CYBERWAR – A Ameaça Invisível

Tenente-general PilAv
Alfredo Pereira da Cruz

Na noite de 5 para 6 de setembro de 2007, duas formações de aviões F-15 e F-16 da Força Aérea Israelita penetraram no espaço aéreo da Síria, surpreendentemente sem

serem detetados pelos radares de defesa aérea. As duas formações voaram inicialmente ao longo do mediterrâneo, sobrevoaram o espaço aéreo turco, posteriormente voltaram para sul e, finalmente, a cerca de 140 quilómetros da fronteira entre a Turquia e a Síria, atacaram um complexo militar sírio, supostamente um reator nuclear na cidade de *Deir ez Zor,* no nordeste da Síria.

A Síria acabara de investir biliões de dólares no seu moderno sistema da defesa aérea. O pessoal que guarnecia o centro de comando da defesa aéreo estava treinado, vigilante e alerta. Contudo, por volta da meia-noite, minutos antes do ataque, para os controladores do centro de defesa aéreo o céu sobre a Síria permanecia calmo e os écrans não mostravam quaisquer contactos. De facto, os aviões israelitas haviam penetrado no espaço aéreo sírio sem serem detetados. Nas horas seguintes, os sírios descobriram, incrédulos e de forma dolorosa, que Israel tinha tomado positivamente conta do seu sistema de defesa aéreo.

Através das mais modernas tecnologias eletrónicas e informáticas, Israel entrara no sistema de computadores do centro de comando e controlo e desta forma manipulara todo o sistema de defesa aérea da Síria. Sem necessidade da destruição física dos radares, conseguiram o efeito surpresa manipulando o sistema através das mais modernas técnicas da «CIBERWAR».

O que é a Guerra Cibernética (*Cyberwar)*? A "*Encyclopaedia Britannica"* define este tipo de guerra como «… a guerra feita por computadores e as redes que os interligam, conduzida contra governos e redes militares com o objetivo de degradar, destruir ou negar a sua utilização e levada a cabo por estados ou seus intermediários…". Embora, teoricamente, a "cyber-espionagem" e o cibercrime não façam parte da definição da "Cyberwar", hoje, com o evoluir das capacidades de ataque e da sua extensão aos setores privados, nomeadamente, aos serviços financeiros, à economia e aos serviço de saúde, considera-se genericamente que a "Cyberwar" pode englobar todos os tipos de ataque.

O «Cyberspace» ou o ciberespaço é o grande oceano onde confluem os rios da informação e os vários «*bits* e *bites*» dos sistemas computacionais. É neste espaço volátil que se movimentam as organizações públicas e privadas, as instituições militares, os sistemas financeiros, a economia, os serviços de saúde, o comércio, os serviços públicos e privados, mas também as organizações criminosas, terroristas, de espionagem e subversivas. É aqui no «Cyberspace» que acontece a «Cyberwar».

Há trinta anos atrás, o «Cyberspace» era apenas um termo utilizado para descrever a rede nascente de computadores interligados a meia dúzia de laboratórios universitários. Com o avanço exponencial da tecnologia, o mundo modificou-se vertiginosamente. Modernamente, aquilo que definimos como o "Domínio do Cyberspace" é o conjunto dos computadores, das redes que os interligam e os sistemas de comunicação onde se apoiam.

O "Domínio do Ciberespaço" é composto por três camadas. A primeira, é a camada física, incluindo o *hardware*, os cabos, satélites e outros equipamentos, sem esta camada física,

as outras camadas não podem funcionar. A segunda, a camada sintática, inclui o *software* que fornece as instruções de operação para o equipamento físico. A terceira, é a camada semântica que envolve as interações humanas com a informação gerada pelos computadores e a forma como a informação é percecionada e interpretada pelo utilizador.

Os ciberataques podem ser executados contra a estrutura física, através da utilização de armamento convencional. Por outro lado, podem ser efetuados ataques contra a camada sintática, através da utilização de "cyberweapons" capazes de destruir, interferir, corromper, monitorizar ou pura e simplesmente danificar o *software* do sistema operativo do computador.

O mundo desenvolvido depende e apoia-se no ciberespaço para o seu funcionamento diário, para quase todos os aspetos da sociedade moderna. A sociedade, a cada ano que passa, está mais dependente no ciberespaço. Tudo que a sociedade moderna necessita para funcionar – infraestruturas críticas, instituições financeiras, a economia, o comercio e as ferramentas para segurança nacional – estão dependentes e confiam no ciberespaço. Como tal, as ameaças da "Cyberwar" e os seus efeitos pretendidos são uma fonte de preocupações para governos, forças militares e setores privados.

Alvin e *Heidi Toffler* afirmavam, nos anos de 1980: "*… as guerras da primeira vaga foram-no em prol da revolução agrária, as da segunda vaga foram-no pelo controlo da capacidade produtiva, as guerras da terceira vaga serão combatidas pelo controlo do conhecimento…*". E acrescentavam, "*… desde que a forma de combater em quaisquer sociedades segue a forma da produção de bem-estar dessa sociedade, as guerras do futuro serão cada vez mais guerras de informação…*".

A operação "Desert Storm", em 1992, pressagiou as guerras do século XXI, as "smart bombs", os satélites de reconhecimento altamente sofisticados, os guerreiros modernos armados com armas da "Era do Conhecimento". A utilização intensiva das mais modernas tecnologias na microeletrónica e nos processadores permitiu um crescimento no campo das comunicações e no processamento e armazenagem de dados, de forma cada vez mais rápida.

Em plena "Era da Informação", o mundo é uma enorme aldeia global onde tudo pode ser partilhado, o conhecimento globalizou-se. A «Era da Informação», por definição, permite o acesso e o controlo da informação que definem as características da moderna corrente da civilização humana em pleno século XXI. Tudo acontece derivado de múltiplos fatores, nomeadamente, ao acelerado desenvolvimento tecnológico: processadores cada vez mais poderosos, que permitem velocidades de processamento da informação, já não medidas em segundos, mas, sim, em nano segundos; as tecnologias nano; as biotecnologias; a Inteligência Artificial (IA) e os seus algoritmos associados.

O Ciberespaço modificou fundamentalmente a economia global e segurança e soberania das nações. Transformou a forma como vivemos em sociedade, fornecendo a milhões de cidadãos no mundo o acesso instantâneo às comunicações, às informações e às

oportunidades económicas. O Ciberespaço é a nova fronteira para a plena prosperidade no século XXI. Contudo, apesar destas possibilidades, também é acompanhado por novos perigos e ameaças.

O futuro da humanidade estará diretamente ligado ao tratamento da "Data", factos e dados sobre tudo e mais alguma coisa, que exigem múltiplas aplicações, que vão ter de ser integrados, por isso o futuro terá de resolver os problemas de integração de dados, números e figuras, isto é, estamos a falar da "Big Data", "terabytes" ou "zettabytes" (1 "sextillion" de bytes, isto é, um número igual a 1 seguido de 21 zeros), para incorporar, estruturar e organizar, para serem compreensíveis e a partir daí construir as informações, destinadas à ciência, à economia, aos sistemas de defesa dos estados, à medicina, à industria, isto é, à vida da humanidade vista de forma holística. No futuro não muito distante, a "Big Data" será um alvo prioritário dos "hackers" (piratas informáticos).

A *Internet* é um sistema aberto e facilmente acessível, como o deve ser. Mas, infelizmente, também um novo campo para o desenvolvimento de novas e perigosas batalhas. É e será o campo de batalha onde os adversários procurarão causar danos a estados e a organizações antagónicas. Ela constitui a espinha dorsal da «Era do Conhecimento e da Informação», digamos que é o sistema dos sistemas por onde flui toda a informação global, a privada e a institucional. As vulnerabilidades dos sistemas informáticos existem e têm vindo a aumentar exponencialmente. Mais de 9 mil milhões de registos de vulnerabilidades e ataques de «malware», durante 2019, apontam para um crescimento da insegurança. O termo «malware», proveniente do inglês "malicious software" (*software* malicioso), é um *software* destinado a infiltrar-se em sistemas de computadores alheios de forma ilícita, com o intuito de degradar, causar danos, alterações ou roubo de informações (confidenciais ou não). Vírus de computador, *worms*, *trojans* e *spywares* são considerados "malwares".

Nos últimos anos, têm crescido de forma avassaladora um novo tipo de ataques criminosos contra os estados soberanos e grandes organizações privadas, o "ransomware". O "ransomware" é um tipo de "malware" que assume e limita um sistema informático, como uma espécie de bloqueio. Para desbloquear o sistema, os "hackers" exigem elevados resgates, que no caso de não serem pagos ameaçam a distribuição e a publicação pública dos arquivos, ou mesmo a sua destruição.

Os "hackers" são jovens muito talentosos, alguns, uns verdadeiros prodígios nos domínios da informática e da computação, responsáveis pela criação de "malware", com o objetivo de infiltrar redes de computadores e sistemas, com intentos maliciosos e criminosos. Muitos destes grupos de "hackers" operam ou são coordenados por estados ou por organizações internacionais, na sua maioria ilegais. Não existe um sistema à "prova de bala" disponível que permita a total segurança das redes e dos sistemas de computação contra este tipo de ataques.

Estados autocráticos apoiam este tipo de organizações criminosas, entre os quais a China e a Rússia são os mais conhecidos. Um dos mais recentes casos envolvendo a Rússia foi o ataque à "Solar Winds", uma empresa privada americana de Tecnologias de Informação.

Em síntese, provavelmente, a Rússia, foi capaz de comprometer uma empresa privada e a partir daí ter acesso a diversos departamentos e redes computacionais do governo americano. Como resultado, um número indeterminado de "Data" foi exfiltrado, o que constituiu uma admirável façanha de espionagem.

É do conhecimento público que a Rússia continua a apoiar grupos de ciber criminosos, incluindo grupos como, o "Cl0p" o "Ryuk", o "Revil", o "DarkSide", grupo que atacou, num ataque de "ramsonware", o oleoduto "Colonial" nos EUA. O presidente russo afirmou numa entrevista à cadeia de TV NBC americana, em 2016, que "… desde que os cibercriminosos não infrinjam a lei russa, ele não terá qualquer interesse em os perseguir…".

As autoridades americanas sempre basearam as suas defesas no ciberespaço numa estratégia de dissuasão, tendo para tal elaborado um novo conceito, a "defence forward" (defesa avançada), para prevenir e responder a comportamentos maliciosos no ciberespaço. Contudo, no caso da "Solar Winds", chamar este assalto ao governo dos EUA um caso de ciberataque estará fora das marcas, do que é conhecido, parece ter sido um puro ato de espionagem para roubar informações classificadas sobre a segurança nacional, e não degradar, negar ou interferir nas redes e informações (Big Data).

Os mais recentes ataques de "ransomware" levantaram a necessidade de discussões sobre a natureza das ciber ameaças aos países soberanos. A grande maioria dos especialistas em segurança sempre se focou na necessidade de se defenderem contra ataques a alvos críticos e sistemas de redes, planeados por países antagonistas ou inimigos declarados, num cenário tipo "Armageddon". Até muito recentemente, os cibercrimes e outras atividades maliciosas, levadas a cabo por "hackers" ou organizações mafiosas, não eram uma preocupação prioritária para os governos. Como resultado, o sistema interconectado de segurança nacional dos estados não está preparado para defender as infraestruturas críticas contra ciberataques cometidos por grupos do crime organizado.

Conhecer as atividades do ciberespaço na China não é tarefa fácil, em virtude do secretismo envolvendo todo o tipo de atividades nesta área. O presidente *Xi Jinping* afirmou, em 2014 "… não há segurança nacional sem segurança no ciberespaço…".

Na China, os "hackers" são apoiados pelo Estado e focados no roubo de propriedade intelectual, segredos comerciais e informação comercial sensível, com um claro objetivo de amplificar as capacidades competitivas chinesas. Contudo, mais recentemente, a China parece mudar de rumo, tentando que os seus "hackers" obtenham informações sobre capacidades militares e funcionários governamentais que interagem com os negócios de defesa. É visível que a China está a dar uma maior importância ao ciberespaço como um importante domínio da segurança nacional e uma área da competição estratégica.

Estamos na alvorada de uma nova revolução tecnológica, também chamada de 4.ª Revolução Industrial. Esta revolução digital é caraterizada pela fusão de diversas

tecnologias que desfocam as linhas de fronteira entre aquilo que é físico (mecânico), o digital e as áreas da biologia, da biotecnologia e a da IA. Esta mudança radical irá alterar profundamente a maneira como vivemos, trabalhamos, nos relacionamos em comunidade e, particularmente, como iremos combater. Não temos certezas como se desenvolverá a transformação, mas quase certamente será complexa em tamanho e será algo nunca acontecido na história da humanidade.

O campo de batalha do futuro, conjunto por natureza, será totalmente digitalizado, as comunicações e a transferência de dados serão executadas em todas as direções, horizontalmente e verticalmente, a velocidades inimagináveis num passado recente. Computadores e *robots*, associados à IA e aos algoritmos, serão uma realidade cada vez mais intensa nos modernos campos de batalha e progressivamente, no muito longo prazo, podendo vir a substituir os seres humanos na tomada de decisão.

Os ciberataques, em contraste com o cibercrime, são versões sofisticadas de três atividades tão antigas como a humanidade: a sabotagem, a espionagem e a subversão. Contudo, ao contrário dos ataques físicos convencionais, estes tipos de ataque são invisíveis e acontecem sem qualquer aviso prévio, e na maioria das vezes sem causar danos físicos.

Nos atos de sabotagem é possível provocar danos gravosos nos sistemas operativos computacionais, sem causar danos físicos ao material. Ao realizar ataques de pura espionagem, é possível exfiltrar informações valiosas, sem qualquer necessidade de infiltrar agentes em operações de alto risco, como analisado anteriormente no caso "Solar Winds". Por último, em atos de subversão não haverá necessidade de ações diretas.

No seu livro "Da Guerra", Clausewitz afirmou: "*… a guerra é um ato de força para obrigar o inimigo a cumprir a nossa vontade…*". A guerra é por natureza violenta. Na visão do autor, se um ato não for potencialmente violento não é um ato de guerra, e como tal não é um ataque armado. Um ato de guerra ou um ataque armado é, na grande maioria das vezes, letal para alguns dos intervenientes, pelo menos, para um dos lados da contenda.

Na primavera de 2009, num período de seis meses, funcionários das Nações Unidas observaram nas instalações de enriquecimento de urânio em Natanz, no Irão, o desmantelamento de cerca de 10% das 9000 centrifugadoras utilizadas no processo. Esta situação resultou de falhas mecânicas graves nas centrifugadoras. Mais tarde, veio a perceber-se que estes danos materiais foram o resultado de um ataque coordenado aos computadores da central por um "worm", que ficou mundialmente conhecido como "Stuxnet".

Este ataque devastador a uma instalação nuclear foi, talvez, o primeiro ciberataque onde se procurou, e foram atingidos, danos físicos graves ao material. Foi também aqui que, pela primeira vez, se utilizou uma arma que, embora digital, se comportou como de uma bomba convencional se tratasse. O "Stuxnet" foi o precursor das "Cyberweapons" ou

"Logic Bombs" (bombas virtuais). Os criadores da "Stuxnet" mantém-se desconhecidos, contudo, especialistas suspeitam que operacionais americanos e israelitas foram responsáveis pelo ataque.

As seguranças dos sistemas de informação assentam em três princípios básicos: a Confidencialidade; a Integridade; e a Disponibilidade. Os ataques à confidencialidade resultam da entrada maliciosa nos sistemas computacionais, com a finalidade de vigiar e extrair dados e informações classificadas, ou da interceção de informação enquanto esta transita pelo ciberespaço entre intervenientes, como, por exemplo, um *email*. A integridade dos sistemas é posta em causa através de ataques, cuja finalidade é a extração de informação ou dados. A disponibilidade permanente dos sistemas é fundamental para o sucesso do funcionamento dos mesmos. Ataques que se destinem a impedir o acesso a uma rede, sejam eles executados através de uma esmagadora inundação de visitas, conhecido por «Denial of Service» (negação de serviço), ou mesmo ao seu encerramento (*offline)* através do encerramento físico ou do processo virtual do qual ele é dependente, são efeitos altamente perniciosos à disponibilidade do sistema. Um ataque, «Denial of Service», prolongado no tempo que seja capaz de encerrar temporariamente partes das infraestruturas digitais de um estado ou de uma grande organização podem e devem ser considerados como um ataque aos interesses estratégicos desse estado.

Modernamente, os ataques têm-se sucedido a uma velocidade vertiginosa, nomeadamente, os ataques de "ramsonware" aos sistemas de produção de energia e serviços de saúde, com pedidos de resgate financeiros cada vez mais volumosos, normalmente pagos em moeda tradicional, dólares ou euros, e ultimamente pedidos de pagamento em "bitcoins". Portugal não está imune a este tipo de ataque; são exemplos, os recentes ataques "ramsonware" aos serviços de saúde, à EDP e possivelmente a outros serviços que não foram do conhecimento público.

Modernamente, a maioria das forças militares no mundo desenvolvido, têm, em maior ou menor desenvolvimento, ferramentas de planeamento e organização operacionais para a «Cyberwarfare» A Força Aérea Americana descreve-a com a capacidade de Destruir, Negar, Degradar, Interromper e Enganar, e simultaneamente montar as defesas contra o uso do ciberespaço pelo inimigo cujos desígnios serão semelhantes aos seus.

Em terminologia militar, este novo tipo de guerra é vulgarmente conhecido como a «NETWORK CENTRIC WARFARE». Dentro da rede de comunicações e informações do inimigo, pode interromper-se ou mesmo incapacitar os sistemas de comando e controlo, impedindo os comandantes de enviar ordens, unidades impossibilitadas de falarem umas com as outras, ou mesmo sistemas de armas incapazes de partilharem dados e informações fundamentais à conduta das operações. A grande mudança entre o passado e o presente resume-se numa simples frase: «É a diferença entre ler os sinais rádio do inimigo e ser capaz de tomar o controlo do próprio rádio».

Tradicionalmente, as ameaças resultam de uma conjugação de capacidades de um determinado ator internacional (Estado ou Organização) e a vontade da utilização dessas

capacidades contra potenciais adversários ou inimigos. A avaliação das ameaças é um processo difícil e que envolve riscos. Existem diversos graus de incerteza na avaliação das nossas vulnerabilidades e das capacidades e intenções do adversário ou potencial inimigo. A natureza das ameaças no ciberespaço torna a sua avaliação ainda mais difícil.

No caso da "Cyberwar", o uso da força é efetivamente mais complexo e acaba por ser um resultado de causas e consequências que, em último grau, podem resultar em violência e vítimas. Num ataque convencional há sempre um aviso prévio, no lançamento de um míssil balístico intercontinental o aviso poderá ser de minutos, num disparo de um míssil ar-terra o aviso pode ser de segundos, mas, na realidade, existe sempre um tempo prévio que permite uma reação mais ou menos imediata. Por outro lado, na maioria das vezes, conhece-se a fonte do ataque, possibilitando uma reação atempada.

No ciberespaço não há avisos prévios, na maioria das situações só se tem conhecimento do ataque depois dele acontecer. A indefinição da natureza dos atores, a incerteza na definição das fronteiras físicas, torna extremamente difícil a montagem de contra-ataques. Os ataques podem ser originados interna ou externamente, podem ser executados por autores privados, estatais, ou por ambos em conjugação. O ataque preventivo aos sistemas computacionais do adversário ou potencial inimigo é o método e a solução mais eficaz como garante da segurança dos nossos sistemas. Contudo, para um ataque preventivo ter sucesso, dois axiomas são fundamentais: conhecer a fonte da ameaça e ter a capacidade ofensiva para o realizar; adicionalmente e devido à própria natureza do ciberespaço, a possibilidade de danos colaterais é muito superior, uma vez que os sistemas militares partilham do mesmo tipo de *software* que os sistemas civis. Torna-se assim difícil distinguir quais os sistemas que se pretendem atingir. Por último, há que ter em consideração as razões éticas e morais que – para estados como a Rússia e a China serão de importância relativa – para os estados ocidentais são premissas básicas para a tomada de decisão.

A "Cyberwar" é um problema de hoje e não de amanhã; o risco à segurança e defesa dos estados soberanos existe e tem-se multiplicado exponencialmente. É necessário e urgente procurar soluções e novas metodologias para responder de forma efetiva às ameaças no ciberespaço. Muitos estrategas militares e civis têm expressado grande preocupação sobre as leis e a compreensão do conflito armado que não têm acompanhado os desafios, nomeadamente, sobre as capacidades ofensivas da «Cyberwar».

As doutrinas e a definição de estratégias fundamentadas no pensamento de *Clausewitz* não respondem satisfatoriamente às novas realidades do mundo emergente da «Era da Informação» e da "Cyberwar". É necessário definir novos conceitos e estratégias de combate às ameaças emergentes, é exigível revisitar os conceitos sobre segurança e defesa. Tradicionalmente, ao nível estatal, a Segurança lida com as ameaças internas, enquanto a Defesa assume as responsabilidades das ameaças externas. Pelo que foi exposto, não faz sentido continuar a discutir a validade, a hierarquia ou as responsabilidades da cibersegurança e da ciberdefesa no mundo do ciberespaço. É preciso desenvolver esforços para que as diferentes organizações interajam e se organizem hierárquica e funcionalmente. No mundo liberalizado em que vivemos é

necessário coordenar, regular e fiscalizar as entidades não governamentais, que têm responsabilidades no âmbito da cibersegurança, serviços financeiros, sistemas de comunicações, economia, serviços de saúde, energia, água, universidades, entre outros.

A abordagem à resiliência das redes e a definição de novos conceitos e doutrinas deve mudar de um paradigma de aplicação da Lei, para um diferente paradigma, o da segurança nacional. Este novo paradigma é importante, porque vai afetar o enquadramento sobre o qual as operações são executadas. Isto é, o ênfase transfere-se para as realidades da defesa ativa, adaptação, identificação de vulnerabilidades e uma redundância e resiliência sistémica.

Os estados mais poderosos e mais avançados tecnologicamente dispõem de departamentos governamentais responsáveis pelas medidas de segurança no ciberespaço, coordenando todas as medidas que salvaguardem a livre utilização das redes e dos sistemas computacionais, sejam eles públicos ou privados. Simultaneamente, têm desenvolvido enormes capacidades ofensivas no campo da «Cyberwar» como forma de dissuadir os ataques por agentes antagónicos.

Os EUA, para garantir a segurança e o bom funcionamento do ciberespaço, organizam-se em dois grandes departamentos: O *United States Cyber Command*, dependente do Comando Estratégico dos Estados Unidos (*US Strategic Command*), responsável na estrutura militar pelas políticas de segurança, tanto defensivas como ofensivas; e o *Department of Homeland Security* (*DHS*), responsável pela cibersegurança ao nível interno, vigiando e protegendo os sistemas governamentais e fornecendo assistência especializada aos setores privados.

No Reino Unido, o *GCHQ* (*Government Communications Headquarters*) é o ponto central de todos os assuntos relacionados com a cibersegurança. O *GCHQ* é uma organização de segurança e informações (*intelligence*) responsável por manter o Estado em segurança no ambiente dos modernos sistemas de comunicações e informações. O *CESG* (*Communications-Electronics Security Group*) é o braço do *GCHQ* para proteger as comunicações e sistemas de informação do governo e áreas críticas da infraestrutura nacional do Reino Unido.

Na Rússia, as responsabilidades do ciberespaço estão centralizadas no "Federal Security Service of the Russian Federation – FSB". Na perspectiva russa a "Cyberwar" ou o equivalente russo "information-techonological warfare" é uma parte do conceito predominante as information confrontation" (informatsionnoe protivo borstvo). O FSB é considerado o serviço especial mais poderoso, e visto como o sucessor do KGB. Não obstante o seu foco doméstico, as suas ações têm vindo a aumentar no exterior da Rússia. O FSB é o responsável pelas contra-informações e pela coleta de informações, incluindo o ciberespaço. É também o principal responsável pela segurança interna e trabalha e coopera com as agencias federais, como a "Roskomnadzor" (Federal Service for Supervision of Communications, Information Technology and Mass media), o "Minsifri" (Ministry of Digital Development, Communications and Mass Communications of Russian Federation) e outras agências.

É muito difícil avaliar o estágio de desenvolvimento das capacidades da «Cyberwar» na China. São conhecidos diversos ataques cuja origem é direcionada para este país. A organização chinesa é quase clandestina e centralizada no Estado, está organizada num misto de militares e civis, muitas das vezes trabalhando em conjunto ou em coordenação. O Exército chinês continua a ser o principal responsável pela "ciberwar", contudo, muitas das atividades diretamente ligadas às atividades ilícitas dos "hackers" estão sendo direcionadas para o "Chinese State Security Ministry – MSS" (ministério da segurança do estado), após uma reorganização das operações do ciberespaço, em 2015.

O Estado de Israel desenvolveu uma organização de cibersegurança, reconhecida internacionalmente como um dos melhores sistemas de segurança do mundo.

O seu sistema de cibersegurança está focado no principal departamento israelita para os assuntos do ciberespaço, o "Israel National Cyber Bureau – INCB". Os seus objetivos são claros e baseiam-se em três pilares principais: defender as infraestruturas nacionais de ciberataques; desenvolver as capacidades de Israel como líder mundial nas Tecnologias da Informação; encorajar a cooperação entre as universidades, a indústria e os setores privados, assim como entre as agências governamentais e a comunidade da segurança.

Como órgão de execução foi criado, em 2017, o "National Cyber Directorate", responsável por todos os aspetos da ciberdefesa na esfera civil, desde a formulação da doutrina através da R&D até às atividades operacionais. O "National Cyber Directorate" é a agência para a segurança nacional e para o desenvolvimento tecnológico, responsável para a defesa do ciberespaço de Israel e edificar o Poder de Israel no ciberespaço.

Pelas razões históricas da permanente ameaça aos seus territórios, as atividades da "Cyberwar" de índole militar estão totalmente concentradas na IDF (Israel Defense Forces), através do AMAN (Israel Military Intelligence) e em permanente ligação e coordenação com o INCB e o "National Cyber Directorate".

Perante as ameaças reais no ciberespaço, e com a firme intenção de dotar a Aliança com capacidades robustas na defesa contra a "Ciberwar", a NATO, durante a cimeira no País de Gales (Newport – 4/5 de setembro de 2014), adotou uma nova doutrina e um renovado plano de ação, sancionado por todos os países aliados. Esta mudança determina que a ciberdefesa é parte integrante da missão de defesa coletiva da Aliança e confirma que as leis internacionais, nomeadamente, as leis dos conflitos armados, se aplicam ao ciberespaço.

Pela primeira vez, um ciberataque a um dos seus vinte e oito membros poderá ser declarado um ataque a todos, em tudo similar a uma invasão terrestre, um ataque aéreo ou naval. A inclusão do ciberataque na definição de «ataque armado» permite que uma ação contra um dos seus membros pode conduzir a uma resposta coletiva da Aliança de acordo com o artigo V do Tratado de Washington.

A Doutrina da NATO sobre a Ciberdefesa é implementada pelas autoridades políticas, militares e técnicas aliadas, assim como pelos países aliados. O Conselho do Atlântico Norte (North Atlantic Council – NAC) fiscaliza, ao mais alto nível político, todos os

aspetos de implementação. O Conselho será informado de todos os incidentes e ataques e exercita a sua autoridade durante a gestão de crises relacionadas com a ciberdefesa. É criado um novo Comité de Ciberdefesa (Cyber Defence Committee), subordinado ao NAC, responsável pela definição da doutrina e aconselhamento dos países aliados nesta área.

No combate às ciberameaças, a prevenção é certamente a melhor resposta às múltiplas ameaças que as organizações e os indivíduos estão sujeitos em permanência no ciberespaço. A cibersegurança é muito mais do que a aplicação da tecnologia nesse sentido. Muitos livros e artigos escritos sobre estas matérias focam-se apenas nas possíveis respostas técnicas perante as ameaças. Na realidade, a falibilidade humana e outras vulnerabilidades conhecidas, continuam a permitir que os ataques aconteçam quando não se consideram estes fatores. Uma cultura de segurança é absolutamente vital na forma de comportamento individual e coletivo perante as ameaças, permitindo um complemento às medidas de ciberdefesa baseadas na tecnologia.

A prevenção deverá ser baseada em vários patamares: utilização intensiva de redundâncias (*backups*) e outras ferramentas digitais e físicas impeditivas ou que dificultem o acesso aos sistemas (*firewalls* e antivírus); criação de uma cultura de segurança, dentro e fora do local de trabalho; formação e treino permanente dos utilizadores; Resiliência, aqui definida como capacidade de defesa e recuperação perante fatores ou condições adversas. No ciberespaço, Resiliência é a capacidade de se adaptar às condições adversas e ser capaz de recuperar as suas funcionalidades. A resiliência dos sistemas tem de estar preparada e manter algumas das suas funcionalidades e controlo mesmo sob um ataque.

Uma das áreas chave no combate aos ciberataques é a formação e o treino. A formação contínua deve ser uma premissa básica ao longo do processo, e deve começar nas escolas, nas universidades nos locais de trabalho. A educação é fundamental para a criação de uma cultura de segurança. A questão-chave do ciberespaço é a sua segurança.

Hoje, na era da informação, do conhecimento e da globalização, desde as comunicações, à economia e à guerra, todos dependem da *Internet.* A integridade e a disponibilidade desta rede, e os assuntos ligados à sua segurança são um desafio de todos. Neste mundo interligado e global, nesta miríade de novas ameaças quase invisíveis, o indivíduo, a família e a comunidade enfrentam novas realidades no âmbito dos seus direitos e responsabilidades.

Em Portugal, as preocupações por estas matérias são relevantes e muito importantes, contudo, não existe uma perceção da gravidade, presente e futura, das ameaças emergentes da "Cyberwar".

O governo de Portugal publicou legislação sobre a temática do ciberespaço. O Decreto-Lei n.º 69/2014, de 9 de maio, procede à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, que aprova a orgânica do Gabinete Nacional de Segurança (GNS), estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança (CNCSeg). O CNCSeg tem por missão contribuir para que o país use o ciberespaço de

uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional. Em Portugal, estes assuntos são geridos de uma forma redutora e não de uma forma holística, multidomínio e agregadora das áreas económicas, financeiras, segurança, e dos setores da energia e da saúde. Talvez por razões culturais, somos levados a acreditar que os ataques da "Cyberwar" são ataques de baixo risco, nada mais enganador. É notório que para os diversos governos em Portugal os assuntos do ciberespaço nunca foram uma elevada prioridade.

Colocar o CNCSeg na dependência do GNS parece não ter sido uma decisão coerente. Sem pôr em causa a importância do GNS, efetivamente, o CNCSeg é de uma maior importância estratégica e operacional para o futuro da segurança nacional, a "Cyberwar" será uma das maiores ameaças, no futuro não muito longínquo, à Segurança Nacional. Portugal precisa de repensar toda a estrutura da cibersegurança nacional e de uma forma holística, multidomínio, que incorpore os setores críticos, públicos ou privados.

É preciso mudar mentalidades e é necessária a constituição de um departamento ao nível mais elevado, com responsabilidades de coordenação entre os vários ministérios, nomeadamente, os mais sujeitos a este tipo de ameaças. Estudar e analisar diferentes modelos e organizações internacionais é importante, contudo, copiar o que existe é sempre perigoso; é necessário desenvolver modelos que estejam em consonância com a nossa cultura e organização. A organização israelita pode ser um bom "template", desde que adaptado a nossa realidade e cultura.

A criação de um departamento responsável pela segurança do ciberespaço, dependente do presidente do Conselho de Ministros, seria uma solução interessante. O Departamento seria responsável pela defesa das infraestruturas críticas nacionais, coordenar as Tecnologias de Informação e fomentar a cooperação entres as universidades, a indústria, os setores privados e a comunidade de segurança.

Na sua dependência deveria ser criado um departamento operacional, responsável por todos os aspetos do ciberespaço, incluindo as esferas civis, públicas e militares, e garante da formulação conceptual do desenvolvimento tecnológico das áreas do ciberespaço. Em síntese, este serviço seria o responsável operacionalmente pela defesa do ciberespaço em Portugal. Por razões de operacionalidade, pela experiência de planeamento e pelas capacidades técnicas residentes nas Forças Armadas, seria, talvez, uma boa solução constituir um comando operacional no Ministério da Defesa Nacional (MDN) e sobre a gestão do Chefe do Estado-Maior General das Forças Armadas (CEMGFA).

Como descrito anteriormente, as leis dos Conflitos Armados, a Convenção de Genebra e os seus Protocolos adicionais já não respondem convenientemente perante os ataques da no ciberespaço. O almirante *Michael S. Rogers,* ex-Director da "National Security Agency (NSA)" e ex-comandante do "US Cyber Command", afirmou *"… Os mares à volta do mundo, como o domínio Cyber, não são governados por uma simples nação. Criámos normas marítimas e teremos de fazer o mesmo no ciberespaço para assegurar o livre fluxo das informações e das ideias…"*. É urgente revisitar os conceitos e as doutrinas definidas por *Clausewitz,* é necessário reavaliar e analisar, de acordo com as novas

realidades das novas ameaças emergentes, as Leis dos Conflitos Armados e a Convenção de Genebra.

No corrente mandato das Nações Unidas (ONU) sobre as discussões relativas ao ciberespaço, muitos assuntos têm sido discutidos sobre a legalidade e implicações políticas da aplicação da Lei Internacional Humanitária, no decurso de operações militares no ciberespaço durante um conflito armado, e a lei "Jus Ad Bellum". A "Jus Ad Bellum" é uma lei internacional que orienta o uso da força por um estado e é baseada no uso de normas costumeiras (costumes da guerra) internacionais e nos princípios, do inerente dever de defesa própria, como explicito no artigo 51 da Carta da ONU. A questão charneira a responder implica o determinar como a Lei se pode aplicar às atividades militares conduzidas no ciberespaço por um estado, e saber se existe um conflito armado entre um estado e um qualquer adversário e se será um estado ou grupo. Efetivamente, "Jus Ad Bellum" é um bom princípio de discussão e análise para o uso legal das atividades no ciberespaço pelos militares de um estado.

O Ciberespaço é – e será no futuro – o centro nevrálgico da economia global e, cada vez mais, também o da segurança mundial. Está exposto a múltiplas ameaças de origem difusa que podem, se não sustidas, porem em causa a nossa liberdade, os direitos humanos, as economias e a segurança das nações soberanas.

O atual conceito de Guerra conjunta já não estará em consonância com o futuro da guerra, para ser efetivo tem de se focar no âmbito do espaço e do ciberespaço. A guerra no ciberespaço é uma inevitabilidade, não será demais lembrar que a questão chave é, de facto, a sua segurança.

Ao longo do artigo explicámos de forma sintética, como funciona, a sua importância e o que todos nós podemos fazer para que as redes por onde correm e fluem as informações continuem a desempenhar a sua função em perfeitas condições de credibilidade e confiança.

A "Cyberwar" e os ciberataques são parte de um novo mundo caótico e completamente desordenado, alimentado pela globalização e pela revolução da informação. No ciberespaço global é muito mais difícil abater a atividade que desfoca as linhas entre os governos e os cidadãos privados, os domínios nacionais e internacionais, entre o roubo e a guerra.

O Ciberespaço não é um espaço de dissuasão, mas um ambiente ofensivo e persistente.

«A vitória sorri aos que melhor se adaptam às mudanças do caráter da guerra e não aos que esperam adaptar-se depois dela ocorrer»

General Giulio Douhet.

Bibliografia

Amy, Chang (December 2014. "Warring State: China's Cybersecurity Strategy," Center for New American Security. Retirado de https://s3.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf?mtime=20160906082142.

Bebber, J. (July 6, 2017). Beijing´s Views on Norms in Cyberspace and Cyber Warfare Strategy Pt.2. CIMSEC. Retirado de https://cimsec.org/beijings-views-norms-cyberspace-cyber-warfare-strategy-pt-2/.

Benoliel, D. (2015). Towards A Cybersecurity Policy Model: Israel NationalCyber Bureau Case Study. North Carolina Journal ofLaw & Technology, Volume 16, Issue 3.

Borger, J. (15 October 2007). Israeli air strike was aimed at Syrian reactor, report says. The Guardian. Retirado de https://www.theguardian.com/world/2007/oct/15/syria.israel.

Borghard E, & Schneider J (2020). Russia's Hack Wasn't Cyberwar. That Complicates US Strategy. The Wired. Retirado de https://www.wired.com/story/russia-solarwinds-hack-wasnt-cyberwar-us-.

Clarke Richard, Knake Robert, 2012. Cyber War: The Next Threat to National Security and What to Do About It: New York, Harper Collins Publishers.

Clausewitz, C. V. (1955). De la Guerre. Paris: Les Editions de Minui.

Cruz, A.S.P. (2019). 100 anos de Poder Aéreo – A história da aviação militar. Coleção "ARES", 27. Lisboa: Instituto Universitário Militar.

Cruz, A. (2014). Cyberwarfare, o Futuro é Hoje. Revista Mais Alto, 412

Grange, Miranda (2014). Cyber Warfare and the Law of Armed Conflict. Victoria University: Wellington.

Newman, H. L (17JUN2021). The Cl0p Bust Shows Exactly Why Ransomware Isn't Going Away. The Wired. Retirado de https://www.wired.com/story/cl0p-ransomware-russia-putin-biden/.

Phillips, K G. (2013). Unpacking cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain. National Defense University Press. JFQ issue 70, 3rd quarter 2013.

RAND Corporation (2015). The US-China Military Scoreboard. Retirado de https://www.rand.org/content/dam/rand/pubs/research_reports/.

Rid Thomas, 2013. *Cyber War Will Not Take Place*: London, C Hurst & Co Publishers

Ltd.

RR300/RR392/RAND_RR392.pdf Rask, M. (March 8, 2017). China's evolving cyber warfare strategies. Asia Times. Retirado de http://www.atimes.com/article/chinas-evolvingcyber-warfare-strategies/.

Ou, Si-Fu (OCT 2018). China Cyber Corps and Strategies. Taiwan Institute for National Defense and Research. Defense Security Briefing, Volume 7, Issue 1.

Perkovich, G., & Levite, A. E. (2017). Understanding Cyber Conflict, 14 Analogies. Washington D. C.: Georgetown University Press.

Singer PW, Friedman Alan, 2014. *Cybersecurity and Cyberwar, What Everyone Needs to Know*: New York, Oxford University Press.

Tofler, A., & Tofler, H. (1993). War and Anti-War, Survival at the Dawn of the 21 Century. London: Little, Brown and Company.

UN Geneva Agreements 1954, 20-21 (July 1954). Retirado de https://peacemaker.un.org/sites/peacemaker.un.org/files/KH-LAVN_540720_GenevaAgreements.pdf.

Wilson, Z. (April 4, 2001). Hacking: The Basics (versão PDF). SANS Institute: InfoSec Reading Room. Retirado de https://www.sans.org/readingroom/whitepapers/hackers/hacking-basics-95.