Ciberdefesa – Uma componente de Segurança

Capitão-de-mar-e-guerra
Helder Fialho de Jesus

1. Introdução

O ciberespaço tem mudado a forma como nos relacionamos na sociedade dos dias de hoje, seja no contexto do indivíduo, das organizações, das empresas ou do Estado. Por outro lado, também eliminou diversas barreiras, como a geográfica, pois as distâncias físicas são irrelevantes, ou a temporal, onde a questão dos fusos horários perderam relevância. Daí a expressão "à distância de um clique".

Conforme refere o General Medina[1], provavelmente, o impacto do ciberespaço sobre a humanidade, hoje, é maior do que a invenção da impressão no século XV. Assim, o ciberespaço permite uma diversidade enorme de atividades, sendo que muitas estão associadas ao desenvolvimento social e económico, mas outras decorrem de interesses maléficos para a nossa sociedade. Estas últimas estão associadas a atores que se aproveitam da facilidade de anonimato que o ciberespaço permite, a sensação de impunidade, bem como da dificuldade de imputação, o que por sua vez prejudica a ação das forças que zelam pela proteção dos seus cidadãos, empresas e País. O caráter assimétrico e disruptivo das ações que podem ser efetuadas também é uma caraterística particular do ciberespaço, o que torna mais complexa a ação de proteção.

Numa visão mais abrangente, relembram-se as declarações do Secretário-geral das Nações Unidas, Engenheiro António Guterres, que constituem um alerta importante ao

afirmar que uma próxima guerra será precedida de um ciberataque[2], e que se verifica alguma falta de regras para as atividades dos Estados no ciberespaço. Hoje, vive-se num mundo mais competitivo, multipolar, onde a natureza complexa do sistema global tem criado condições para que os Estados possam ter certo tipo de atuações, as quais noutros tempos seriam definidas como de guerra.

O desenvolvimento tecnológico, em diversas áreas, permite encontrar soluções para a complexidade que o ciberespaço apresenta, particularmente, no que diz respeito ao campo de batalha. Nestas, encontra-se a inteligência artificial, mas cuja aplicação terá de ser estudada profundamente, face aos potenciais efeitos benéficos e maléficos que daqui poderão advir para a humanidade, bem como às implicações éticas que poderá ter.

Com este artigo pretende dar-se a conhecer um pouco o assunto em título, que é complexo e com muitas variáveis. Tendo em vista ajudar a compreender a equivalência dos efeitos na sociedade decorrentes de ações no ciberespaço, são também apresentados alguns exemplos comparativos com o mundo físico. Num próximo artigo serão apresentados desafios de futuro à ciberdefesa, dando continuidade à presente exposição.

2. Ameaças

No ciberespaço, como em qualquer outro domínio da vida, importa ter-se o conhecimento das vulnerabilidades próprias. No presente contexto, de sistemas e ciberespaço, pode estabelecer-se que uma vulnerabilidade constitui uma fraqueza passível de ser explorada para daí se tirarem vantagens, cuja forma de operar decorre geralmente de forma remota, sem perceção da vítima. A exploração de vulnerabilidades também já em tempos foi abordada por Sun Tzu, no seu livro a "Arte da Guerra", as quais têm aplicabilidade à vida, independente da dimensão ser física ou digital. São precisamente estas vulnerabilidades que irão ser exploradas pelos atacantes para ganhar acesso aos sistemas alheios e atingir o seu intento.

As ciberameaças externas às organizações situam-se, de uma forma genérica, em duas grandes categorias[3]: (1) roubo e/ou alteração de dados/informação e (2) ataques disruptivos. Estes podem ser conduzidos por diversos tipos de atores, desde Estados a grupos ou indivíduos criminosos. Por sua vez, o potencial de impacto, complexidade e sofisticação de um ciberataque varia do nível de acesso do perpetuador aos recursos e à tecnologia disponível. Assim, pode afirmar-se que um ator estatal, para atingir um alvo estratégico sem ser detetado, tenderá a optar pela utilização de técnicas de encriptação e de anonimato num *malware*[4] a utilizar numa "vítima", de forma a ganhar acesso aos sistemas pretendidos. No entanto, as situações mais comuns na sociedade decorrem de *malware* menos sofisticado que é desenvolvido para redes e sistemas específicos tendo em vista o roubo de dados/informação, para depois chantagearem as vítimas e obterem dividendos.
A forma como estes *malware* são distribuídos varia da plataforma utilizada, podendo ser através de técnicas de *phishing* ou *spearphising,* no caso dos Email, ou de *Smishing* SMS,

no caso dos telemóveis, entre outras.

A este respeito, a Holanda definiu uma matriz de ameaças[5] onde são apresentadas as principais ameaças e, no que à área governamental diz respeito, são realçadas três situações: (1) espionagem, (2) manipulação de dados efetuada por Estados e (3) disrupção criada por organizações criminosas. Esta matriz, em muitas situações, é semelhante na generalidade dos países ocidentais. Assim, para fazer face a esta realidade, identificam-se três grandes áreas de atuação no ciberespaço, sendo elas: o combate ao cibercrime, a cibersegurança e a ciberdefesa, as quais têm muitas vezes por base o importante trabalho dos serviços de informações, que é relevante para o aviso antecipado, podendo dizer-se que é transversal às áreas referidas.

Tal como no mundo físico, os atores no ciberespaço movem-se por interesses próprios e que são bem diversificados. No que à área da ciberdefesa diz respeito, os principais atores[6] são os Estados Unidos da América, a Rússia e a China, situação esta natural, atendendo às questões históricas e às componentes de poder associadas. Para a sociedade ocidental, e no domínio da defesa, pode considerar-se a ciberespionagem entre as principais ameaças tendo em vista a obtenção de informação privilegiada relativamente à atuação dos Estados e das suas capacidades, entre elas as militares, onde a atuação de *Advanced Persistent Threat* (APT) constitui uma preocupação. Isto porque utilizam técnicas avançadas de recolha de informação, entre elas o desenvolvimento de *malware* específico, direcionado a pessoas com responsabilidades (administradores de sistemas ou gestores de topo) e são persistentes, pois assentam numa monitorização contínua de comportamentos e atividades, não tendo uma atuação baseada na casualidade ou oportunidade. Neste campo, as principais ameaças decorrem de APT associados à China e à Rússia[7].

Uma outra preocupação[8] tem a ver com o desenvolvimento de um sofisticado sistema de compra e venda de "ciber armas" na *Dark Web*, levando a que pessoas ou organizações mal-intencionadas as possam adquirir, mesmo desconhecendo a sua utilização, e onde a identificação dos alvos se pode constituir como único critério.

3. O contexto de Ciberdefesa

a. Enquadramento Geral

A ciberdefesa não tem uma definição exclusiva, podendo ser encontradas várias definições nos documentos enquadradores dos respetivos países. No caso português, em 2019, foi promulgada a Estratégia Nacional de Segurança do Ciberespaço (ENSC)[9], que estabelece: "Ciberdefesa consiste na atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço", onde se pode verificar o campo de atuação da ciberdefesa nos seis eixos de intervenção que integram esta estratégia. Numa partilha de conhecimento mais global, dá-se ainda a conhecer o sítio na internet do Centro de Excelência de Ciberdefesa da Estónia (CCDCOE[10]), que tem uma página dedicada à

documentação estratégica para o ciberespaço de muitos países dos diversos continentes.

No entanto, apesar da sua grande diversidade, pode dizer-se que existe uma base comum. Aqui são consideradas três situações: (1) a defesa e proteção das suas redes e sistemas militares/Defesa, para garantir a continuidade das atividades; (2) a capacidade de exploração do ciberespaço, para haver um conhecimento do que neste domínio acontece, bem como a capacidade de se atuar de forma ativa, minimizando ou eliminando uma fonte que se constitui como ameaça, ou na realização de ações ofensivas/criação de efeitos, tomando a iniciativa no ciberespaço; e (3) a cooperação entre as várias entidades com responsabilidades no ciberespaço, para uma resposta consolidada e integrada de uma capacidade nacional.

A primeira situação descrita aplica-se à maioria das organizações, no âmbito da cibersegurança para garantir a sua autonomia e ser resiliente em caso de ataque. A segunda situação, na parte de conhecimento do meio, é transversal aos serviços de informações dos Estados, ao combate ao cibercrime, à garantia de um quadro situacional no contexto da cibersegurança e às ações militares a serem empregues no ciberespaço e tem em vista a prevenção de atuações hostis e a garantia de aviso antecipado. No que ao carácter ofensivo diz respeito, esta tarefa está geralmente atribuída às Forças Armadas e constitui efetivamente o elemento diferenciador. Nos países com mais capacidades ofensivas constitui também um fator de dissuasão. Por sua vez, a terceira situação comporta a existência de um compromisso nacional entre os diversos atores, aos vários níveis (técnico, operacional, estratégico e político), onde o embaixador para a Ciberdiplomacia tem a sua relevância no contexto internacional, constituindo-se assim a garantia da eficácia na resposta do Estado.

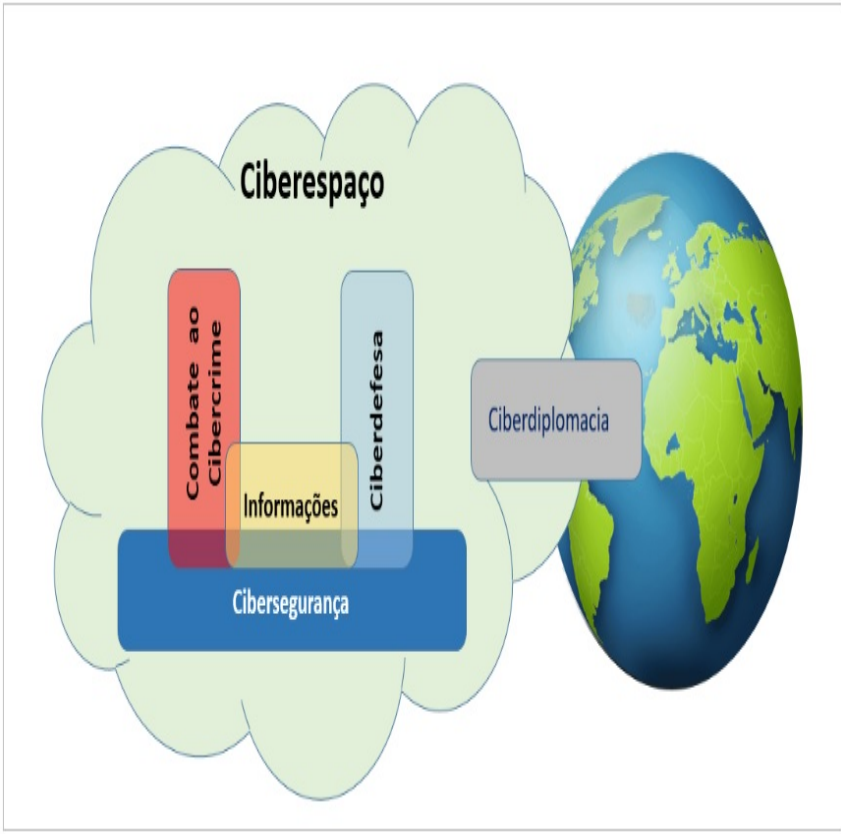

Figura 1 – Modelo de Segurança no Ciberespaço (infografia do autor) – proposta.

b. Regulamentação

Naturalmente que este tipo de atividades deverá ser enquadrado dentro da ordem internacional e que terá por base regras de empenhamento (ROE) devidamente estabelecidas. A este respeito, importa referir que a NATO assumiu, em 2014, na sua cimeira de Gales, que a lei internacional se aplica ao ciberespaço[11], situação também assumida pela UE[12] e por diversos outros países, como, por exemplo, o Reino Unido

Mas uma outra caraterística do ciberespaço é precisamente a dificuldade da sua regulação. Como exemplo, tem-se o "Manual de Tallinn", que foi elaborado por um grupo internacional de especialistas independentes sob a liderança de Michael Schmitt[13], a convite do CCDCOE, tendo em vista a análise da aplicação do direito internacional num conflito no ciberespaço. Na sua 2.ª versão são examinados os principais aspetos do direito internacional público que governam as operações no ciberespaço durante o tempo de paz, por se considerar ser a situação mais provável que os assessores jurídicos dos Estados irão encontrar, em relação às atividades no ciberespaço.

No âmbito das Nações Unidas, existem atualmente dois grupos para tratar da presente problemática, nomeadamente, o *Group of Governamental Experts on Information Security* (GGE 2019-2021) e o *Open-Ended Working Group* (OEWG), com lideranças

suportadas pelos EUA e Rússia, respetivamente. A tarefa é a de continuar a desenvolver as regras, normas e princípios de comportamento responsável dos Estados no contexto da segurança, discutir formas de sua implementação e estudar a possibilidade de estabelecer um diálogo institucional regular, com ampla participação sob os auspícios da ONU[14].

No entanto, importa referir que algumas normas atualmente existentes têm aplicação no ciberespaço, como a Carta das Nações Unidas[15], tendo em vista a manutenção da paz e estabilidade. Situação idêntica para a "Lei dos Conflitos Armados", nas situações em que os ciberataques que têm efeitos cinéticos generalizados sobre os civis, e cujos resultados sejam semelhantes aos causados por armamento.

c. Treino

Um aspeto bastante relevante para a componente militar na ciberdefesa tem a ver com o seu grau de preparação e prontidão. Aqui, a formação é um aspeto relevante para garantir que os recursos humanos afetos a esta área tenham os conhecimentos fundamentais associados ao ciberespaço, como prevenir e mitigar as ameaças e riscos dos sistemas. Por sua vez, o desenvolvimento de capacidade na componente ofensiva constitui-se como um elemento preponderante e que contribui para a soberania nacional, para a dissuasão e para a afirmação de Portugal no contexto internacional.

A participação em exercícios de ciberdefesa apresenta assim uma grande mais-valia, tanto para os operadores, como para os gestores dos sistemas e decisores. Os primeiros, porque podem treinar situações que não são usuais no seu dia-a-dia, preparando-os para essas situações no futuro. Para os gestores dos sistemas, porque aqui poderão explorar melhor os sistemas, colocá-los em situações de exaustão e outras, o que não é possível fazer nos sistemas em produção, que estão em uso diário para a defesa e proteção dos seus organismos. Um bom exemplo disto é o exercício NATO *Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise* (CWIX), que se constitui como o maior exercício de interoperabilidade da NATO, onde existe uma grande componente técnica, e no qual se têm verificado diversos desenvolvimentos na área da ciberdefesa, área esta que é liderada por Portugal, desde 2018. A nível internacional são realizados diversos exercícios de ciberdefesa e cibersegurança. Relativamente aos primeiros, podem mencionar-se os exercícios *Locked Shields* e *Cross Swords*, organizados pelo CCDCOE, bem como o *Cyber Coalition,* que se constitui como o exercício de referência da NATO neste domínio. Existem ainda outros exercícios, de âmbito menos vasto, como sejam o exercício Iberoamericano de Ciberdefesa, ou outros de caráter nacional, organizados pelos organismos de Ciberdefesa nacionais, como o *Cyber Flag* (EUA), o DEFNET (França), o *Guardião Cibernético* (Brasil) e o *CyberDEx* (Portugal). Ainda num contexto nacional, importa mencionar os exercícios *CYBER SPARTAN II* (Reino Unido) ou o *CIBER PERSEU* (Portugal), da responsabilidade dos Exércitos desses países. No que aos decisores diz respeito, ao nível da governação (político, administração pública e empresarial), importa o conhecimento desta nova

dimensão, na forma como pode criar impactos na sua organização e como terão de ser resolvidos. A este nível é de realçar o exercício nacional de cibersegurança (*ExNCS*), que se realiza em Portugal, desde 2018. Merece um destaque especial o exercício "EU CYBRID 2017"[16], um exercício *Table Top* de ciberdefesa, organizado pela primeira vez, pela Estónia, aquando da sua presidência do Conselho da União Europeia (UE), e que visava a resposta a uma crise originada por campanha ofensiva no ciberespaço contra as estruturas militares da UE num contexto de guerra híbrida. Os seus objetivos estavam orientados para o aumento da sensibilização na coordenação de incidentes de cibersegurança a nível político e para os efeitos potenciais das campanhas ofensivas no ciberespaço, tendo sido jogado pelos ministros da defesa da UE.

Assim, os exercícios constituem um fator de motivação, pela possibilidade de se testarem novas soluções, no aprofundar do conhecimento dos sistemas e equipamentos e de encontro de soluções/respostas organizacionais e de governação, que de outra forma dificilmente se conseguiria.

4. Contexto Internacional

a. Organização das Nações Unidas (ONU)

A ONU vê a cooperação internacional como uma das formas de combater países e/ou indivíduos ou entidades que são responsáveis por abusos do ciberespaço, cujas atividades afetam a paz e segurança internacional. Lembrando as declarações de António Guterres[17], aquando do seu doutoramento *Honoris Causa*, em Lisboa, em fevereiro de 2018, ao afirmar que as suas duas grandes preocupações da atualidade são as alterações climáticas que se constituem "a maior ameaça para a vida coletiva", bem como as questões ligadas à segurança, pela "falta de mecanismos regulatórios para as novas tecnologias". Concretamente, para o ciberespaço, enfatizou existirem "de forma mais ou menos escondida, episódios de ciberguerra no mundo" entre Estados e não haver nenhum esquema regulatório. "Estou convencido que a próxima guerra entre dois estados vai ser antecedida por um maciço ciberataque com objetivo de destruir as capacidades militares". Esta preocupação esteve naturalmente na base do "Roteiro para a Cooperação Digital"[18], apresentado pelo Secretário-Geral das Nações Unidas, em junho de 2020.

De referir ainda um estudo[19] efetuado à doutrina militar dos cinco membros[20] permanentes do Conselho de Segurança das Nações Unidas, que mostra que os eventos no ciberespaço estão a crescer de forma considerada, sendo referido que também existe um entendimento que estes terão consequências militares. No entanto, mantêm-se uma grande ambiguidade na utilização das ferramentas associadas, bem como na interpretação efetuada do seu emprego pelos governos e pelos militares, não havendo ainda uma definição consensual de guerra no ciberespaço.

b. North Atlantic Treaty Organization (NATO)

Face ao impacto que o ciberespaço tem na sociedade atual, a ciberdefesa passou a figurar no conceito estratégico da NATO, em 2010, na cimeira realizada em Lisboa. Atendendo à sua relevância nas operações, em 2016,
na cimeira de Varsóvia, os Chefes de Estado e de Governo consideraram o ciberespaço como um novo domínio das operações, situação idêntica aos domínios terrestre, marítimo e aéreo[21]. Decorrente disto, também foi assumido o *Cyber Defence Pledge*, que consiste num compromisso tendo em vista a melhoria das capacidades de ciberdefesa dos Estados aliados sendo considerado um assunto prioritário.

Ainda neste contexto, um aspeto relevante na defesa do ciberespaço passa pela partilha de informação. A NATO *Deputy Secretary General* Ms. Rose Gottemoeller, numa iniciativa do Shangri-La Dialogue[22], referiu que importa ter as melhores parcerias possíveis com os governos e a indústria, para que se partilhe informação sobre as ameaças em tempo real, as quais são crescentes, bem como técnicas de defesa para lhes fazer frente. Desta forma, também se consegue tirar o melhor partido e benefícios que as tecnologias têm para oferecer.

Na continuidade da preocupação com o ciberespaço e decorrente da cimeira da NATO de 2018, em Bruxelas, a Aliança procedeu a uma restruturação organizacional com a criação de um Centro de Operações no Ciberespaço (CyOC – *Cyber Operations Center*), no SHAPE, tendo também ficado estabelecido que a criação de efeitos no ciberespaço, em apoio às missões ou operações da Aliança, ficaria esta a cargo das nações[23].

O posicionamento da ciberdefesa na NATO está claramente definido, através da declaração do Secretário-Geral da NATO Jens Stoltenberg[24] de que "*Our deterrence and defence includes conventional capabilities, cyber defence, missile defence, and the nuclear dimension*", contribuindo para o pilar da defesa coletiva. Por sua vez, também já alertou para os desenvolvimentos tecnológicos que estão a alterar a natureza da guerra, nomeadamente ao nível da Inteligência Artificial e da *machine learning*, situação que está a ser acompanhada nesta organização[25].

c. União Europeia

Tendo em consideração que as ameaças atuais (terrorismo, ameaças híbridas, volatilidade económica, alterações climáticas e insegurança energética) afetam as pessoas e o território europeu, torna-se necessário definir um nível de ambição para a promoção da paz e segurança na Europa e nas suas vizinhanças. Desta forma, foram identificadas como áreas de focalização de esforços a Defesa, o ciberespaço, o contraterrorismo, a energia e as comunicações estratégicas. Por sua vez, é considerado que a segurança coletiva da UE é garantida em ligação próxima com os seus parceiros, com ênfase na NATO. Verifica-se então que a UE tem privilegiado uma atuação mais ao abrigo do *Soft Power*.

De notar ainda uma Proposta de Resolução do Parlamento Europeu[26] sobre ciberdefesa, abordando diversas áreas como o desenvolvimento de capacidades de ciberdefesa e ciberdissuasão, a ciberdefesa das missões e operações da *Política Comum de Segurança e Defesa* (*PCSD*), a educação e formação em ciberdefesa, a cooperação UE-NATO no domínio da ciberdefesa, as normas internacionais aplicáveis ao ciberespaço, a cooperação civil e militar, o reforço institucional e as parcerias público-privadas. Esta proposta mostra que a forma como a "Europa" vê o ciberespaço, e concretamente a ciberdefesa, está a alterar-se.

d. Outros elementos de informação relevantes

A Estónia tem um Centro de Excelência acreditado pela NATO, o NATO *Cooperative Cyber Defence Centre of Excelence* (CCDCOE), desde 2008, o qual se constitui como um centro multidisciplinar e de conhecimento nesta área. Conta com a presença de diversos especialistas nesta área, nomeadamente, de militares, analistas e professores, oriundos de 29 nações, tendo Portugal aderido, em abril de 2018.

Para fazer face às ameaças e oportunidades que caracterizam o ciberespaço, na área da ciberdefesa, têm-se verificado um aumento de recursos (financeiros e humanos), levando a alterações estruturais. Como exemplos, temos a criação de cibercomandos, como já aconteceu nos EUA, França, Holanda, Espanha e Brasil, entre outros. A Alemanha, por seu lado, foi mais além e criou um novo ramo das Forças Armadas, o *Cyber and Information Space Command*[27], que integrou as diversas capacidades de Comunicações e Sistemas de Informação militares, informações e guerra eletrónica. Relativamente a Portugal, a aposta no crescimento na ciberdefesa foi contemplada na Diretiva Estratégica do EMGFA 2018-2021, constando como um dos nove objetivos estratégicos, integrada em termos organizacionais na estrutura deste Estado-Maior.

Conforme já referido, verifica-se que as ações realizadas no ciberespaço têm entidades com competências específicas, como sejam o combate ao cibercrime, a garantia de cibersegurança e as ações ofensivas na área da ciberdefesa. Entretanto, também se verifica que existem diversas áreas que se podem considerar como de sobreposição, como acontece com a parte da exploração do ciberespaço pelos serviços de informações de segurança (que vigiam o ciberespaço para garantir a segurança do Estado) e dos militares (que também necessitam da vigilância para o planeamento e condução de operações neste mesmo domínio). Tendo em conta estas mais-valias, já vários países optaram por uma abordagem holística, integrando os esforços de exploração do ciberespaço, como sejam os EUA, o Reino Unido e a Holanda. Atendendo que as ameaças são cada vez mais complexas, sofisticadas e onde é difícil diferenciar o seu móbil, esta será, naturalmente, uma solução de futuro, rompendo com as soluções tradicionais.

5. Casos Reais

A utilização do ciberespaço para a realização de ataques considerados de larga escala, e com grande sofisticação, tem como exemplos o ataque sofrido pela Estónia (2007) que bloqueou o País, decorrente de uma decisão política do governo da Estónia e que não foi aceite pela minoria russa, a Geórgia (2008), aquando do avanço das tropas russas, e a Ucrânia (2014), aquando da anexação da Crimeia pela Rússia, sendo que estas duas últimas configuram um interesse comum na sua origem. Por outro lado, como exemplos de sabotagem, das mais relevantes, têm-se a ação levada a cabo contra o programa nuclear do Irão (2010) e na infraestrutura elétrica da Ucrânia (2015). Estes, em contextos diferentes, tornaram clara a necessidade dos Estados garantirem a ligação e a troca de informação considerada vital entre as suas principais estruturas, concretamente no que toca às suas infraestruturas críticas[28]. Estas, que são fundamentais para assegurar a ação do Estado, terão de ser alvo de uma atenção especial, no que ao ciberespaço diz respeito.

Conforme anteriormente referido, existem três fatores que contribuem para a realização de atividades ilícitas no ciberespaço: o anonimato, a sensação de impunidade e a imputação, que em inglês se designa de "*Attribution*". A estes pode juntar-se ainda a possibilidade da distribuição espacial no lançamento de um ataque, suportado numa dispersão geográfica de várias origens, e que poderá ocorrer simultaneamente de diversos locais fisicamente distintos no planeta, sendo a situação da Estónia um exemplo claro, onde foi claramente percecionada a razão do ataque[29], identificadas as origens, mas não foi possível a sua imputação para que tudo ficasse claro, conforme demonstrou o INFOSEC *Institute*[30].

Aqui também se questiona o enquadramento do tipo de ataques. Assim, um ataque físico a uma infraestrutura causando danos ou destruição nesta infraestrutura ou sistema é considerado como um ataque cinético. Por sua vez, no ciberespaço existe o conceito dos efeitos e, assim, uma ação que tenha origem neste domínio também poderá ser considerada como cinética se os resultados forem idênticos aos do mundo físico[31].

Ainda num contexto de equiparação das operações militares no ciberespaço às operações militares no mundo real, Glenn A Crowther[32] apresenta uma abordagem considerando dois tipos específicos de operações: (1) as operações convencionais; e (2) as operações especiais. Assim, como exemplo de operações convencionais no ciberespaço, são apresentadas as "ações ofensivas no ciberespaço da coligação internacional contra o Daesh". Estas destinaram-se à negação da capacidade da liderança do ISIS de comandar e financiar as suas forças e controlar as suas populações; à identificação e localização dos "ciberatores" do ISIS; e a minar a capacidade de recrutamento desta organização para inspirar ou dirigir extremistas violentos[33]. Como tal, é considerada uma operação convencional na medida em que não requer técnicas especiais ou modos de emprego únicos, e não requer uma abordagem encoberta à operação.

Por outro lado, para uma operação especial no ciberespaço foram apresentados, como

exemplo, os ataques de Stuxnet, no Irão[34], que requerem modos únicos de emprego, táticas, técnicas, procedimentos (TTP) e equipamentos. Esta operação foi conduzida num ambiente hostil, negados ou politicamente e/ou diplomaticamente sensíveis. Foi uma operação de baixa visibilidade caracterizada por uma natureza clandestina ou encoberta, manifestada pelo fato de que ninguém ainda provou, de forma evidente, quem a conduziu, apesar de muitas tendências apontarem para os EUA em colaboração com Israel. Também aqui está um exemplo da dificuldade da imputação que o ciberespaço permite e do efeito assimétrico e disruptivo das ações aqui praticadas.

Em 2016, a resposta eficaz dos países ocidentais ao ISIS constitui um marco relevante na utilização da capacidade ofensiva através do ciberespaço. Isto porque foi reconhecido este tipo de atividade, saindo-se de um anonimato que se pretendia "cauteloso". Primeiro, os EUA[35], com o Pentágono a reconhecer o uso de novas armas digitais para atacar as redes de comunicação do Estado Islâmico. Posteriormente, o Ministro da Defesa britânico[36] confirmou que o seu país estava a conduzir uma operação ofensiva no ciberespaço contra o Estado Islâmico, mencionando que tal aconteceu pela primeira vez nessa campanha, como parte da coligação internacional. A estas declarações o secretário-geral da NATO[37] declarou que os aliados tinham utilizado as suas capacidades de ciberdefesa de forma efetiva contra o ISIS.

Já em janeiro de 2020, os EUA desclassificaram[38] mais alguma informação relativa a esta operação, designada de *Operation GLOWING SYMPHONY*, que foi atribuída ao US CYBERCOMMAND, a qual é considerada por alguns especialistas como a maior operação americana no ciberespaço[39], num conceito de interagências (NSA, CIA, FBI, entre outros) e na qual participaram outros países, entre eles a Austrália, através do *Australian Signals Directorate* (ASD)[40].

Uma situação curiosa tem a ver com o facto de os *Anonymous*[41] terem declarado guerra ao ISIS, em 2015, após os atentados de Paris de 13 de novembro, onde morreram 130 pessoas, das quais 90 na sala de espetáculos "Batlacan". Assim, verificou-se uma ação "alinhada", mas não conjunta, de atores bem diferentes para um fim comum.

Ainda nas comparações entre ciberespaço e mundo físico, o então Primeiro-ministro da Estónia, Andrus Ansip, referiu que o ciberespaço representa uma forma diferente de se atingirem os mesmos fins que os utilizados por uma força convencional. O exemplo que apresentou comparava a utilização extensiva de um ataque de *Distributed Denial Of Service* (DDoS)[42] em sítios governamentais a um bloqueio a um porto marítimo. Tal como um bloqueio a um porto, este tipo de ataque limita a distribuição de bens (exemplo: através da limitação das transações financeiras *on-line*) e as atividades governamentais e de comunicação (bloqueando *websites* e portais de comunicação na sociedade). E se considerarmos que esse porto marítimo também constitui a base naval de um país, torna-se efetivamente uma situação bastante complicada.

Para terminar este ponto, podem referir-se duas ações cinéticas objetivas com efeitos reais no mundo físico, tendo por base informações produzidas no ciberespaço: (1) Uma dos EUA contra o ISIS, em 2015, em que Junaid Hussain, *hacker* desta organização

terrorista, foi abatido com um ataque de drone, após roubar e divulgar registos *on-line* relativos a pessoal deste país e (2) outra, em maio de 2019, em que as *Israel Defense Force* (IDF) efetuaram um ataque aéreo contra um prédio em Gaza, onde estaria a ser preparado um ataque contra o seu país através do ciberespaço. Esta situação constituiu uma novidade, pois teria sido a primeira vez em que ocorreu um ataque cinético em tempo real em resposta a uma situação que estaria a correr no ciberespaço[43].

6. Conclusões

Em termos gerais, a atuação das Forças Armadas no âmbito do ciberespaço tem em vista a salvaguarda da soberania nacional e a garantia dos interesses nacionais no, ou através do, ciberespaço. Desta forma, na sociedade ocidental, as Forças Armadas têm a sua missão bem clara na utilização do ciberespaço, assentando na generalidade dos casos nos seguintes pontos: a prioridade na defesa das suas redes e sistemas, a capacidade para utilizar a componente ofensiva no ciberespaço em caso de necessidade para criação de efeitos e a cooperação, tendo em vista garantir a segurança do ciberespaço de interesse nacional.

No ciberespaço, um domínio da criação humana que permite atividades assimétricas e disruptivas à sociedade, existem vários tipos de ameaças, e que no caso do Estado propriamente dito constituem preocupações maiores as associadas à espionagem e manipulação de dados efetuada por outros Estados ou outras entidades por estes controladas, com impacto em informação sensível, na propriedade intelectual e dados pessoais, bem como a disrupção passível de ser criada por organizações criminosas. Este tipo de atuações beneficia da falta de mecanismos regulatórios para as novas tecnologias, situação bem visível ao nível das Nações Unidas, da facilidade de anonimato e da sensação de impunidade existentes no ciberespaço. As diferenças entre o mundo físico e o mundo digital verificam-se fundamentalmente na forma como são praticados os atos, pois a sua génese é a mesma e assenta no fator humano.

Uma resposta adequada e eficaz de uma nação às ameaças no ciberespaço, numa visão holística, assenta na cooperação institucional entre o combate ao cibercrime, a cibersegurança e a ciberdefesa, tendo por base o importante trabalho dos serviços de informações. E aqui a deteção atempada das ameaças constitui um elemento preponderante na articulação destes intervenientes. No caso de uma atuação direta e ativa das Forças Armadas face a determinadas ameaças, esta deverá ter por base o suporte jurídico necessário, que irá assentar basicamente no direito internacional e em Regras de Empenhamento. Assim, e verificando-se o aumento da complexidade das ameaças, a sua maior sofisticação e onde se torna cada vez mais difícil diferenciar o seu móbil, uma solução de futuro poderá passar pela integração da componente de vigilância e aviso antecipado, a qual já foi adotada por alguns países por questões de eficiência na resposta e que é uma opção de conjunto.

A colocação da ciberdefesa a um nível idêntico ao da dimensão nuclear e da defesa anti

míssil, no que à defesa e dissuasão da Aliança diz respeito, e a importância dada aos desenvolvimentos tecnológicos, os quais estão a alterar a natureza da guerra, vem mostrar que o campo de batalha do futuro será muito diferente daquele que temos hoje, e para o qual teremos de nos preparar atempadamente.

Neste sentido, a capacitação das Forças Armadas em ciberdefesa constitui-se como um elemento preponderante para a resposta que o país deve ter, seja ao nível das plataformas e sistemas, mas acima de tudo ao nível dos recursos humanos, em número e em massa crítica. A este respeito, a inclusão da Ciberdefesa como um dos nove Objetivos Estratégicos da DEEMGFA 2018-2021 constitui-se como um elemento que visa a sua capacitação. De referir ainda que a prontidão é um elemento marcante na componente militar e para a qual os exercícios são um fator importante, nos quais se podem treinar as situações que mais se perspetivam encontrar, bem como outras passíveis de ocorrer, assim como fomentar o espírito de grupo interno e de cooperação com outros atores externos. Complementarmente, podemos dizer que se integra como um elemento contributivo para a dissuasão, constituindo-se, assim, como uma componente de segurança.

---

1 General de División Carlos Gómez López de Medina, Comandante Jefe del Mando Conjunto de Ciberdefensa das Forças Armadas de Espanha – "Prologo". In *Cyberspace, Risks and Benefits for Society, Security and Development*. J. Martín Ramírez e Luis A. García-Segura – pg XV. 2017.

2 FIDLER, David – *"The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions Than Answers"*. 2018. Disponível em https://www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers.

3 Intelligence and Security Committee of Parliament – *"Annual Report 2016-2017"* – pág. 6. 2017. Disponível em http://isc.independent.gov.uk/committee-reports/annual-reports.

4 *Malware* – Termo que vem de *Malicious software* (*software* maligno), o qual tem como objetivo interferir com a informação num computador, num sistema ou rede informática. Esta interferência pode ser de exfiltração de informação, disrupção de funcionamento ou mesmo danificação física. No fundo, define uma variedade de formas de *software* hostil ou intruso, onde se incluem os vírus, os cavalos de tróia e *spyware*, entre outros.

5 National Coordinator for Security and Counterterrorism – *"Cyber Security Assessment Netherlands 2019"*. 2019. Disponível em https://english.nctv.nl/topics/cyber-security-assessment-netherlands/documents/publications/2019/06/12/cyber-security-assessment-netherlands-2019.

6 CRANDALL, Matthew e THAYER, Bradley – "*The Balance of Cyberpower*". 2018. Disponível em https://nationalinterest.org/feature/balance-cyberpower-36637.

7 HO, Kah-Kin – Senior Director for EMEA Public Sector of FireEye / III Cyber Defence Symposium of the Spanish Joint Cyber Defence Command – Military Operations In Cyberspace (22May2018 – Kinépolis Madrid, Ciudad de la Imagen).

8 MARQUES, António Gameiro – "O Poder da Informação no Poder Militar". In Revista Militar – *pág.* 772. 2017. Disponível em https://www.revistamilitar.pt/artigo/1271.

9 ENSC 2019-2023. 2019. Disponível em https://dre.pt/home/-/dre/122498962/details/maximized.

10CCDCOE – Cooperative Cyber Defence Centre Of Excelence – *Cyber Security Strategy Documents*. Disponível em https://ccdcoe.org/cyber-security-strategy-documents.html.

11*NATO – "Wales Summit Declaration"*. 2016. Disponível em https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

12*European External Action Service – A Global Strategy for the European Union's Foreign and Security Policy* – pg 8. 2016. Disponível em https://europa.eu/globalstrategy/en/global-strategy-foreign-and-security-policy-european-union.

13*Michael Schmitt – chairman of the Stockton Center for the Study of International Law at U.S. Naval War College.*

14Digital Watch Observatory – "*UN GGE and OEWG*". 2020. Disponível em https://dig.watch/processes/un-gge.

15*NATO – "Gales Summit Declaration"*. 2014. Disponível em https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

16https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/09/07/first-cyber-exercise-at-eu-ministerial-level-focuses-on-strategic-decision-making.

17PINTO, Domingos – "Secretário-geral da ONU recebe "Honoris Causa" em Lisboa". 2018. Disponível em https://www.vaticannews.va/pt/mundo/news/2018-02/secretario-geral-da-onu-recebe-honoris-causa-em-lisboa.html.

18*Secretary-General's High-level Panel on Digital Cooperation*. 2020. Disponível em https://www.un.org/en/digital-cooperation-panel/.

19*VERTIC, Oxford Research Group (ORG) – Defining Remote Warfare: Cyber*. 2018. *Disponível em* http://www.css.ethz.ch/en/services/digital-library/articles/article.html/af089894-19ee-4fc8-983e-129386c25a0f.

20China, Estados Unidos da América, França, Reino Unido e Rússia.

21NATO – *"Warsaw Summit communique"*. 2016. Disponível em https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

22Iniciativa do Shangri-La Dialogue em Singapura (junho de 2018), na sessão dedicada às New Strategic Technologies and the Future of Conflict. NATO – "NATO Deputy Secretary General Rose Gottemoeller addresses the Shangri-La Dialogue in Singapore". 2018. Disponível em https://www.nato.int/cps/en/natohq/news_155086.htm.

23NATO – "Brussels Summit Declaration". 2018. Disponível em https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180713_180711-summit-declaration-eng.pdf.

24https://www.nato.int/cps/en/natohq/opinions_158705.htm.

25https://www.nato.int/cps/en/natohq/opinions_166039.htm.

26Parlamento Europeu – "Proposta de Resolução do Parlamento europeu sobre Ciberdefesa", 2018. Disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2018-0189+0+DOC+XML+V0//PT#title2.

27PAGANINI, Pierluigi – "German Military to Launch the Bundeswehr's new Cyber and Information Space Command". 2017. Disponível em http://securityaffairs.co/wordpress/57607/cyber-warfare-2/cyber-and-information-space-command.html.

28NUNES, Paulo Viegas – "Ciberameaças e Quadro Legal dos Conflitos no Ciberespaço". In Ameaças e Riscos Transnacionais no Novo Mundo Global. Porto: Fronteira do Caos Editores – Pg 204. 2016.

29Em abril de 2007, e durante vários dias, a Estónia foi vítima de um ataque de DDOS, o qual bloqueou muitos serviços governamentais, bancos e limitou muito a sociedade, pois é um País que assenta muitos dos seus processos na intenet. A origem desta ataque ainda não é conhecida, apesar de indiciarem uma origem da Rússia. No entanto, a origem dos ataques está distribuída por diversos países do Planeta.

30INFOSEC Institute – *"Estonia: To Black Out an Entire Country – part one"*. 2013. Disponível em http://resources.infosecinstitute.com/estonia-to-black-out-an-entire-country-part-one/#gref.

31Idem 28.

32CROWTHER, Glenn – *"The Cyber Domain". In The Cyber Defense Review Vol. 2 No. 3 (Fall 2017)*. Disponível em https://cyberdefensereview.army.mil/Portals/6/Documents/CDR-FALL2017.pdf.

33CLARCK, Colin – "*Carter Details Cyber, Intel Strikes Against Daesh at NORTHCOM Ceremony"*. 2016. Disponível em https://breakingdefense.com/2016/05/carter-details-cyber-intel-strikes-against-daesh-at-northcom-ceremony/.

34Vírus informático que foi direcionado para atingir o programa nuclear do Irão e toda a sua capacidade industrial, através do sistema operacional iraniano que controlava todas as reservas nucleares (SCADA – *Supervisory Control and Data Acquisition*). O Stuxnet acabou por ter uns contornos inesperados para os atacantes, cujos indícios recaem nos EUA e Israel, apesar de nunca confirmado, tendo atingido de forma colateral outros serviços, como a distribuição da rede elétrica, o abastecimento de água e transportes públicos (https://www.e-konomista.pt/artigo/ataques-informaticos-que-ficaram-para-a-historia/).

35ACKERMAN, Spenser – "*Pentagon admits it is 'looking to accelerate' cyber-attacks against Isis*". 2016. Disponível em https://www.theguardian.com/world/2016/feb/29/pentagon-admits-cyber-attacks-against-isis

36BBC – "*Michael Fallon: Britain using cyber warfare against IS*". 2016. Disponível em https://www.bbc.com/news/uk-37721147

37Atlantic Council – "*Here's Why NATO's Cyber Operations Center is a Big Deal*". 2017. Dis-ponível em http://www.atlanticcouncil.org/blogs/new-atlanticist/here-s-why-nato-s-cyber-operations-center-is-a-big-deal

38National Security Archive – "USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY". 2020. Disponível em https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony

39POMERLEAU, Mark – What new documents reveal about Cyber Command's biggest operation". 2020. Disponível em https://www.fifthdomain.com/dod/cybercom/2020/01/21/what-new-documents-reveal-about-cyber-commands-biggest-operation/

40BORYS, Stephanie – *Licence to hack: using a keyboard to fight Islamic State*. 2019. Disponível em https://www.abc.net.au/news/2019-12-18/inside-the-islamic-state-hack-that-crippled-the-terror-group/11792958?nw=0

41Independent – "Paris attack: Anonymous launches 'biggest operation ever' against Isis". 2015. Disponível em https://www.independent.co.uk/life-style/gadgets-and-tech/news/paris-attacks-anonymous-launches-its-biggest-operation-ever-against-isis-promises-to-hunt-down-a6735811.html

42Ataque DDOS – Método que consiste na inundação de um sítio com um elevado volume de tráfego de dados ou acessos, levando ao limite o servidor, o qual, ao não conseguir lidar com o excesso de tráfego, deixa de responder aos acessos legítimos.

43https://www.theverge.com/2019/5/5/18530412/israel-defense-force-hamas-cyber-attack-air-strike.