idn E-Briefing Papers

Conceito Estratégico de Defesa Nacional - "Espaço, Ciber e Novas Tecnologias Disruptivas"

Resumo da Conferência realizada na Universidade dos Açores, no dia 14 de dezembro de 2022, integrada no Ciclo de Eventos subordinados à revisão do Conceito Estratégico de Defesa Nacional.

Pedro Rito
Rui Garrido
Beatriz Barqueiro

CONCEITO ESTRATÉGICO DE DEFESA NACIONAL

idn Instituto da Defesa Nacional

Os *E-Briefing Papers* do Instituto da Defesa Nacional visam proporcionar o acompanhamento de temas e debates atuais nos planos da segurança internacional e das políticas de defesa nacional, incluindo resultados da investigação promovida pelo Instituto da Defesa Nacional, sobretudo na sua vertente aplicada e de apoio à decisão política, bem como contributos de outros analistas e investigadores associados do Instituto.

FICHA TÉCNICA

Diretora
Isabel Ferreira Nunes

Coordenação Científica
Isabel Ferreira Nunes

Editor
Luís Cunha

Centro Editorial
António Baranita e Luísa Nunes

Propriedade, Edição e *Design* Gráfico
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa, Portugal
Tel. + (351)211 544 700 **Fax**: + (351)211 548 245
Email: idn.publicacoes@defesa.pt
http://www.idn.gov.pt

ISSN: 2184-8246

Conceito Estratégico de Defesa Nacional – "Espaço, Ciber e Novas Tecnologias Disruptivas"

Resumo da Conferência realizada na Universidade dos Açores, no dia 14 de dezembro de 2022, integrada no Ciclo de Eventos subordinados à revisão do Conceito Estratégico de Defesa Nacional.

Pedro Rito

Rui Garrido

Beatriz Barqueiro

Conteúdo

Sessão de Abertura

Professora Doutora Isabel Ferreira Nunes
Diretora do Instituto da Defesa Nacional

Excelentíssimo Senhor Professor Doutor Artur José Freire Gil, Vice-Reitor da Universidade dos Açores, na pessoa do qual cumprimento as demais autoridades, entidades e convidados presentes.

O Instituto da Defesa Nacional (IDN) foi mandatado para organizar um conjunto de eventos de debate público, antecedendo a elaboração das Grandes Opções do Conceito Estratégico de Defesa Nacional e contando, em certos casos, com a colaboração de instituições de ensino superior na promoção de uma discussão informada e descentralizada, sobre matérias relevantes na área da segurança e defesa.

Este ciclo de debate e reflexão, que iniciámos em outubro no Instituto da Defesa Nacional, seguido de Braga, Coimbra, Madeira e Évora, encerra-se hoje na Universidade dos Açores, num total de cinco conferências. A conferência sobre "Espaço, Ciber e Novas Tecnologias Disruptivas" compreende um conjunto de matérias que se revestem da maior relevância, porquanto representam domínios não tradicionais da defesa e cuja expressão exige uma ligação estreita entre os órgãos da governação, as instituições do complexo científico-tecnológico, as empresas e outros organismos relevantes daqueles setores.

A eclosão da Guerra na Ucrânia veio revelar o quão a combinação entre a digitalização da guerra por um Estado, a exploração de plataformas espaciais e a utilização inteligente de tecnologias disruptivas, como a inteligência artificial, suplementam e fortalecem a capacidade de resiliência dos cidadãos face a um ataque deliberado e multidimensional de uma grande potência.

No garante da continuidade de serviços críticos, muito tem contribuído o setor do designado "Novo Espaço", o setor da economia digital e a presença de decisores que valorizam a inovação, o investimento tecnológico e o espírito empreendedor.

É manifesto o interesse de diversas entidades na democratização e comercialização dos serviços baseados em plataformas espaciais, sendo notória a sua presença crescente na gestão quotidiana das sociedades. No entanto, a sua relevância crítica para a defesa nacional apresenta-se como uma novidade absoluta que não pode ser negligenciada. O Conceito Estratégico de Defesa Nacional em revisão incluirá, por certo, o domínio espacial como um domínio de afirmação de soberania nacional no âmbito dos bens comuns globais.

Alinhando as decisões de política nacional com as de nível europeu, transatlântico e dos seus aliados internacionais, Portugal estabeleceu o desígnio da exploração do espaço e das tecnologias associadas, através da aprovação de um conjunto de documentos fundamentais como a Estratégia Nacional Portugal Espaço 2030; a Lei do Espaço de 2019; tendo criado uma autoridade espacial, desempenhada provisoriamente pela ANACOM e aprovado em 2020[1] a Estratégia da Defesa Nacional para o Espaço 2020-2030. Esta veio estipular os objetivos estratégicos, definindo um Plano de Ação que materializa o Programa Espacial da Defesa e potencia a interligação com outras entidades.

No quadro da cibersegurança foi aprovada a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, contribuindo para a definição conceptual e para a definição dos contextos de identificação, análise, reporte e mitigação das ameaças no domínio do ciberespaço.

O Ministério da Defesa Nacional ativou células para acompanhamento e participação em diversos programas europeus, nomeadamente o consórcio *Space Surveillance and Tracking*, com uma forte implantação no arquipélago dos Açores[2]. No capítulo exclusivamente militar, com a aprovação da nova LOEMGFA, foi criado o Departamento do Espaço, que integra o Centro de Comunicações e Informação, Ciberespaço e Espaço do EMGFA. Do mesmo modo que reforçará o quadro de atuação do Centro Nacional de Cibersegurança, no enquadramento dado pelas decisões decorrentes da recentemente aprovada Bússola Estratégica da União Europeia com a constituição de uma *CyberToolbox* da União Europeia e da equipa de *Cyber Rapid Reaction* no contexto NATO.

É conhecida a importância geoestratégica do arquipélago dos Açores, ligando a Europa e a América do Norte. O setor do Espaço e o domínio ciber destacam e potenciam essa importância, especialmente porque tem características únicas nos contextos nacional e da União Europeia. Deste modo, não podia haver melhor localização para debater novos domínios de interesse para a defesa nacional, sabendo-se que nos últimos anos têm vindo a ser instalados vários sistemas e um centro nacional de operações espaciais[3], em três ilhas do arquipélago, acompanhados de uma forma dedicada pelas autoridades regionais através da aprovação de legislação[4], assim como da elaboração de uma Estratégia dos Açores para o Espaço[5].

Por outro lado, à medida que o processo de digitalização da sociedade prossegue, assim foram sendo reveladas as potencialidades e as vulnerabilidades do domínio cibernético.

O Estado português tem promovido neste contexto um ambicioso programa de governo eletrónico ou *e-governance*, ao mesmo tempo que as empresas e restantes entidades públicas e privadas dependem crescentemente de plataformas digitais.

Os ativos deste universo recorrem hoje às vantagens tecnológicas decorrentes do uso de comunicações móveis de 5ª Geração e de um extenso complexo de redes interligadas, muitas delas sustentadas nas comunicações por cabos submarinos. Acidentes como aquele que isolou as Ilhas Shetland há cerca de dois meses, em que o corte, alegadamente acidental, de cabos submarinos, impactou no uso regular dos domínios ciber e espacial[6].

A Internet das Coisas surge como o novo paradigma que liga o mundo real e o digital. No domínio operacional começa a falar-se da Internet das Coisas Militares, no qual agentes oportunistas podem explorar vulnerabilidades, como demonstram os recentes ataques cibernéticos a empresas mediáticas e de telecomunicações nacionais, a sistemas de saúde e até à segurança social.

A Estratégia Nacional de Ciberdefesa, aprovada pelo Conselho de Ministros no mês passado, visa dotar as Forças Armadas das competências e capacidades necessárias à condução de operações militares nesse novo domínio, antecipando riscos, mitigando ameaças e criando as condições da reposição da segurança e a ordem. Aquela, sempre que articulada com a Estratégia Nacional de Segurança do Ciberespaço, aproxima os instrumentos nacionais daqueles utilizados pelas organizações de que Portugal faz parte, designadamente a União Europeia e a NATO.

Os domínios do espaço e cibernético são apoiados por sistemas de processamento e comunicações digitais, cuja programação é cada vez mais feita por recurso a formas de inteligência artificial. A transferência da decisão em ambiente de inteligência artificial começa a ser recorrente em determinados setores e a autonomia emerge como uma característica que terá de ser estudada e compreendida. A Inteligência Artificial surge como área de disputa geopolítica, com a China a pretender alcançar a liderança do setor, estabelecendo um regime de Inteligência Artificial Generalizada no ano de 2030.

Portugal fez aprovar, em 2019, uma Estratégia Nacional de Inteligência Artificial, alinhando os esforços nacionais com os da União Europeia na promoção do uso destas tecnologias na resolução de desafios globais, como são os da saúde, do clima, da segurança alimentar, energética ou da cibersegurança.

Por fim, as novas tecnologias emergentes e eventualmente disruptivas, como a quantum, a biotecnologia e a nanotecnologia, ocupam o horizonte especulativo das discussões

prospetivas pelas potencialidades e vantagens comparativas que poderão oferecer, bem como pelo elenco de desafios, completamente novos, que colocam à humanidade.

A reflexão que iremos promover hoje, concorrerá para o acervo de contributos que o IDN irá apresentar e terá, seguramente, consequências na formulação de um pensamento estratégico mais abrangente, interligado e estruturante, visando o conhecimento e a exploração de domínios decisivos para a segurança e defesa nacional, bem como o contributo nacional para as organizações internacionais que o país integra, em especial a União Europeia e a NATO.

Minhas senhoras e meus senhores,

Para terminar gostaria de agradecer a colaboração da Universidade dos Açores, que amavelmente nos acolhe na pessoa do seu vice-reitor, destacando ainda os especiais contributos do Professor Doutor Luís Andrade, nosso interlocutor há muito tempo, e do Professor Doutor Ricardo Teixeira, pró-reitor para a Comunicação, Qualidade e Imagem da Universidade dos Açores, cuja intervenção foi decisiva na operacionalização desta conferência.

Agradeço o contributo de todos os oradores e moderadores desta conferência.

Ao Coronel António Eugénio agradeço o seu profissionalismo, dedicação e empenho na organização desta conferência por parte do Instituto da Defesa Nacional.

Uma última nota gostaria de dedicar a todos os presentes nesta última conferência, agradecendo-lhes o manifesto interesse nesta matéria central à defesa nacional, honrando-nos com a sua presença. Obrigada.

Professor Doutor Artur Freire Gil
Vice-Reitor da Universidade dos Açores

Em nome da Magnífica Reitora da Universidade dos Açores agradeço o convite que lhe foi endereçado para estar aqui presente. É para nós uma honra acolher mais um evento do IDN na Região Autónoma dos Açores, desta vez dedicado à cada vez mais discutida temática do "Espaço, Ciber e as Novas Tecnologias Disruptivas".

A contribuição da Universidade dos Açores para a promoção de um cluster espacial nos Açores é, desde há muito, uma prioridade estratégica, como provam a sua acreditação como academia Copernicus (2017), a criação do grupo de trabalho para a promoção das Ciências do Espaço (2019) e a sua contribuição para a discussão pública da Estratégia Regional dos Açores para o Espaço (2021).

Nesta contribuição, reafirmamos a nossa total disponibilidade para sermos o parceiro estratégico público de excelência do Governo Regional dos Açores para o apoio à implementação da referida estratégia, com o objetivo claro e inequívoco de contribuir ativamente para o desenvolvimento de aplicações com base em dados espaciais, a instalação de locais de ensaio para tecnologias espaciais, integração de redes e para a promoção de um mais amplo e seguro acesso ao espaço, promoção da investigação e desenvolvimento e inovação sobre o espaço, a divulgação e educação científica para o espaço e, finalmente, para a especialização académica e capacitação técnica no domínio do espaço e das aplicações geoespaciais.

Estamos, portanto, à disposição do país e da Região Autónoma dos Açores para o que for necessário para que este desígnio, tanto regional como nacional, se concretize e contribua decisivamente para a nossa segurança e para os nossos desenvolvimentos científico, tecnológico e socioeconómico.

Engenheiro Paulo Quental
Coordenador da Estrutura de Missão dos Açores para o Espaço

Cumprimento os meus colegas de mesa, excelentíssimo Vice-Reitor Doutor Artur Gil e excelentíssima Senhora Diretora do Instituto de Defesa Nacional, Doutora Isabel Nunes, a quem agradeço o convite e a organização deste evento aqui nos Açores, principalmente com o tema do setor do espaço, que nos é tão querido e tão importante para a região.

Gostaria, também, de deixar uma nota relativa à impossibilidade de nenhum membro do Governo Regional estar presente nesta sessão, mas é, de facto, uma semana fundamental na Assembleia Legislativa Regional e, consequentemente, os membros do governo não conseguiram ter disponibilidade para comparecer, tendo delegado em mim esta apresentação.

Trago uma mensagem do Senhor Presidente do Governo Regional que, em várias vezes e de forma explícita, afirmou o compromisso do Governo Regional com o setor espacial. Assim, temos a oportunidade de apresentar o que se perspetiva desenvolver, aqui nos Açores, bem como outras considerações que possam ser tidas em conta na revisão do Conceito Estratégico de Defesa Nacional. Tal surge como uma oportunidade para potenciar o ecossistema espacial dos Açores, que não deixa de ser, em si, parte do ecossistema espacial nacional.

Quando falamos de uma estratégia espacial para Portugal, esta passa por um vínculo criado para a sua implementação, bem como para o potenciamento do crescimento económico e da criação de empresas. Estas deverão cooperar de forma próxima com a Agência Espacial Portuguesa, a única organização nacional cuja sede fica aqui na região Autónoma dos Açores.

Também, e como forma de focar a relevância estratégica dos Açores, aludo ao caráter inovador da Lei do Espaço e às condições que apresentou, em 2019, aquando da sua aprovação em Conselho de Ministros. De facto, em Portugal quando se pensa ou legisla o acesso ao espaço, os Açores adquirem um papel preponderante, pois apresentam as condições técnicas necessárias para que se possa desenvolver a atividade espacial em segurança.

Neste sentido, relembro que o setor espacial em Portugal tem um ecossistema com cerca de seis dezenas de empresas e centros de investigação, que têm a maior parte da sua atividade no continente. No entanto, a Região Autónoma dos Açores, e também a Região Autónoma da Madeira, apresentam um enorme potencial para o desenvolvimento tecnológico e para a

criação de capacidades no setor espacial nacional. Acrescento, ainda, que a política espacial é uma responsabilidade do Estado, como tal, os Governos Regionais têm um papel importante a desempenhar, seguindo uma lógica de cooperação no princípio da subsidiariedade.

Finalmente, gostaria de agradecer a todos os presentes o interesse em participarem nesta sessão e, em nome do Governo Regional, prestar um agradecimento à motivação e à cooperação estreita para desenvolver não só este processo que está a ocorrer, como também outros que estão a desenrolar e que compartilham uma grande utilidade ao país.

Keynote Speech:

"Relevância Estratégica do Ecossistema Espacial Açoriano"

Engenheiro Paulo Quental
Coordenador da Estrutura de Missão dos Açores para o Espaço

Localização Estratégica

A importância geoestratégica dos Açores tornou-se patente logo após o seu povoamento, com o arquipélago a servir de porto seguro para as rotas comerciais atlânticas, bem como para a descoberta de outros territórios. Relembre-se que Cristóvão Colombo, em 1492, aportou em Santa Maria durante a sua expedição.

Avançando cinco séculos, até ao século XX, destaca-se a criação da Base das Lajes (na década de 1930), enquanto aeroporto militar relevante e cuja importância viria a ser incrementada e vincada com a Segunda Guerra Mundial (tendo sido chave para os Aliados) e todo o período da Guerra Fria, mantendo-se relevante, ainda, na atualidade. Numa perspetiva civil, refira-se o aeroporto de Santa Maria, com mais de 75 anos de operação, que durante grande parte dos anos 60 e 70 do Século XX, foi o principal ponto de paragem técnica em travessias aéreas transatlânticas. Este potenciou, ainda, Santa Maria enquanto primeiro ponto de entrada, por via aérea, na região.

Atualmente a relevância geoestratégica dos Açores continua a existir no âmbito da navegação de lazer, bem como enquanto porto de abrigo para a navegação mercante. No entanto, de um ponto de vista aeronáutico, esta é cada vez menos relevante em virtude dos avanços tecnológicos que permitem o voo transatlântico sem condicionantes. Ainda assim, a geografia açoriana ainda se revela como uma linha extra de segurança para operações aéreas, sendo estas de carácter civil ou militar.

Ainda referindo a importância geoestratégica dos Açores, deve-se ressalvar que o arquipélago surge como um *pivot* atlântico da Europa, conferindo a esta uma vertente de centralidade no Atlântico. Tal permite à região prestar um importante serviço não só ao país, como também à Europa, nomeadamente atendendo à realidade do continente após os acontecimentos de 24 de fevereiro de 2022. Aí ficou patente que, no âmbito espacial, a Europa deve apostar na cooperação, mas também deve ser autónoma na sua capacidade de atuar neste domínio.

Deve-se salientar a importância dos Açores enquanto parte fundamental da proposta de extensão da plataforma continental, ao mesmo tempo que se apresenta como a maior Zona Económica Exclusiva (ZEE) nacional (sendo maior que a ZEE do continente ou da

Madeira). Desta forma, a capacidade espacial surge como um dos maiores aliados para a garantia das nossas responsabilidades soberanas dentro do espaço territorial marítimo que Portugal compreende, do que almeja alcançar, além da aérea de busca e salvamento que é da sua responsabilidade.

Acrescento, ainda, a importância da FIR – Área de Controlo e Tráfego Aéreo e Oceânico de Santa Maria, que tende a coincidir com a área de busca e salvamento, cuja localização e capacidade de coordenação se apresentam como potenciadores de novas tecnologias espaciais.

New-Space

O *New Space* é uma tendência que se vem estendendo desde há 15 ou 20 anos, colocando-se a questão se deve ser, de facto, assim denominado. Para todos os efeitos, este é um setor que se encontra em franco crescimento, sendo este medido tendo como referência o investimento privado que atrai. De facto, o *New Space* permitiu que o espaço deixasse de ser altamente institucionalizado e apenas acessível aos Estados, passando a incluir entidades privadas que, cada vez mais, se apresentam como peças importantes para a estratégia espacial, nomeadamente de países recém-chegados a este domínio.

Este conceito, o de *New Space*, está profundamente ligado ao empreendedorismo, com os serviços no espaço a estarem globalmente disponíveis e fazendo parte do nosso dia-a-dia (uso de GPS ou televisão por satélite), fruto de uma acessibilidade generalizada ao espaço. Ou seja, o desafio é como ajudar a criar mais e melhores comunicações e produtos de valor acrescentado na Terra, pois por muito que nos impressionem os lançamentos espaciais, estes são apenas tão úteis na medida da utilidade, na Terra, da tecnologia desenvolvida.

No especto económico, em 2020, a economia do espaço estaria avaliada em 371 mil milhões de dólares, 386 mil milhões em 2021, notando-se um claro crescimento (mesmo em anos de pandemia) atestando a resiliência deste setor que, juntamente com outros com quem compartilha complexidade e resiliência, nos torna mais capazes de enfrentar cenários de crise. Atendendo-se ao ano de 2021 será importante notar que os serviços de satélite (de televisão ou localização) compreendiam um valor total de 118 mil milhões de dólares, dos quais 45 mil milhões são referentes apenas aos Estados Unidos. O setor de lançamentos espaciais apresentou-se com um valor na ordem dos 5,7 mil milhões; tal surge como confirmação do potencial deste filão de mercado que poderá ser explorado nos Açores.

Reforçando a ideia de crescimento e resiliência desta indústria, entre 2009 e 2020, o crescimento desta foi constante, se excluirmos os anos de 2015 e 2016, tendo tal reflexo não

só nas capacidades existentes, como também no aumento crescente do número de *start-ups* de âmbito espacial (sendo 2021 um ano particularmente marcante), apoiado, por vezes, por *danger capital* (capital de risco).

No entanto, o *New Space* não pode ser visto como algo em que *os stakeholders* e investidores são apenas os privados. Aliás, a Space X, bandeira do *New Space,* apenas consegue operar graças ao grande financiamento desta por parte da NASA. Evidentemente tal permitiu à Space X desenvolver tecnologia inovadora, ao mesmo tempo que permitia à NASA reduzir significativamente os seus custos de operação.

Com o horizonte em 2040, tem-se como principais *drivers* da economia *New Space* o lançamento de satélites, a internet por satélite (já acessível, mas cada vez mais fiável), a exploração do espaço profundo (catalisadora de tecnologias de uso comum que tenham sido desenvolvidas para a exploração espacial), o regresso à Lua, a observação da Terra (visível e eletromagnética), a mineração de asteroides, os problemas associados aos detritos espaciais (com a Defesa Nacional a ter um papel preponderante neste campo), o turismo espacial (que não deve ser visto como um capricho daqueles com vastos meios, mas antes uma forma de financiar a tecnologia espacial e de acesso ao espaço), a investigação científica em órbita e o fabrico em órbita e na terra (como motores impressos em 3D ou lançadores a baterias).

Perante esta realidade descrita nos parágrafos anteriores, encontrámo-nos perante a decisão de seguir por uma bolha de crescimento ou apostar em algo com um crescimento menos acentuado, mas que se apresenta sustentável ao longo do tempo, tendo como base o conhecimento e a inovação. Para a implementação de um ecossistema espacial sustentável (não apenas a nível ambiental, mas acima de tudo económico) nos Açores, a segunda opção apresenta-se como o caminho a trilhar. Desta forma, dever-se-á envolver as comunidades, identificar as atividades que possam desenvolver o potencial existente e atrair *start-ups* ou novas empresas.

Ecossistema Espacial dos Açores

O Ecossistema Espacial dos Açores compreende, entre outros: 1) o Centro de Operações Nacionais do SST, na Ilha Terceira, operando quatro telescópios para a monitorização de detritos espaciais; 2) o AIR Centre, na Terceira, centro de investigação focalizado no uso de dados espaciais para estudar a bacia do Atlântico, as bacias costeiras dos oceanos e o ecossistema das ilhas; 3) a Rede Atlântica de Estações Geodinâmicas e Espaciais (RAEGE) na Ilha das Flores, com uma estação em fase de desenvolvimento e capacitação, havendo a ambição futura de aí se colocar um telescópio; 4) o Teleporto de Santa Maria (operado por

uma empresa privada com ligações à Defesa), a Galileu Sensor Station (que apoia a calibração dos satélites europeus Galileu), a antena de acompanhamento dos lançamentos da Agência Espacial Europeia (ESA) (a partir da Guiana Francesa), a antena do programa europeu de monitorização meteorológica e a antena de comunicações do espaço profundo da Agência Espacial Portuguesa (que permitirá que Portugal participe em missões da ESA, tendo, também, uma aplicação comercial). 5) a Rede Atlântica de Estações Geodinâmicas e Espaciais (RAEGE), na Ilha de Santa Maria (esta tem a capacidade de estudar as placas tectónicas fazendo uso de dados espaciais, compreendendo, também, um telescópio).

Perspetivas Futuras

A Estratégia dos Açores para o Espaço foi apresentada, na sua forma inicial antes de consulta pública, em novembro de 2021, com a sua redação final a ser apresentada brevemente. Neste documento, Santa Maria deverá afirmar-se como ponto de acesso e retorno do espaço, incluindo de veículos com capacidade de realizar experiências em microgravidade (de grande relevo para a investigação de materiais e produtos farmacêuticos). Este projeto servirá de pivot para a criação de um centro tecnológico que permita fazer a integração e manipulação de cargas úteis, criando sinergias para mais projetos relacionados com o espaço (indo da integração de lançadores a veículos de teste).

Também perspetivamos a criação de um centro de testes de motores e componentes em Santa Maria, tirando proveito das cerca de 40 *start ups* europeias que se dedicam a este setor de negócio, sendo necessária celeridade para lhes apresentar esta capacidade. No entanto, a maior ambição é a criação de um porto espacial.

Tecnologias Disruptivas

Podemos olhar para uma série de tecnologias que, ainda não se podendo afirmar como disruptivas, perante determinados avanços tecnológicos poderão atingir esse patamar. Podemos tomar como exemplo o lançamento horizontal de acesso ao espaço (que já conta com cinco lançamento bem-sucedidos), permitindo o envio de satélites entre os 300 e os 400 quilogramas para órbitas baixas terrestres (até 800 km), órbitas estas preferenciais para comunicações de baixa latência, bem como para observação terrestre. Estas operações poderão decorrer de aeroportos convencionais, com os satélites a desacoplarem-se da aeronave a usarem os seus motores para atingirem a órbita pretendida. Santa Maria afirma-se como bem capacitada em virtude do seu aeroporto.

Também o lançamento espacial através de plataformas marítimas se apresenta como bastante interessante para os Açores, pois conseguimos ter muitos dos sistemas de apoio e seguimento em terra, com esse tipo de plataformas a ser compatível com a nossa realidade territorial. A vantagem desta forma de lançamento prende-se com a capacidade de contornar as regras de lançamento a partir de terra, que condicionam o tipo de lançadores que podem ser utilizados. Assim, numa perspetiva de médio-longo prazo e se quisermos que sejam operados lançadores de maiores dimensões aqui nos Açores, esta solução apresenta-se como uma das alternativas mais fiáveis. Esta valência já despertou o interesse de outros países como a Espanha (a partir das Canárias) ou a Alemanha (Mar do Norte).

Outra tecnologia disruptiva onde a Região Autónoma dos Açores pode ser um importante contribuinte surge na figura dos *space planes*. Estes meios de transporte suborbitais servem de ligação entre pontos terrestres, com a geografia açoriana a permitir a criação de zonas de exclusão que conferem maior segurança ao teste destas naves.

Os voos suborbitais surgem como mais uma hipótese a desenvolver em Santa Maria, havendo a possibilidade de se estabelecerem as condições necessárias à sua operação em 2023. Estes sistemas não permitem uma efetiva colocação em órbita de determinado objeto, no entanto mostram-se valorosos para a acreditação de material ou para o teste de equipamentos a orbitar.

Destaca-se, por último, os voos de Gravidade zero (em que aeronaves que descrevem padrões de voo balístico permitem, durante curtos períodos, simular a ausência de gravidade), os balões estratosféricos (de grande utilidade para missões de vigilância e soberania, permitindo a observação de uma área superior a 300km, ou servindo como *relay* de comunicações em determinados cenários) e aeronaves não tripuladas, que se apresentam como soluções de exploração interessante para os Açores.

Cooperação e Atratividade

Para conseguir desenvolver e implementar as ideias anteriormente referidas, será necessário recorrer a uma cooperação entre os diversos *stakeholders*. Se, por um lado, é reconhecido que a racionalização de recursos nos impede de dispor de grandes verbas para atrair investimento (ao contrário de outros países que podem subsidiar a instalação de empresas no seu território), será na agilização de processos que encontraremos a referida atratividade. No entanto, tal não significa uma redução no nível de exigência para licenciamentos. Neste âmbito, adquirem especial importância a Agência Espacial Nacional e a Agência Espacial Europeia.

No âmbito da cooperação, não pode deixar de ser referido o papel fundamental da Defesa para as atividades espaciais, nomeadamente na questão de coordenação do espaço aéreo e marítimo.

Finalmente, dever-se-á reforçar que o facto de os Açores possuírem um vasto leque de capacidades contidas numa área territorial relativamente pequena apresenta-se como uma das principais vantagens competitivas da região no que toca ao Espaço.

Painel:

"Espaço, Ciber e Novas Tecnologias Disruptivas"

Coronel João Barbas
Assessor de Estudos do Instituto da Defesa Nacional

A dependência das sociedades atuais do uso das tecnologias de informação e comunicação (TIC) é hoje um dos maiores desafios em matéria de cibersegurança. As TIC conheceram um considerável salto tecnológico nas últimas três décadas que permitiu aproximar as sociedades. Exemplo disso é a transmissão em direto da conferência em causa. Mas há outros avanços no campo das tecnologias do Espaço e emergentes, bem como nas tecnologias disruptivas, que devem muito às tecnologias de informação e comunicação. Neste sentido, é fundamental a reflexão em torno da governação de cibersegurança, em especial ao nível da gestão das organizações.

O termo ciber-resiliência deve o seu cunho ao Fórum Económico Mundial, que numa publicação dedicada ao tema, aborda a questão com uma ênfase na questão da liderança, na estratégia da cultura, bem como na gestão de topo das organizações e a sua corresponsabilização. Não é viável termos segurança sem um contributo de todos. No mundo real é impossível termos segurança em todos os lugares, a todo o momento. Essa impossibilidade, desde logo em termos de meios e recursos, implica uma avaliação dos riscos e uma seletividade das áreas de atuação. Assim, no espaço cibernético, e à semelhança do mundo real, é necessário fazer uma avaliação dos riscos, observando as dinâmicas dos *hot spots* e investir um maior esforço de segurança nessas zonas mais críticas. Assim, no ciberespaço deve ser tido o mesmo cuidado, em termos de segurança, que na vida real.

O ciberespaço é caracterizado por um domínio de redes e infraestruturas interdependentes de informação, que inclui a internet, as redes de telecomunicações e de computadores, bem como a integração de processadores e controladores. A transformação do paradigma da comunicação, no sentido da sua digitalização, resultou numa massificação da comunicação de dados que, por sua vez, foi transferida para o ciberespaço. Esta massificação de dados impõe que sejam tomadas medidas no sentido da minimização dos riscos. No entanto, o ciberespaço apresenta um conjunto de forças e oportunidades que devem ser exploradas, mas também fraquezas e ameaças, em especial as ações de caráter ofensivo e as dificuldades em defender. A disponibilidade da infraestrutura da internet que interliga todas as redes corporativas e os dispositivos, tem um custo associado, uma vez que foi inicialmente pensada

para ser redundante, para ser interoperável. É esta interoperacionalidade que permite a comunicação com qualquer computador no mundo a partir de equipamentos de diferentes fabricantes. Esta interoperacionalidade comporta um risco. Este advém, sobretudo, dos atores que pretendem influenciar a vida pública e que, para tal, interagem na esfera do ciberespaço com esse propósito de condicionar ou influenciar os demais utilizadores. A questão que se impõe é saber como lidar com esse risco.

Neste sentido, temos de pensar em termos de segurança no ciberespaço. Assim é a cibersegurança. O termo suscita várias interpretações, sendo muitas vezes rotulado como uma questão de caráter estritamente tecnológico, mas hoje está relativamente consensualizado que se trata de uma questão de gestão. E deve ser gerido pelas organizações de uma forma holística, compreendendo também a dimensão e os componentes tecnológicos. Por isto mesmo, é uma responsabilidade das organizações a sua gestão, não se podendo delegar exclusivamente nos departamentos de sistemas de informação a responsabilidade pela cibersegurança, pois eles são apenas um dos elementos nessa teia complexa da cibersegurança. A *Estratégia Nacional de Segurança e Ciberespaço* (2019) define a segurança como um conjunto de medidas e ações que procuram prevenir, monitorizar, detetar, reagir, analisar e corrigir situações para uma manutenção de um estado de segurança satisfatório, mas também como forma de garantir a confidencialidade, a integridade, a disponibilidade e o não repúdio da informação das redes, sistemas e pessoas em interação no ciberespaço.

No que concerne à gestão dos riscos, é imperativa a identificação do risco através do cruzamento do conhecimento dos ativos da organização. Um desses ativos é o *big data*, que resulta de informação que é disponibilizada voluntariamente no ciberespaço, mas que é importante proteger da captura de dados ou aquisição abusiva por terceiros. Assim, as organizações devem conhecer bem os seus ativos para, a partir daí, identificar as ameaças e vulnerabilidades. É através desta avaliação cruzada que é possível aferir o risco associado. O *Quadro Nacional de Referência para a Cibersegurança* (2019), em conformidade com a norma internacional ISO 2705, esquematiza a gestão do risco como um exercício de identificação de vulnerabilidades, estabelecimento de prioridades para fazer face ao inerente grau de incerteza. Estas medidas, de acordo com os padrões internacionais, devem ser implementadas de forma progressiva, tendo sempre em mente o conhecimento que a organização dispõe.

Face ao supramencionado, há outro aspeto a ter em consideração e que é a ciber-resiliência. Este conceito não tem uma definição consensual, mas, no essencial, deve atender à

capacidade de antecipação e adaptação para resistir a um evento disruptivo, procurando lidar com o seu impacto e o risco envolvido. As organizações devem, assim, adotar medidas para a sua minimização, em conformidade com os padrões e legislação internacional e nacional – como no caso de Portugal, que publicou recentemente a *Estratégia Nacional para a Ciberdefesa* – bem como a necessidade de observar requisitos de *compliance* e exigências regulamentares. A observância destas regras é essencial para orientar a política de segurança da organização, a qual e, através da avaliação dos riscos, permitirá à organização a produção de mecanismos de controlo – não necessariamente mecanismos tecnológicos –, que podem ser organizacionais, humanos, físicos e tecnológicos, isto é, as organizações têm mecanismos de controlo em camadas que deverão usar de forma adaptativa consoante a avaliação do risco efetuada.

Apesar disto, as tendências atuais na área da cibersegurança apontam para, desde logo, uma lacuna na sensibilização e ou consciencialização para a necessidade de uma estratégia para a segurança da informação. Verifica-se, também, uma desconformidade da estratégia das organizações, tendo em consideração aquela que é a sua área de negócio ou atividade, com aquela que é a sua estratégia de cibersegurança. Esta desconformidade, não raras vezes, resulta numa priorização das soluções de natureza técnica, em detrimento dos ajustes organizacionais que serão mais eficazes na resolução de problemas. Por fim, há uma ausência de uma arquitetura organizacional orientada para os sistemas de informação.

A Governação da Segurança da Informação (GSI) procura, desta forma, auxiliar uma organização no processo de orientação e controlo no estabelecimento de uma cultura de segurança, respondendo de forma adequada aos requisitos de segurança da organização. A cultura de segurança enquadra vários fatores, sejam crenças, comportamento, capacidade e ações. A GSI deve contribuir para um efetivo alinhamento da segurança e da informação, com a atividade da organização. Deve procurar a gestão do risco, através de execução de medidas de gestão e mitigação de riscos, bem como na redução dos seus impactos. A GSI deve ainda priorizar a valorização e otimização dos investimentos dos sistemas de informação, a gestão dos recursos e a medição da performance. A concretização da arquitetura de Governação da Segurança da Informação deve, assim, obedecer a cinco eixos essenciais, que são: 1) o alinhamento estratégico; 2) a gestão eficaz dos riscos; 3) o valor acrescentado da atividade; 4) a gestão – eficiente – dos recursos; e, 5) a medição da performance.

No entanto, existem situações e factos que contribuem para uma ineficácia ou inadequação da GSI. Desde logo, porque é prática comum a concentração da responsabilidade num único

departamento dentro da organização, por regra, departamento de sistemas informáticos. Por outro lado, contribui para a sua ineficácia a falta de envolvimento das direções das organizações, desde logo ao nível do recrutamento de quadros não são escrutinados sobre as suas competências para as áreas específicas. Outros fatores que concorrem para o fraco desempenho da GSI são o desenho e a correta implementação de políticas e diretivas de segurança, mas também os projetos e as iniciativas que não estão adequados com aqueles que são os eixos da estratégia de segurança da organização.

Em sentido oposto, uma GSI eficiente e eficaz é aquela em que: 1) toda a organização é envolvida – com o conhecimento dos ativos e respetiva definição das medidas de segurança a aplicar; 2) existe a definição das responsabilidades – as quais devem envolver a direção da organização e a gestão nos processos de decisão, mas também os níveis intermédios, no sentido de uma melhor definição, implementação e aplicação de políticas e estratégias; 3) o nível de proteção vai depender do nível do risco – o que se traduz em distintos níveis de risco consoante a área de atuação da organização; e, 4) a Segurança tem de ser gerida de forma ativa através de políticas, normas e orientações concretas.

Em jeito de conclusão, e recordando Robert Mueller, as organizações necessitam de ser ciber-resilientes.

Coronel António Eugénio
Assessor de Estudos do Instituto da Defesa Nacional

Dirigir esta breve comunicação sobre tecnologias disruptivas, inserida no ciclo de eventos de revisão do Conceito Estratégico de Defesa Nacional apresenta-se como uma honra. E porque é que é importante falar deste assunto? Porque se antecipa que estas tecnologias tenham um impacto transformacional nas operações militares, nas capacidades de defesa e no espaço de decisão política. Depois, também, porque os países europeus procuram organizar-se, através da União Europeia, no sentido de obter uma maior autonomia estratégica nestas matérias.

Como temos vindo a assistir diariamente desde há cerca de 10 meses nos órgãos de comunicação social, a propósito da Ucrânia, a guerra continua presente nas relações entre Estados, como mecanismo de resolução de contendas. Tem sido assim, infelizmente, ao longo da História da Humanidade. A guerra é um produto de cada época. As partes em conflito servem-se de utensílios gerados por uma determinada base industrial e tecnológica, intimamente ligada à economia e ao poder. Se houve uma altura em que o poder provinha da posse de terra, a base tecnológica e os materiais utilizados para produzir alfaias agrícolas eram também aqueles que eram utilizados nas batalhas. O dote principal dos guerreiros de então seria a perícia em manejar o armamento, muito assente na força física. Assim aconteceu, também, com a revolução industrial, onde a emergência das plataformas motorizadas deu origem a uma expansão tridimensional do espaço em disputa, envolvendo carros de combate e demais viaturas terrestres, navios e aeronaves, bem como a procura da respetiva mestria na sua operação. A revolução informacional iniciada nos anos 60 do Século XX alargou ainda mais esse espaço, acrescentando domínios mais sofisticados, como os espaços sideral e ciber e o espetro eletromagnético. Trouxe, também, a participação das mulheres para a liça. A força física deu lugar ao intelecto, como capacidade decisiva para fabricar e utilizar os complexos sistemas de armas.

Assistimos atualmente a uma nova corrida armamentista entre as grandes potências. O pano de fundo desta corrida é caracterizado, essencialmente, por um combate pelo conhecimento científico-tecnológico e pela vantagem de decisão.

O estudo da Organização da Ciência e Tecnologia (Science & Technology Organization – STO) da NATO distingue três tipos de tecnologias: Emergentes, Disruptivas e Convergentes.

Comecemos pelas emergentes que são definidas como embrionárias e bastante especulativas. Envolvem:

1. As tecnologias quânticas que exploram determinadas particularidades físicas da escala atómica e subatómica, designadamente o entrelaçamento e a sobreposição quântica, nas seguintes aplicações: criptografia, computação; navegação de precisão e temporização; sensores diversos e de processamento de imagem, comunicações e materiais. Se vingarem, a geração de computação que se avizinha tornará obsoleta toda a infraestrutura existente, especialmente as técnicas de proteção digital, por força da quebra fácil de chaves criptográficas.
2. As biotecnologias utilizam organismos, tecidos, células ou componentes moleculares derivados de organismos vivos para atuar noutros organismos vivos, em componentes celulares, incluindo o material genético. As tecnologias de melhoramento humano são definidas por intervenções biomédicas que aumentam o desempenho humano para além do que é exigido para restaurar ou manter a saúde.
3. Os novos materiais e manufatura tratam de materiais artificiais, com propriedades novas e únicas, cujo processo de fabrico resulta de nanotecnologia e de biologia sintética. Exemplos: revestimentos que resistem ao calor extremo, estruturas internas blindadas, coberturas furtivas, que oferecem sofisticadas técnicas de camuflagem, colheita e armazenamento de energia, supercondutividade, sensores avançados e descontaminação, produção massiva de comida, combustível e outros materiais. Existe muito interesse em materiais designados bidimensionais, compostos por uma única camada de átomos e noutros com topologias inovadoras. Como exemplo, menciono o grafeno, o material mais forte, mais leve e mais fino que existe. Para se ter ideia, 3 milhões de camadas de grafeno empilhadas têm uma altura de apenas 1 milímetro. Por outro lado, existe muito interesse na manufatura aditiva (isto é, impressoras 3D) que podem criar sólidos a partir de modelos digitais pela adição de camadas, usados para prototipagem rápida, produção local de componentes para reparação de material militar, ou de peças únicas, como por exemplo na Estação Espacial Internacional.

Passemos, agora, às tecnologias consideradas pela STO como disruptivas. Estas são tecnologias ou descobertas científicas que, espera-se, tenham um efeito profundo, até mesmo revolucionário, nas funções de defesa, segurança e atividade geral. Neste caso, elas já estão

em uso, se bem que experimentalmente e o seu efeito disruptivo provém da sua massificação. Neste capítulo, apresenta-se a classificação com exemplos que nos chegam da Ucrânia, que se constitui, infelizmente, num autêntico laboratório de guerra.

O termo *Big Data* descreve os desafios relacionados com dados, em especial pelo seu volume, velocidade, variedade, veracidade e visibilidade. A digitalização crescente da sociedade, a proliferação de novos sensores, novos meios de comunicação, a internet das coisas e as redes sociais contribuíram para o surgimento de um oceano de dados. Podemos dizer que vivemos atualmente num verdadeiro *Big Bang* de dados.

A análise desses dados necessita da automatização e de ferramentas de compreensão e visualização, em ordem à produção de conhecimento. Estas técnicas abarcam um conjunto de áreas à volta das ciências de decisão, incluindo a inteligência artificial, a otimização, a modelação e simulação, a engenharia de fatores humanos e a investigação operacional.

Além das empresas designadas pela expressão *Big Tech*, especialmente americanas, também existem *Big States*, como a China e a Rússia, que tiram partido da análise de dados para alvejarem públicos que satisfaçam as suas estratégias, comerciais, no primeiro caso, e geopolíticas no segundo.

No caso da Ucrânia, as iniciativas do portal de governo eletrónico *diia* (que quer dizer "Ação" e é, também, um acrónimo ucraniano para "O Estado e Eu") permite um leque alargado de interações entre o Estado e os cidadãos, que vão desde o pagamento expedito de pensões, indemnizações por danos provocados pela guerra, carteira eletrónica até ao relato da presença de forças russas, que transformam cada cidadão num "combatente" da nova era. A ambição do ministro da transformação digital é que o Estado ucraniano seja como as plataformas que utilizamos no nosso dia-a-dia (desde o transporte aos serviços de entrega de refeições ou compras *online*) que esteja ao alcance de um clique, sempre que o cidadão necessite.

A inteligência artificial refere-se à capacidade das máquinas para executarem tarefas que normalmente requerem inteligência humana – por exemplo, reconhecimento de padrões, aprender com a experiência, tirar conclusões, fazer previsões, ou fazer qualquer coisa – quer digitalmente ou como uma camada de software por trás dos sistemas físicos autónomos.

No caso ucraniano, empresas americanas foram contratadas para fornecerem os seus serviços de reconhecimento facial para efeitos de controlo nas fronteiras, de cadáveres e prisioneiros de guerra, como é o caso da Clearview, e para escuta, tradução e transcrição automática de comunicações russas, no caso da Primer. A indústria ucraniana de armamento desenvolveu um sistema integrado para artilharia (o GIS ARTA), baseado em inteligência artificial, cuja melhor descrição popular é o Uber da artilharia, pela partilha da situação e atribuição de alvos à unidade mais bem posicionada para os alcançar.

A autonomia é a capacidade de um sistema responder a situações incertas através da composição e seleção entre várias modalidades de ação, de modo a alcançar objetivos baseados em conhecimento e de um entendimento contextual do ambiente em seu redor. É caracterizada por graus de comportamento autodirigido designados níveis de autonomia.

A robótica é o estudo do design e da construção de sistemas autónomos englobando todos os níveis de autonomia. Sistemas sem tripulação podem ser remotamente controlados ou agir independentemente, dependendo da missão.

No caso ucraniano, vemos a atuação de diversas tipologias de *drones*, por enquanto todos com um ser humano no circuito, mas com elevados graus de autonomia. A iniciativa "Army of Drones" tem em vista a recolha de donativos internos e externos para a constituição de diversas frotas de *drones*, usando meios de financiamento clássicos e originais, como as criptomoedas.
Enquanto domínio operacional, as características do espaço sideral incluem: a liberdade de acesso e de ação, um campo de observação global, a velocidade e a cobertura potencial dos sensores das plataformas espaciais.

Os desafios do designado "Novo Espaço" – democratização e comercialização – conduzido por empresas dedicadas já são evidentes no conflito da Ucrânia, com o apoio crítico prestado pela Strarlink no fornecimento de comunicações seguras por uma constelação de microssatélites. Outro exemplo são os serviços das firmas Maxar e outras, incluindo a portuguesa Geosat, no fornecimento de imagens para recolha de informações e de meios de prova na questão dos eventuais julgamentos por crimes de guerra.

Os sistemas de armas hipersónicos (mísseis e outros veículos) operam a velocidades maiores que Mach 5 (6.125 km/h) e utilizam a força gravítica (reentrada na atmosfera) ou propulsão por foguete, *scramjet* ou propulsão de ciclo combinado para obterem essa gama de velocidades. Têm a vantagem da velocidade dos sistemas balísticos com a manobrabilidade dos mísseis de cruzeiro. Podem utilizar apenas o efeito cinético ou conter diversos tipos de ogivas. As contramedidas são difíceis. Tome-se por exemplo o hipersónico *Kinzhal,* que a Rússia anunciou ter sido lançado sobre a Ucrânia, muito embora não tenham sido divulgadas provas convincentes desse emprego. Na Europa, só a França tem um programa dedicado à exploração destas tecnologias.

Por fim, relativamente ao grande grupo das tecnologias convergentes, que são agregados de tecnologias que são combinadas de uma maneira nova, de modo a criar um efeito disruptivo, apresento apenas um exemplo, discutido no estudo da STO, que menciona as tecnologias de fazer sentido (*sense making*) que resulta do efeito sinérgico de *Big Data & Advanced Analytics*, Inteligência artificial e Autonomia, a combinação de tecnologias que poderá ter mais impacto nas capacidades militares no horizonte de dez anos.

O uso de sensores inteligentes, distribuídos, ubíquos, baratos e interligados e de entidades autónomas (reais ou virtuais) produzirá um volume de dados que serão impossíveis de analisar com as metodologias e aproximações atuais.

Fazendo referência à aproximação da União Europeia a esta temática, deixo a definição de tecnologia disruptiva que podemos encontrar no Regulamento do Parlamento Europeu que cria o Fundo Europeu de Defesa. Este fundo, a par de outros mecanismos de cooperação no domínio da defesa, como a Revisão Anual Coordenada de Defesa, e a Cooperação Estruturada Permanente, pretendem estimular gradualmente a sincronização e o alinhamento dos ciclos de planeamento de defesa dos Estados-membros, visando um reforço da relevância estratégica da União Europeia.

As orientações para o desenvolvimento de tecnologias disruptivas provêm essencialmente de dois estudos prospetivos promovidos pela RAND Corporation Europe, o primeiro, com o horizonte de 2035, produzido para a Agência Europeia de Defesa em 2018 e outro, mais recente, dirigido ao Parlamento Europeu, com o horizonte de 2040. Na substância, estes estudos não variam muito do estudo da STO.

No âmbito da aprovação da Bússola Estratégica para a Segurança e a Defesa, a Comissão Europeia publicou dois documentos relevantes: um roteiro acercas das tecnologias críticas, que irão ser definidas por um Observatório dedicado, a implementar dentro da Comissão, e um plano de ação sobre as sinergias entre as indústrias civis, de defesa e do espaço. Esse plano inclui 11 ações para estímulo da fertilização cruzada entre tecnologias, a interoperabilidade, a estandardização e a demostração de programas emblemáticos.

Como realça o roteiro sobre as tecnologias críticas para a segurança e defesa da Comissão Europeia, é necessária uma maior interação entre as comunidades de investigação e desenvolvimento civis e da defesa. Portugal já desenvolveu um conjunto de estratégias setoriais relacionadas com as tecnologias disruptivas, tema deste painel. Dispõe, também, de uma Estratégia de Desenvolvimento da Base Tecnológica e Industrial de Defesa, recentemente revista pela Direção-Geral de Recursos da Defesa Nacional. A gestão da BTID e a interface com o Sistema Científico-Tecnológico está a cargo da idD, Portugal Defence, SA, cuja missão é, resumidamente, a gestão e a promoção nacional e internacional das indústrias de defesa portuguesas. A BTID inclui cerca de 400 entidades, a maioria das quais pequenas e médias empresas dos setores naval, aeronáutico, comunicações, espaço, segurança, robótica, automação e materiais. No entanto, aquilo que se verifica a nível nacional é um espelho das conclusões tiradas a nível europeu: a procura na defesa está fortemente fragmentada e dependente de países terceiros, devido à histórica separação estrita entre a pesquisa, o desenvolvimento tecnológico e a inovação civil e de defesa, assim como aos baixíssimos investimentos nesta área (em média na União Europeia, 1,2% do orçamento de defesa). Temos, assim, margem para melhorias, que passam por uma maior ligação entre as diversas comunidades interessadas, assim como o necessário investimento.

Em forma de conclusão, tomemos, para reflexão, a frase de Roy Amara: "tendemos a um deslumbramento tecnológico inicial para, depois, esquecermos os seus efeitos profundos no longo prazo".

Engenheiro Duarte Cota
Vogal da Estrutura de Missão dos Açores ara o Espaço

O nosso quotidiano é marcado pela facilidade que temos em comunicarmos com os outros, quer através de *messaging* ou outras plataformas de comunicação. Curiosamente, esquecemo-nos, muitas vezes que, quando o fazemos, estamos a usar tecnologia espacial; tal sucede porque aí utilizamos redes de comunicação e estas dependem de mecanismos de sincronismo extremamente apurados. Para tal são utilizados os relógios atómicos em satélites de navegação, cuja constelação, proveniente de diversos países, não só nos fornece a localização, mas também o tempo. Refira-se que a precisão desses relógios atómicos é de tal forma elevada, que apresenta apenas desvios de um segundo numa dezena de milhares de anos.

Voltando a nossa atenção para a questão do *New Space*, este apresenta-se como o paradigma atual, suscitando novos desafios de cibersegurança. Tal relaciona-se com a própria natureza do *New Space* que é marcada por duas vertentes: 1) a comercialização do Espaço; 2) a democratização do acesso ao Espaço, caracterizada por diminuição dos custos (tanto de lançamento como de produção dos objetos espaciais). Atualmente, uma determinada universidade que disponha dos recursos necessários, poderá desenvolver um *CubeSat* (com cerca de 1 dm^3 de volume e cerca de 1,3 kg de massa) e neste incorporar tecnologia por si desenvolvida (ou por um qualquer parceiro) a um preço relativamente convidativo, enviar esse objeto para o Espaço e, através de um link próprio ou contratado, recolher determinados dados. A China apresenta-se como um exemplo da denominada "Democratização do Espaço", com várias empresas e entidades a oferecerem diversos serviços espaciais.

De um ponto de vista da cibersegurança, os sistemas espaciais são, como qualquer sistema, vulneráveis e apetecíveis a ciberataques, especialmente para a obtenção de dados sensíveis e confidenciais, embora também existam indivíduos e organizações que o fazem por mera recriação.

No Antigo Espaço, o *Old Space*, a tecnologia espacial tinha um carácter fechado, funcionando numa lógica de "sistemas de proprietário" (ou seja, quem coloca determinado objeto em órbita conhece, perfeitamente, esse objeto). Já o *New Space,* democratizado e comercial, leva a que cada vez mais existam satélites cuja tecnologia opera numa lógica de *black box* (ou seja executa o que é pretendido, mas não se tem pleno conhecimento dos seus componentes, o que se reflete no desconhecimento das vulnerabilidades que essa mesma tecnologia poderá compreender).

Para adquirirmos um pouco de perspetiva sobre o fenómeno securitário no Espaço, ressalvo que, entre 1977 e 2019, teve-se conhecimento de 405 incidentes de ataques contra satélites, com a maioria destes, 83, a visar o *Ground Segment* (ou seja, o segmento de TT&C – *telemetry tracking and control* – de forma a inviabilizar o uso desses equipamentos, podendo essa inviabilização ser simples *blackout* do sistema ou chegar ao próprio *hijacking* do satélite). Refira-se, também que, em 91 desses 405

incidentes, o alvo foi o setor governamental e a maioria do dos ataques teve como alvo o sistema de comunicações em terra. Assim, e com a democratização do acesso ao espaço, a questão não será tanto se seremos atacados, mas antes quando seremos atacados.

Outra questão relevante, de um ponto de vista securitário, é a forma como o setor da Defesa irá lidar com a realidade do *New Space*. Recentemente uma empresa de referência do setor espacial lançou um sistema de observação e comunicações para clientes governamentais. Desta forma, o *New Space* surge como uma oportunidade aos Estados de adquirirem capacidades, ao mesmo tempo que nos leva a refletir sobre qual será o papel da defesa e segurança neste cenário em que os Estados dependem, em questões de Segurança Nacional, de fornecedores de um serviço que do qual não conseguem dispor por si próprios.

Destacaria, ainda, no âmbito das tecnologias quânticas, a importância das comunicações quânticas para a segurança. De facto, esta tecnologia leva-nos a repensar os meios de encriptação atualmente usados, pois a questão não é a possibilidade ou não de decifrar determinada palavra-passe, mas sim o tempo que tal demora. Ora, com um aumento enorme da capacidade computacional que advém da computorização quântica, a questão do tempo de processamento passa de anos para decifrar as encriptações mais complexas, para uma questão de minutos.

Gostaria de referir as capacidades de predição e classificação de ataques que os modelos de *machine learning* e de *deep learning,* poderão proporcionar, tendo por base a análise de padrões e interação de dados.

Para terminar, gostaria de fazer alusão à *digital engineering*, que permite simular circunstâncias extremas de ataque permitindo uma avaliação da capacidade de resiliência dos sistemas operados e em desenvolvimento.

Reflexões do Debate

Coronel João Barbas:

O quadro nacional é extremamente amplo. Portugal tem uma lei do cibercrime que adota a Convenção de Budapeste do Conselho da Europa e que é normalmente utilizada como elemento de referência em termos da legislação do cibercrime.

Perante atividade cibercriminosa, podemos falar de entidades não estatais ou de Estados, sendo muito difícil a identificação do cibercriminoso. Contudo, mais uma vez, esse quem é quem, encontra-se enquadrado no que é possível alcançar através da lei porque, normalmente, esses atores estão associados a Estados, encontrando-se salvaguardados por um nível de proteção.

Aliás, na maior parte dos casos que têm ocorrido, nos últimos dez ou quinze anos, muito raramente houve uma imputação clara. O que observou foi uma atribuição política a uma determinada origem de ataque, podendo haver retaliação entre as partes.

Engenheiro Duarte Cota:

Existe uma espécie de competição entre os *hackers* russos e norte-coreanos sobre quem consegue entrar nos diversos sistemas, com os russos a aparentarem tomar a dianteira nesta competição.

Existindo legislação e protocolos de segurança, a ordem natural é que estes sejam seguidos pelos Estados, sendo que as instituições privadas desejam ter segurança nos seus sistemas, investindo acentuadas quantias para tal.

Contudo, a relação entre a legislação nacional e as empresas privadas deverá ser alvo de uma avaliação. Será necessário verificar se estas cumprem com o enquadramento legal nacional ou contratual de determinado serviço tendo, também, em conta as próprias relações entre o Estado e empresas tecnológicas e inovadoras. Esta interação será fundamental, dado que uma empresa não quererá investir na produção e desenvolvimento de tecnologias que depois não serão usadas por motivos de legislação e de segurança.

Coronel António Eugénio:

Em relação ao enquadramento geral das tecnologias disruptivas, existe por parte da União Europeia uma força para trazer para o plano de negociação questões que podem ser mais difíceis de tratar. Por exemplo, a inteligência artificial tem sido uma bandeira da União Europeia, que tem chamado os Estados a assinar convenções para alguma regulamentação, de forma a tentar contornar o caracter difuso em que a presente matéria se apresenta. É algo difícil, mas terá de ser negociado.

Conclusões da Conferência

- A importância estratégica dos Açores, que se tornou menor após o fim da Guerra Fria, tem vindo a refirmar-se com a extensão da plataforma continental, a Guerra da Ucrânia e com o setor espacial.
- Portugal, contando com a contribuição da Região Autónoma dos Açores, tem no setor espacial um potenciador da sua importância geoestratégica internacional, bem como da sua economia.
- O *New Space* surge como uma grande oportunidade para os Açores e para Portugal no seu todo, apresentando, porém, uma série de desafios securitários.
- A tecnologia quântica apresenta uma revolução nas capacidades de processamento, permitindo não só uma maior capacidade de tratamento de dados, mas também exigindo novos sistemas de encriptação.
- A cibersegurança e a ciberdefesa não são mais temáticas do futuro próximo, mas sim a nossa realidade quotidiana, devendo ser encaradas da mesma forma que as suas congéneres do mundo físico.
- Os atores não estatais apresentam-se, cada vez mais, como parte incontornável nos âmbitos do espaço, ciber e das novas tecnologias disruptivas. Alguns destes surgem como parceiros fundamentais dos Estados, ao mesmo tempo que outros tomam a forma de agentes altamente perigosos para a segurança e defesa dos Estados, das empresas e dos cidadãos.

Referências

[1] Despacho n.º 68/MDN/2020 de 18 de dezembro.

[2] https://portal.azores.gov.pt/web/ema-espaco/sst

[3] Estação de rastreio de lançadores da Agência Espacial Europeia (ESA) em Santa Maria, em 1999; Estação de medição de radiação atmosférica (ENA-ARM) do Departamento de Energia dos EUA na Graciosa, em 2009; Estação da Rede Atlântica de Estações Geodinâmicas e Espaciais em Santa Maria, em 2016; Estação de sensores Galileo em Santa Maria, em 2017; Sensor ótico de Vigilância Espacial e Rastreio (SST) do programa EUSST em Santa Maria e o centro nacional de operações espaciais da rede SST na ilha Terceira, em 2020; Antena de telecomunicações de 15 metros em Santa Maria, em 2020; e Instalação da Estação da EUMETSAT em Santa Maria, em 2021.

[4] https://portal.azores.gov.pt/web/ema-espaco/legislacao

[5] https://portal.azores.gov.pt/documents/3729727/856c3c4a-7f34-5649-60b4-586db26c82cc

[6] https://www.dailymail.co.uk/news/article-11335761/Shetland-completely-cut-mainland-phones-internet-computers-hit-blackout.html. Nota: as Shetland são concorrentes dos Açores. https://www.gov.uk/government/news/shetland-enters-new-frontier-as-uk-space-industry-leader