Ciberespaço, NATO, Inteligência Artificial.

1. INTRODUÇÃO

No âmbito da unidade curricular de Ética e Deontologia, realizou-se a conferência intitulada "Cyber Threat Intelligence e as suas Implicações Táticas e Operacionais", organizada pelo Professor Jorge Barbosa e apresentada pelo Major Rui Filipe Santos, representante do Comando de Operações de Ciberdefesa. Este relatório tem como objetivo resumir e analisar criticamente os principais conteúdos abordados. A palestra destacou a segurança digital e o papel das forças armadas na proteção do ciberespaço, discutindo como a inteligência cibernética pode enfrentar as ameaças do mundo digital.

O relatório apresenta os tópicos fundamentais, como o desenvolvimento do ciberespaço enquanto área estratégica, as diferenças entre cibersegurança e ciberdefesa, e as implicações da inteligência de ameaças cibernéticas (CTI). Também explora os desafios éticos, legais e tecnológicos associados. A ciberdefesa é vista como crucial para a soberania nacional e a estabilidade internacional, exigindo não apenas competências técnicas, mas também planeamento estratégico e cooperação global para lidar com ameaças digitais em constante evolução.

O documento está dividido em quatro capítulos:

1. **Introdução**: Explica o tema da conferência, a sua relevância e os objetivos do relatório, detalhando a estrutura para facilitar a compreensão.

2. **Desenvolvimento Temático**: Analisa os tópicos apresentados pelo Major Rui Santos, como a história do ciberespaço, a inteligência de ameaças cibernéticas, os desafios legais e o papel da inteligência artificial.

3. **Perspetiva Crítica**: Faz uma análise fundamentada, relacionando os pontos abordados na palestra com investigações adicionais.

4. **Conclusões**: Reflete sobre os temas explorados, avaliando o papel da CTI na segurança global e resumindo os principais pontos da análise.

O Major Santos salientou que a ciberdefesa deve ser considerada uma área multidisciplinar, abrangendo aspetos técnicos, táticos, operacionais e estratégicos. O relatório analisa questões como a dificuldade em atribuir ciberataques devido ao anonimato, o uso de inteligência artificial tanto em ataques como em defesas, e a necessidade de quadros legais sólidos, como os desenvolvidos pela NATO e as diretrizes europeias. A experiência prática do Major oferece perspetivas reais que ilustram a aplicação dos conceitos teóricos em cenários operacionais.

2. Descrição do Tema Abordado na Palestra

2.1. Diferença entre cibersegurança e ciberdefesa

A distinção entre cibersegurança e ciberdefesa é fundamental para a compreensão das estratégias de proteção no ciberespaço. Enquanto a cibersegurança se concentra na prevenção e mitigação de vulnerabilidades tecnológicas, a ciberdefesa alarga este conceito ao incorporar uma abordagem pró-ativa e estratégica, visando a proteção de infraestruturas críticas e a resposta coordenada a ameaças cibernéticas, muitas vezes conduzidas por Estados.

No decurso da sessão, foi enfatizada a distinção entre estes dois domínios. O Major Santos esclareceu que a cibersegurança se traduz na implementação de medidas técnicas e procedimentais destinadas a garantir a proteção de redes, sistemas e dados contra ameaças como malware, phishing e ransomware. Esta abordagem, predominante no setor privado, assenta em três princípios essenciais: confidencialidade, integridade e disponibilidade da informação. Como exemplos concretos, foram mencionados os sistemas de firewall empresariais, os mecanismos de deteção de intrusão implementados por instituições financeiras e a autenticação multifatorial utilizada em plataformas digitais.

Por sua vez, a ciberdefesa foi caracterizada como uma disciplina de carácter militar que transcende a simples proteção passiva, adotando uma postura ofensiva e estratégica no ciberespaço. Recorrendo à analogia entre o escudo (cibersegurança) e a lança (ciberdefesa), o Major destacou o uso de operações cibernéticas ofensivas, tais como a exploração de vulnerabilidades desconhecidas (zero-day exploits) e o desenvolvimento de malware específico para neutralizar infraestruturas adversárias. Um exemplo ilustrativo mencionado foi a desativação de radares inimigos através de ataques cibernéticos, precedendo operações militares convencionais.

A ciberdefesa encontra-se, assim, intrinsecamente ligada à salvaguarda da soberania nacional e à dissuasão de potenciais adversários. O Major Rui Filipe Santos referiu que a utilização de campanhas de desinformação, frequentemente articuladas com operações físicas, tem sido um instrumento relevante em contextos de conflito, como se verificou na guerra na Ucrânia. Foi igualmente sublinhado que, enquanto a cibersegurança está ao alcance de entidades privadas, a ciberdefesa exige recursos altamente especializados, incluindo analistas de inteligência e infraestruturas militares avançadas. Para além disso, foi abordada a crescente importância da cooperação internacional na ciberdefesa, evidenciada pela formação de alianças estratégicas entre países com vista ao desenvolvimento de capacidades conjuntas e à implementação de respostas coordenadas a ataques de grande escala.

Foi ainda observado que a fronteira entre cibersegurança e ciberdefesa tem vindo a tornar-se menos distinta, dado que técnicas inicialmente exclusivas da ciberdefesa têm sido progressivamente incorporadas na cibersegurança, nomeadamente a análise preditiva de ameaças. O Major concluiu a sua intervenção recorrendo a uma metáfora esclarecedora: enquanto a cibersegurança protege o "castelo digital", a ciberdefesa assegura a integridade de todo o "reino". Esta evolução demonstra a crescente interdependência entre ambas as áreas e sublinha a necessidade de uma abordagem integrada, envolvendo entidades civis e militares, para garantir a segurança e resiliência do ciberespaço nacional e internacional.

2.2. O Ciberespaço como Quinto Domínio Estratégico

O ciberespaço foi reconhecido como o quinto domínio estratégico, complementando os tradicionais domínios terrestre, marítimo, aéreo e espacial. Esta evolução reflete a crescente interdependência das infraestruturas digitais nas sociedades modernas e a necessidade de garantir a sua segurança e resiliência. Um ataque cibernético pode comprometer infraestruturas críticas, incluindo sistemas financeiros, redes de transporte e comunicação governamental, podendo, em casos extremos, ter impactos comparáveis aos de um conflito militar convencional.

A NATO reconheceu oficialmente o ciberespaço como domínio operacional na Cimeira de Varsóvia de 2016, consolidando a sua relevância estratégica. O Major Santos caracterizou o ciberespaço como um ambiente virtual de caráter global, dinâmico e acessível a uma ampla variedade de atores, desde Estados-nação a grupos organizados e indivíduos isolados. A dificuldade de atribuição das ameaças cibernéticas torna este domínio particularmente complexo, exigindo abordagens inovadoras para prevenção, defesa e dissuasão.

Um exemplo notável da utilização do ciberespaço para fins ofensivos foi o ciberataque contra a Estónia em 2007, que resultou na paralisação de serviços bancários, redes de transporte e comunicação governamental por várias semanas. Este ataque, amplamente atribuído a grupos de hackers russos, destacou a vulnerabilidade das infraestruturas digitais e impulsionou a criação do Centro de Excelência de Ciberdefesa Cooperativa (CCDCOE), sediado em Tallinn. Embora não pertença oficialmente à NATO, este centro tornou-se um polo de investigação e formação na área da ciberdefesa.

A NATO tem vindo a reforçar progressivamente a sua abordagem ao domínio cibernético. A Cimeira de Lisboa de 2010 marcou um ponto de viragem, colocando o ciberespaço no centro da estratégia de segurança coletiva da Aliança. Em 2014, procurou-se alinhar as operações cibernéticas com os princípios do direito internacional humanitário, e em 2018, a criação do Cyberspace Operations Center reforçou a capacidade da NATO para responder a ameaças cibernéticas. Casos recentes, como os ataques ao sistema elétrico ucraniano em 2015 e 2016, que resultaram em cortes de energia generalizados, ilustram o potencial destrutivo das operações cibernéticas.

O Major Santos salientou que o ciberespaço é hoje um elemento transversal a todas as operações militares modernas. Desde a segurança das comunicações por satélite até ao funcionamento de aeronaves não tripuladas, a dependência de infraestruturas digitais é crescente. Foi exemplificado como uma missão terrestre pode estar dependente de dados cibernéticos para traçar rotas seguras, sendo que uma falha neste domínio pode comprometer toda a operação. Adicionalmente, abordou-se o mecanismo de Contributos Voluntários de Efeitos Cibernéticos (CEVA), que permite aos Estados-membros da NATO disponibilizar capacidades específicas para ataques cibernéticos, sem que a organização intervenha diretamente. Esta abordagem reflete o desafio de conciliar a soberania nacional com a necessidade de cooperação internacional no combate às ameaças cibernéticas.

Dada a crescente sofisticação das ameaças cibernéticas, é imperativo continuar a investir no desenvolvimento de mecanismos preventivos e dissuasores. A cooperação entre os Estados e organizações internacionais revela-se essencial para a construção de um ecossistema de cibersegurança robusto, capaz de enfrentar os desafios emergentes deste novo cenário de conflito.

2.3. O que é Cyber Threat Intelligence

A inteligência de ameaças cibernéticas (Cyber Threat Intelligence - CTI) constitui uma abordagem essencial para a antecipação, localização e mitigação de ataques no domínio digital. A sua aplicação permite que organizações, tanto do setor público como privado, desenvolvam estratégias de defesa baseadas em informações concretas sobre potenciais ameaças e vulnerabilidades. O objetivo primordial da CTI é transformar dados dispersos em inteligência acionável, capacitando as entidades para uma tomada de decisão informada e proativa.

A CTI pode ser segmentada em três categorias fundamentais:

- Inteligência Estratégica: Orientada para a alta gestão, fornece uma visão abrangente do panorama de ameaças e das tendências emergentes, auxiliando na formulação de políticas e estratégias de cibersegurança a longo prazo.

- Inteligência Tática: Centrada na identificação de táticas, técnicas e procedimentos (TTPs) utilizados por agentes maliciosos, permitindo um alinhamento eficaz das medidas de defesa.

- Inteligência Operacional: Visa a monitorização contínua do ambiente cibernético para deteção e resposta em tempo real a atividades suspeitas, minimizando impactos adversos sobre sistemas e infraestruturas críticas.

2.4. Cyber Threat Intelligence: Estrutura e Áreas de Especialização

A CTI é estruturada em diversas etapas que compreendem a recolha, análise e disseminação de informação útil para a segurança cibernética. O processo segue três fases principais:

1. **Recolha de Dados Brutos:** Inclui a obtenção de informações a partir de múltiplas fontes, tais como registos de rede, artefactos de malware, relatórios de inteligência e conteúdos de redes sociais.
2. **Transformação de Dados em Informação Estruturada:** Implica a correlação de eventos, identificação de padrões de ataque e categorização de ameaças para facilitar a sua interpretação e utilização.
3. **Produção de Inteligência Acionável:** Consiste na elaboração de relatórios e previsões fundamentadas que suportam a tomada de decisão informada, permitindo o reforço das defesas organizacionais.

Adicionalmente, a CTI abrange diversas subáreas especializadas, nomeadamente:

- **Technical Intelligence** – Análise detalhada das tecnologias e ferramentas empregues por agentes maliciosos, incluindo malware, exploits e infraestruturas utilizadas em campanhas de ataque.
- **Financial Intelligence** – Monitorização de transações financeiras ilícitas, rastreamento de fluxos monetários suspeitos e análise do uso de criptomoedas em atividades criminosas.
- **Social Media Intelligence** – Vigilância e análise de conteúdos partilhados em redes sociais para detetar desinformação, antecipar ameaças e monitorizar tendências comportamentais.
- **Transportation Intelligence** – Identificação de padrões de movimentação de indivíduos ou recursos, particularmente em contextos de segurança nacional e operações militares.
- **Blockchain Intelligence** – Investigação de transações em redes blockchain para deteção de esquemas de lavagem de dinheiro, financiamento ilícito e outras atividades suspeitas.

A relevância da CTI na proteção de infraestruturas críticas e cadeias de fornecimento foi também destacada, sublinhando a necessidade de abordagens colaborativas entre entidades governamentais, privadas e organizações internacionais. A implementação de tecnologias avançadas, como inteligência artificial e machine learning, tem vindo a potenciar a eficácia da CTI, proporcionando análises mais precisas e aumentando a capacidade de antecipação de ameaças. Assim, a integração de mecanismos de partilha de inteligência entre setores constitui um fator determinante para a resiliência e segurança no espaço cibernético.

2.5. Implicações, Riscos e Consequências Táticas e Operacionais

Os ataques cibernéticos representam uma ameaça crescente às infraestruturas digitais, podendo provocar desde interrupções em serviços financeiros até a paralisação de setores críticos, como saúde e energia. Estes incidentes comprometem não apenas a segurança e o bem-estar de um Estado, mas também a sua estabilidade económica e política. Além dos prejuízos financeiros diretos, os ataques podem afetar a confiança do público nas instituições e nas empresas, desencadeando crises sistémicas que se propagam por toda a sociedade. A crescente interconectividade global e a sofisticação das ameaças exigem a adoção de estratégias robustas de Cyber Threat Intelligence (CTI) para a mitigação de riscos e para a resposta eficaz a incidentes.

As implicações práticas da Cyber Threat Intelligence podem ser analisadas em três níveis distintos:

- **Tático:** Engloba a identificação e disseminação de indicadores de compromisso (IOCs) e técnicas, táticas e procedimentos (TTPs) utilizados por agentes maliciosos. Esta abordagem permite a resposta imediata a incidentes, como a mitigação de ataques de negação de serviço distribuída (DDoS) e a neutralização de ameaças antes que causem danos significativos. A automação e a inteligência artificial têm desempenhado um papel cada vez mais relevante na deteção e contenção de ataques em tempo real.

- **Operacional:** Diz respeito à monitorização contínua de campanhas cibernéticas, à análise de ameaças emergentes e à utilização de modelos estruturados, como a Cyber Kill Chain, para antecipação de ações adversárias. A recolha e correlação de dados de diversas fontes possibilitam a identificação de padrões de ataque, permitindo às equipas de segurança atuar preventivamente e com maior precisão.

- **Estratégico:** Abrange a elaboração de análises aprofundadas que orientam a tomada de decisões de longo prazo no âmbito da segurança cibernética. A proteção de infraestruturas críticas, como redes de energia, transportes e telecomunicações, depende de políticas públicas eficazes e de uma estreita colaboração entre entidades governamentais e o setor privado. A partilha de informação sobre ameaças e vulnerabilidades é essencial para fortalecer a resiliência nacional e garantir uma defesa cibernética integrada e eficiente.

Esta estrutura evidencia a importância da Cyber Threat Intelligence, desde a resposta técnica até à formulação de estratégias nacionais. O Major destacou que a eficácia da CTI reside na articulação dinâmica entre capacidades tecnológicas e operações humanas, sendo essencial uma abordagem colaborativa entre os setores público e privado para a mitigação das ameaças cibernéticas. A constante evolução do panorama digital exige uma adaptação contínua das estratégias de defesa, assegurando que os Estados e as organizações estejam preparados para enfrentar desafios cada vez mais sofisticados.

2.6. Desafios Jurídicos e Dilemas Éticos na Ciberdefesa

O Major Rui Santos abordou, na sua intervenção, os desafios jurídicos e dilemas éticos inerentes às operações de ciberdefesa, destacando as dificuldades decorrentes da inexistência de um enquadramento legal plenamente consolidado. Sublinhou que, apesar dos avanços legislativos a nível europeu, como a Diretiva DORA (Digital Operational Resilience Act), o atual quadro normativo permanece insuficiente para dar resposta eficaz às ameaças cibernéticas emergentes. A necessidade de um acompanhamento jurídico contínuo revela a fragilidade das normativas existentes, o que acentua a complexidade da atuação neste domínio.

Um dos aspetos mais críticos mencionados foi a exclusão das atividades de ciberdefesa do âmbito de aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD) por razões de segurança nacional. Tal exceção permite a monitorização e recolha de dados sem as restrições impostas ao setor privado. No entanto, este regime levanta importantes questões éticas, uma vez que a legalidade dessas operações não dissipa as incertezas relativas ao seu enquadramento político e moral. Assim, o estabelecimento de regras de empenhamento claras torna-se essencial para garantir a legitimidade das ações conduzidas neste contexto. O Major referiu ainda que, apesar da reconhecida competência nacional evidenciada nos exercícios da NATO, a implementação prática das normativas continua a apresentar desafios significativos, ultrapassando muitas vezes o previsto nos documentos doutrinários.

Outro desafio relevante prende-se com a dificuldade em atribuir responsabilidades por ataques cibernéticos. O uso de intermediários e técnicas de dissimulação, como as chamadas "falsas bandeiras", dificulta substancialmente a identificação dos perpetradores, o que, aliado à morosidade da resposta política e jurídica, coloca os agentes de ciberdefesa em desvantagem face a adversários que operam sem restrições normativas. A ausência de um mecanismo eficaz de atribuição de autoria compromete não apenas a resposta imediata a tais incidentes, mas também a aplicação de sanções internacionais adequadas.

Adicionalmente, foi enfatizada a necessidade de equilibrar a proteção digital com o respeito pelos direitos e liberdades fundamentais dos cidadãos. A definição de limites operacionais para as forças de ciberdefesa continua a ser uma questão central, pois qualquer medida que vise reforçar a segurança nacional não pode comprometer garantias essenciais como a privacidade e a liberdade de expressão.

O Major Rui Santos alertou ainda para a inexistência de princípios éticos bem estabelecidos no âmbito da ciberdefesa, tornando-se evidente que as fronteiras entre o que é legal e o que é moral permanecem indefinidas. Embora novas diretivas europeias possam vir a mitigar estas lacunas, a incerteza normativa continua a representar um desafio tanto no plano técnico como no plano ético. O avanço tecnológico e a constante evolução das ameaças cibernéticas exigem um esforço contínuo na adaptação e regulamentação, de modo a garantir um equilíbrio entre a eficácia operacional e a salvaguarda dos valores democráticos.

Deste modo, a ciberdefesa enfrenta não apenas desafios operacionais e técnicos, mas também um panorama jurídico e ético em constante transformação. O reforço do enquadramento normativo, aliado a um debate contínuo sobre os princípios éticos que devem reger esta área, revela-se essencial para garantir uma atuação eficaz e legitimada, alinhada com os valores fundamentais do Estado de direito.

2.7. Potencial da Inteligência Artificial

A utilização da Inteligência Artificial (IA) na ciberdefesa tem-se revelado um instrumento crucial para a deteção precoce e resposta célere a incidentes cibernéticos, contribuindo significativamente para a redução do tempo de reação e mitigação de danos. Durante a intervenção, o Major destacou o papel da IA no combate à manipulação de informação, respondendo a uma questão do público sobre o impacto das tecnologias emergentes na cibersegurança.

Foi salientado que os avanços tecnológicos têm facilitado a criação e disseminação de conteúdos falsificados, como vídeos manipulados, tornando cada vez mais desafiante a distinção entre informação verídica e adulterada. Como forma de mitigar esta problemática, mencionou-se a utilização de ferramentas especializadas na análise de metadados, nomeadamente a verificação da origem, localização e dispositivo de gravação, com vista à validação da autenticidade dos ficheiros multimédia. Adicionalmente, foi evidenciada a relevância de plataformas open source para a deteção de incongruências, tais como a identificação de vídeos que alegam ter sido captados numa determinada localidade, mas cujos metadados não correspondem à geolocalização indicada.

No entanto, reconheceu-se a inexistência de soluções infalíveis. Com a contínua evolução da IA, a identificação de conteúdos manipulados torna-se progressivamente mais complexa, potenciando riscos acrescidos para a soberania dos Estados. Alguns países já iniciaram o desenvolvimento de infraestruturas digitais autónomas da Internet pública como estratégia de mitigação dessas ameaças, ainda que tal abordagem possa ter implicações nas liberdades civis.

No que concerne a outras tecnologias emergentes, foi enfatizado o potencial do blockchain enquanto ferramenta para assegurar a rastreabilidade e integridade da informação. Esta tecnologia poderá desempenhar um papel fundamental na mitigação dos desafios associados à falsificação de dados e ao cumprimento de requisitos regulatórios. Não obstante, foi sublinhado que, no atual contexto, a estratégia de ciberdefesa permanece alicerçada na verificação meticulosa de conteúdos individuais, recorrendo aos recursos tecnologicamente disponíveis.

2.8. Importância da Cooperação Internacional e a Atuação da NATO

A cooperação internacional desempenha um papel preponderante na resposta a ciberataques de grande escala, sendo a NATO uma das principais entidades a promover uma abordagem colaborativa nesse domínio. Durante a conferência, destacou-se a importância da atuação coordenada entre países aliados para reforçar a resiliência digital e mitigar ameaças no ciberespaço.

O Major referiu o papel fundamental do CCDCOE, localizado na Estónia, como centro de referência para treino e investigação na área da cibersegurança. Além disso, salientou a relevância do Cyberspace Operations Center, criado em 2018, que tem a missão de coordenar as ações digitais da NATO e garantir uma resposta eficaz a incidentes cibernéticos.

A nível nacional, voltou a destacar o grupo G4 como um mecanismo essencial para a partilha de informações e definição de estratégias conjuntas, especialmente no combate à desinformação em períodos eleitorais. Nesse contexto, mencionou o Centro Europeu de Cibersegurança (ECCC), ainda em fase inicial, como uma estrutura com grande potencial para fortalecer a articulação entre os Estados-Membros da União Europeia no âmbito da ciberdefesa.

Embora a NATO não execute diretamente ações ofensivas no ciberespaço, pode solicitar contribuições voluntárias de países aliados por meio do mecanismo CEVA (Cyber Effects Voluntary Contributions). Essa abordagem reforça a capacidade de resposta coletiva e permite a mobilização de recursos especializados para enfrentar desafios emergentes.

Além disso, sublinhou-se a importância da utilização de redes seguras e rádios de campanha como soluções tecnológicas para garantir a comunicação em ambientes onde o acesso à Internet é limitado. Essas estratégias refletem a necessidade de uma coordenação eficiente e de uma infraestrutura robusta para lidar com ameaças globais no domínio digital.

2.9. Estudos de Caso e Perspetivas da NATO

No decurso da palestra, o Major Santos apresentou casos concretos da aplicação da Cyber Threat Intelligence no Comando de Operações de Ciberdefesa e no contexto da NATO. Foram salientadas a utilização de ferramentas como CrowdStrike, VirusTotal, Recorded Future e Maltego, bem como a aplicação do modelo Cyber Kill Chain para a análise de ameaças e a partilha de informação entre analistas. Destacou-se, igualmente, a relevância das redes classificadas, nomeadamente a SNS One da NATO e a rede nacional portuguesa, que se encontram isoladas da Internet pública por motivos de segurança.

Os casos práticos analisados ilustraram o impacto real das ciberameaças e evidenciaram o papel determinante da NATO na coordenação e formulação de políticas de ciberdefesa a nível global. Um dos exemplos referidos foi a substituição da aplicação Signal por uma alternativa mais segura, a plataforma KIQ, baseada em tecnologia Web3, na sequência da identificação de uma vulnerabilidade crítica na versão para computador da Signal. Adicionalmente, mencionou-se o recurso a ferramentas como OnionShare na dark web para a transferência de dados em zonas remotas, sendo clarificado que tal prática se destina exclusivamente a informação não classificada.

A nível nacional, foi apresentado o grupo G4, constituído pelo Comando de Ciberdefesa, Polícia Judiciária, Serviço de Informações de Segurança (SIS) e Centro Nacional de Cibersegurança, como um exemplo de colaboração institucional eficaz. Este grupo tem como uma das suas funções a monitorização das redes sociais em períodos eleitorais, visando a mitigação de ameaças associadas à desinformação. Além disso, foi evidenciado o contributo do Cooperative Cyber Defence Centre of Excellence (CCDCOE), sediado na Estónia, como uma instituição de referência na formação e capacitação de especialistas na área da cibersegurança, beneficiando da experiência do país na resposta a ciberameaças.

O envolvimento da NATO na ciberdefesa é, igualmente, evidenciado pela sua participação em exercícios internacionais, como o Locked Shields, promovido pelo CCDCOE, considerado o maior e mais complexo exercício de ciberdefesa a nível mundial. Estas iniciativas têm como objetivo testar a resiliência das infraestruturas críticas e aperfeiçoar os mecanismos de coordenação entre os estados-membros. Adicionalmente, a NATO tem vindo a reforçar a colaboração com entidades do setor privado e instituições académicas, com vista ao desenvolvimento de soluções inovadoras para a deteção e mitigação de ameaças cibernéticas.

Desta forma, a NATO reitera o seu compromisso com a segurança digital global, promovendo uma abordagem integrada que combina avanços tecnológicos, formação especializada e um forte espírito de cooperação internacional.

2.10. Classificação de Atores Maliciosos e Tipos de Ameaças Cibernéticas

As ciberameaças podem ser conduzidas por diferentes atores, incluindo Estados-nação, grupos ativistas (hacktivistas), redes criminosas organizadas, terroristas e ameaças internas, cada um com objetivos distintos e muitas vezes sobrepostos.

O Major procedeu a uma categorização dos principais tipos de ameaças e atores ativos no ciberespaço, identificando cinco grandes grupos:

1. **Atores estatais** – motivados por interesses geopolíticos e estratégicos, frequentemente visando espionagem, desestabilização de infraestruturas críticas ou influência em processos políticos de outros países.

2. **Cibercriminosos** – orientados por objetivos financeiros, utilizando técnicas como ransomware, fraude digital e roubo de credenciais para obter ganhos monetários.

3. **Hacktivistas** – impulsionados por ideologias políticas ou sociais, utilizando ataques cibernéticos como forma de protesto ou para expor vulnerabilidades institucionais.

4. **Grupos terroristas** – que recorrem ao ciberespaço para fins ideológicos e operacionais, como recrutamento, propaganda e ataques digitais para desestabilização de sistemas.

5. **Ameaças internas/desafiadores** – indivíduos que, por descontentamento, interesse pessoal ou desejo de afirmação técnica, podem comprometer segurança organizacional ou governamental.

O Major assinalou que essas categorias nem sempre são estanques e podem se interligar, dificultando a atribuição clara de responsabilidades. Por exemplo, grupos norte-coreanos podem combinar motivações criminosas com objetivos estatais, enquanto atores não estatais podem agir sob contrato de governos. Essa complexidade justifica os esforços de organizações como a NATO para desenvolver um novo manual que classifique e compreenda essas ameaças de forma mais rigorosa e multidimensional, permitindo uma resposta mais eficaz e coordenada no combate ao cibercrime e aos ataques digitais.

3. Análise Crítica

A palestra ministrada pelo Major Rui Filipe Santos, centrada na Cyber Threat Intelligence (CTI) e nas suas repercussões a nível tático e operacional, proporcionou uma abordagem aprofundada e pragmática sobre o papel do ciberespaço na segurança contemporânea, especialmente no domínio militar e no contexto da NATO. Este relatório procura desenvolver uma análise crítica sobre os principais temas abordados, nomeadamente a evolução do ciberespaço como quinto domínio operacional, a distinção entre cibersegurança e ciberdefesa, os desafios legais e éticos e a integração de tecnologias emergentes, como a inteligência artificial.

Um dos pontos mais relevantes da palestra foi a ênfase na transversalidade do ciberespaço e na sua interligação com os domínios convencionais (terrestre, marítimo, aéreo e espacial). O Major ilustrou esta interdependência com o exemplo do ciberataque à Estónia em 2007, que evidenciou o potencial do ciberespaço para comprometer infraestruturas críticas nacionais. Concordo com esta visão, considerando que o ciberespaço transcendeu a sua função de apoio tático para se tornar um fator determinante na eficácia operacional dos restantes domínios. Um ataque informático capaz de comprometer comunicações militares pode inviabilizar uma operação, demonstrando a necessidade imperativa de integrar a ciberdefesa nas doutrinas militares modernas. No entanto, questiono se os Estados com menor capacidade tecnológica estão devidamente preparados para enfrentar esta realidade, uma vez que a dependência de infraestruturas digitais pode acentuar assimetrias entre atores estatais e não estatais.

Outro aspeto de relevo na palestra foi a distinção entre cibersegurança e ciberdefesa. Enquanto a primeira se foca na proteção passiva de sistemas e dados, a segunda assume uma dimensão estratégica e, potencialmente, ofensiva, alinhada com os interesses nacionais. Esta diferenciação é essencial para compreender a natureza dual do ciberespaço, tanto como meio de defesa quanto de projeção de poder. No entanto, considero que essa separação pode, por vezes, ser excessivamente estanque. O exemplo da Microsoft, que desenvolveu operações ofensivas contra redes botnets, demonstra que entidades privadas estão a atuar em domínios tradicionalmente reservados aos Estados. Esta tendência suscita uma questão fundamental: deverá o setor privado desempenhar um papel mais ativo na ciberdefesa? A falta de um enquadramento legal claro, conforme salientado pelo Major, torna esta questão ainda mais complexa e exige um debate aprofundado sobre as implicações jurídicas e políticas dessa possibilidade.

No que concerne aos desafios éticos e legais, estes representam um dos principais entraves ao desenvolvimento da ciberdefesa. A exceção do Regulamento Geral sobre a Proteção de Dados (RGPD) em operações de interesse nacional e a necessidade de decisões rápidas por parte dos decisores políticos ilustram o delicado equilíbrio entre eficácia operacional e responsabilidade democrática. Embora reconheça que o uso de proxies e de operações de bandeira falsa possa dificultar a atribuição de ataques, não considero esta barreira intransponível. O avanço da investigação forense digital e a cooperação internacional, como a promovida pelo Centro de Excelência para a Defesa Cibernética Cooperativa (CCDCOE), têm permitido avanços significativos na identificação de atores mal-intencionados, como demonstrado na atribuição do ataque NotPetya à Rússia em 2017. No entanto, o fator político continua a ser um obstáculo considerável, especialmente em democracias onde a transparência e a prestação de contas são elementos fundamentais.

Em conclusão, a palestra proporcionou uma abordagem esclarecedora sobre a

complexidade da Cyber Threat Intelligence, evidenciando tanto os progressos alcançados como os desafios que persistem na ciberdefesa. A perspetiva operacional partilhada pelo Major constitui um contributo valioso para a compreensão desta realidade em constante evolução. No entanto, o desenvolvimento sustentado desta área dependerá de uma síntese eficaz entre inovação tecnológica, legislação adequada e uma cooperação internacional genuinamente funcional, capaz de conciliar o poder digital com a responsabilidade coletiva.

4. Considerações Finais

A conferência ministrada pelo Major Rui Filipe Santos, subordinada ao tema da Cyber Threat Intelligence (CTI) e das respetivas implicações táticas e operacionais, realizada no dia 26 de março de 2025, constituiu uma oportunidade valiosa para aprofundar a compreensão da ciberdefesa como uma área em rápida evolução e um elemento essencial da segurança contemporânea. A exposição do Major, sustentada pela sua experiência no Comando de Operações de Ciberdefesa e no seio da NATO, proporcionou uma perspetiva pragmática que interligou os fundamentos teóricos com a aplicação operacional, demonstrando o ciberespaço como um domínio estratégico e destacando os desafios dele decorrentes.

A apresentação foi estruturada de forma clara, iniciando-se com a contextualização do ciberespaço como quinto domínio operacional, conceito formalizado na Cimeira de Varsóvia (2016), ilustrado através do caso paradigmático do ataque à Estónia (2007). Seguidamente, procedeu-se à análise das distinções entre cibersegurança e ciberdefesa, às diversas vertentes da CTI e aos desafios jurídicos e éticos subjacentes. A abordagem, sustentada por exemplos concretos, como a utilização de ferramentas como CrowdStrike e a monitorização de redes sociais para manter a perceção situacional (situational awareness), demonstrou de que forma a teoria se traduz em prática operacional. Embora de forma sucinta, a discussão acerca do impacto da inteligência artificial e do blockchain apontou direções de evolução que merecem um acompanhamento atento. Todos estes elementos reforçam a crescente relevância da ciberdefesa num contexto em que as ameaças digitais comprometem diretamente a soberania dos Estados e o quotidiano dos cidadãos.

Numa abordagem crítica, reconhece-se o mérito da palestra na forma como conjugou a perspetiva histórica com a dimensão operacional. No entanto, algumas fragilidades são dignas de nota. A ênfase colocada na inexistência de uma legislação específica e nas dificuldades inerentes à atribuição de ataques cibernéticos constitui um ponto pertinente, contudo, não foram exploradas em profundidade soluções alternativas para além das diretivas já mencionadas, como a DORA. A exclusão do RGPD em cenários de ciberdefesa é compreensível do ponto de vista operacional, mas suscita questões éticas relevantes: até que ponto será lícito comprometer direitos e liberdades individuais em prol da segurança nacional? A abordagem aos perfis de ameaças, como cibercriminosos e hacktivistas, revelou-se esclarecedora, mas não contemplou de forma aprofundada a crescente interseção entre diferentes motivações e alianças, como as colaborações entre a Coreia do Norte e redes criminosas, o que levanta a questão da adequação dos modelos de classificação tradicionais à realidade atual.

A postura pragmática do Major, refletida na substituição do Signal devido a vulnerabilidades e na adoção da ferramenta KIQ baseada em Web3, demonstra agilidade operacional, mas também revela uma dependência de soluções tecnológicas emergentes que ainda não foram amplamente validadas. A colaboração com a NATO e o G4 representa um avanço significativo, contudo, a exclusividade militar da Escola de Ciberdefesa e a ausência de percursos acessíveis para civis ou estagiários perpetuam um défice de diversidade nos perfis formados para enfrentar ameaças globais. Considera-se que a ciberdefesa deveria assentar numa abordagem mais inclusiva e colaborativa, incentivando a participação de instituições académicas e do setor privado. Embora esta temática tenha sido brevemente mencionada, apenas se materializou na recomendação de cursos especializados, como os da SANS.

Em síntese, a palestra evidenciou que a CTI se constitui como um dos pilares centrais da segurança internacional contemporânea. Contudo, a sua eficácia futura dependerá da capacidade de superar desafios legais, éticos e tecnológicos. A visão apresentada pelo Major Rui Filipe Santos, que alia a experiência operacional ao conhecimento estratégico, representa um contributo significativo para o debate, embora beneficiasse de um enquadramento mais abrangente e integrador.

REFERÊNCIAS

[1] R. F. Santos, Interviewee, *Cyber Threat Intelligence e suas Implicações Táticas e Operacionais.* [Entrevista]. 26 março 2025.

[2] NATO, "Warsaw Summit Communiqué," 2016 julho 8. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_133169.htm. [Acedido em 1 abril 2025].

[3] European Union, "Regulation (EU) 2022/2554 on Digital Operational Resilience (DORA)," 14 dezembro 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj. [Acedido em 1 abril 2025].

[4] CCDCOE, "The 2007 Cyber Attacks Against Estonia," Cooperative Cyber Defence Centre of Excellence, Tallinn, Estônia, 2008.

ANEXOS