REPÚBLICA PORTUGUESA

MINISTRO DA DEFESA NACIONAL

João Gomes Cravinho

Ministro da Defesa Nacional

Intervenção do Ministro da Defesa Nacional, João Gomes Cravinho, no âmbito do VI Seminário SIRP "Ciberdemocracia e cibersegurança"

Reitoria da Universidade Nova de Lisboa, Lisboa, 29 de janeiro de 2019

Um convite para falar sobre ciberdemocracia e sobre cibersegurança. Eis um desafio entusiasmante, mas também intimidante, porque se trata de um dos grandes temas do nosso tempo, exatamente por não haver soluções fáceis e óbvias. Vejo este momento sobretudo como uma oportunidade para partilhar inquietações, e escutar opiniões diversas que estão todas devidamente sedimentadas no objetivo de promover a nossa segurança face a desafios radicalmente diferentes daqueles que se sentiam há um par de décadas atrás.

Desde logo, portanto, quero agradecer ao SIRP, em particular à sua Secretária-geral, a Embaixadora Graça Mira Gomes, pelo convite para estar aqui hoje. Este seminário é já uma referência nacional e quero saudar o SIRP e os seus parceiros, o Instituto de Defesa Nacional e a Universidade Nova de Lisboa, pela realização hoje da sexta edição, que, tal como as anteriores, continua a colocar em debate temas de grande atualidade e relevância para responder aos desafios dos nossos tempos. A importância de abrirmos, à sociedade portuguesa, os

debates em torno das grandes questões estratégicas do nosso país é, a meu ver, um contributo fundamental para a nossa democracia.

A cibersegurança é um tema que tem vindo a ocupar a atenção da Defesa desde há algum tempo. Aliás, a edificação e a consolidação da capacidade de ciberdefesa do país estão plenamente incluídas na proposta de Lei da Programação Militar, que apresentei na semana passada na Assembleia da República, e que se encontra agora em discussão. O aumento significativo de investimento que prevemos nesta área constitui um testemunho da nossa convicção que a defesa nacional não pode deixar de contar com capacidades bastante acrescidas neste domínio, comparado com aquilo que é a situação atual.

Irei referir-me a alguns destes passos estruturantes da política nacional de ciberdefesa, mas gostaria de começar a minha intervenção pela identificação de várias linhas de tensão, que devemos procurar

resolver no âmbito do inter-relacionamento do conjunto das instituições nacionais.

Uma **primeira** clarificação que me parece necessária, prende-se com a **diferença entre cibersegurança e de ciberdefesa**. Os limites conceptuais nem sempre são claros, assim como não são, por consequência, os limites operacionais.

Num trabalho de fundo publicado pela Instituto de Defesa Nacional, em abril do ano passado, a distinção entre os dois conceitos era feita com base no grau de ameaça que era necessário prevenir ou dar reposta. Assim, a cibersegurança incluía "as atividades […] de prevenção, monitorização e resposta às ameaças que […] coloquem em risco o bem-estar e a salvaguarda dos direitos dos cidadãos ou organizações", e a ciberdefesa focar-se-ia nas "a ameaças que coloquem em risco a soberania nacional"[1].

[1] https://www.idn.gov.pt/publicacoes/cadernos/idncadernos_28.pdf

Segurança e Defesa são áreas de governação distintas, é certo, mas são áreas de grande complementaridade. A ação das Forças Armadas, cuja missão inclui a defesa da Soberania Nacional, está centrada na segurança do país e dos seus cidadãos. Elas dão um contributo fundamental para a segurança internacional de que Portugal beneficia. Contudo, não compete à Defesa a definição de uma política de segurança nacional. Compete-lhe, sim, contribuir para o desenho e implementação de uma política de ciberdefesa, que se enquadra no âmbito da nossa cibersegurança.

Mas a natureza difusa da segurança, particularmente visível desde o fim da oposição bipolar da Guerra Fria, oferece-nos alguns dilemas face a esta abordagem que é derivada de uma perspetiva tradicional. Recordo-me por exemplo do nexo segurança interna / segurança externa, como um bom exemplo destes desafios. No âmbito do ciberespaço, as fronteiras entre o domínio interno e externo, entre o

civil e militar e entre o público e o privado, esbatem-se de forma espetacular e talvez sem precedentes. E esta realidade exige clarificação urgente de funções e, essencialmente, mecanismos de coordenação sistemática de esforços.

Aqui se colocam também os primeiros desafios ao exercício da autoridade nesta matéria. É que as estruturas rígidas dos Estados e as estruturas militares altamente hierarquizadas exigem um conjunto de procedimentos – particularmente importantes em contextos democráticos, como é o nosso – que dificilmente se coadunam com o tempo de resposta a um ataque cibernético. O exercício da autoridade tem, assim, de prever a partilha e a delegação de competências, com regras claras de ação, nomeadamente em função do nível de resposta pretendido.

A **segunda** problemática que gostaria de abordar é o de **ciberespaço.**

O desafio central que temos pela frente é como lidar com toda uma área que tem uma dimensão física de infraestruturas que suportam as comunicações (onde a jurisdição e o controlo dos Estados é mais presente), e que tem também toda uma dimensão virtual ou informacional, onde o controlo por parte dos Estados é mais difícil. Há uma profunda interdependência entre as duas dimensões – uma não é possível ou não faz sentido sem a outra - mas os nossos instrumentos e as nossas capacidades de controlo e jurisdição são muito diferentes. O alcance das nossas políticas, e a operacionalidade dos nossos instrumentos, é altamente variável consoante estejamos a tratar de infraestruturas cibernéticas ou o domínio do ciberespaço.

O ciberespaço, por sua vez, acarreta dois entendimentos, porventura incompatíveis. O primeiro entende o ciberespaço como um bem comum da humanidade – um *global common* –, aplicando-se regras de uso partilhado e livre, de utilização responsável para um espaço de bem comum sobre o qual nenhuma nação pode ou deve reclamar

soberania. O segundo entendimento vê o ciberespaço como um novo domínio de atuação soberana, onde os Estados podem e devem projetar poder. Alinhamos com a primeira destas formas de entender o ciberespaço, mas temos de saber conviver, e nos defendermos, num meio em que a atuação de outros países é pautada pelo segundo entendimento.

Dito isso, o ciberespaço não pode ser um domínio em que há descontrolo total e uma ausência de regras. Ao nível da Aliança Atlântica, o ciberespaço é entendido como um novo domínio operacional onde a Aliança se considera mandatada para atuar de forma defensiva e onde o Direito Internacional se aplica. E a realidade atual, pública e bem visível, é de uma escalada de tensão em torno do ciberespaço, existindo motivos de preocupação em torno da preservação da integridade de sistemas civis e militares, que são essenciais para o regular funcionamento das nossas instituições e economias. Mas os riscos de uma militarização excessiva e de uma

competição desenfreada são igualmente reais e devem ser bem ponderados.

A **terceira** linha de problematização que me parece importante entender para a definição de respostas operacionais, prende-se com a **catalogação das ameaças no ciberespaço**. Nesta matéria, tem havido algum consenso – também refletido na nossa organização interna – de que há quatro grandes grupos de ameaças que devem ser acauteladas. O primeiro diz respeito ao **cibercrime**, o segundo ao **ciberterrorismo**, o terceiro à **ciberespionagem** e o quarto à **ciberguerra**. Qualquer uma destas ameaças visa interferir com a ordem interna e externa de um país e, nesse sentido, deve ser objeto das políticas de segurança e defesa. Mas quais as barreiras entre cibercrime e ciberterrorismo? O ciberterrorismo utiliza frequentemente o cibercrime como ferramenta de trabalho, mas naturalmente que nem todo o cibercrime está relacionado com ciberterrorismo. É igualmente difusa e contingente a relação entre cibercrime e ciberespionagem. E a partir de que ponto

se deve considerar que um país enfrenta uma ciberguerra, um termo que sugere um grau muito elevado de conflitualidade, mas que pode na realidade ser algo que passa despercebido ao cidadão comum?

Estas são questões de grande pertinência operacional e cujas respostas se tornarão possivelmente mais claras à medida que Portugal vai ganhando experiência em lidar com estes diferentes tipos de ameaças. Mas creio que não devemos esperar pela iluminação que resulta do empenho operacional, até porque o próprio empenho operacional pode ser prejudicado pela falta de clareza à partida. A meu ver, precisamos de mais discussão teórica, como esta que aqui considero tão útil, acompanhado de debate e convergência interinstitucional, e também de exercícios práticos de simulação, para acelerarmos a criação de defesas e respostas sólidas e automatizadas.

Com todas as reservas já expressas quanto à necessidade de evitarmos uma analogia excessivamente e enganadoramente simplista entre o mundo cíber e o mundo tradicional de segurança e defesa, queria dedicar agora uns minutos à nossa política nacional de ciberdefesa.

[A Política Nacional de Ciberdefesa]

A Defesa tem investido intensamente nos esforços de criação de capacidade nacional de ciberdefesa e, concomitantemente, de cibersegurança. Esta linha de trabalho tem sido muito estimulada pela participação de Portugal em organizações internacionais, incluindo a União Europeia e a NATO, permitindo que a política nacional de ciberdefesa ganhe contornos cada vez mais claros.

O primeiro elemento a destacar é o Conceito Estratégico de Defesa Nacional[2], de 2013, que identifica um conjunto de ameaças ao

[2] https://www.defesa.pt/documents/20130405_cm_cedn.pdf

ciberespaço, a ter em conta. Aí se sublinha o papel da Defesa para a manutenção das infraestruturas que suportam as sociedades e as economias globalizadas e interdependentes do século XXI. Noutros documentos de natureza doutrinária são também identificadas medidas concretas com vista à edificação de uma capacidade de ciberdefesa nacional, incluindo a criação de um Centro de Ciberdefesa, no âmbito do EMGFA. A Orientação Política para a Ciberdefesa[3], que data também de 2013, definiu as orientações específicas nesta matéria, colocando-as no cerne das reformas em curso na Defesa Nacional. Foram passos importantes, e hoje as Forças Armadas estão mais equipadas e mais organizadas no domínio da ciberdefesa, mas estamos nos primórdios, e temos sem dúvida necessidade de mais avanços doutrinários e operacionais.

[3] http://www.operacional.pt/docs/Ciberdefesa.pdf

Na Estratégia Nacional de Segurança do Ciberespaço[4] de 2015, sublinha-se a necessidade de cooperação, de partilha de informação, de gestão integrada de respostas a ameaças e riscos, de coordenação operacional e de autoridade nacional. O Centro Nacional de Cibersegurança, atua como a autoridade nacional nesta matéria e assegura a coordenação das diferentes entidades competentes, incluindo o Centro de Ciberdefesa, entretanto criado no EMGFA.

À Defesa cabe especificamente um conjunto de preocupações com a proteção dos sistemas operacionais essenciais à atuação das Forças Armadas e, por essa via, essenciais ao exercício da nossa soberania. A salvaguarda da capacidade operacional das nossas Forças Nacionais Destacadas ou de quaisquer missões em que os nossos militares venham a estar envolvidos é uma preocupação central. Por outro lado, a nossa capacidade de controlo e vigilância das nossas áreas de soberania e de responsabilidade – estou a pensar na nossa vasta e

[4] https://dre.pt/application/conteudo/67468089

provavelmente alargada plataforma continental – é essencial para a segurança do ciberespaço, já que estão aí localizadas infraestruturas físicas importantes.

Por isso, temos apostado na valorização da nossa participação na Aliança Atlântica e na UE, como dois quadros institucionais multilaterais onde se têm definido princípios e boas práticas centrais à ciberdefesa. Aliás, a mesma Estratégia Nacional de Segurança do Ciberespaço sublinha também a importância da experiência recolhida pela participação das Forças Armadas em Missões no exterior para o desenvolvimento de soluções tecnológicas com interesse para duplo uso civil e militar, em colaboração com universidades, centros de investigação e a indústria.

Vivemos numa era em que a nossa segurança depende mais do que nunca da nossa capacidade de trabalhar em rede com outros parceiros, derivando daí a relevância insubstituível das alianças e parcerias com outros países que nos são próximos. Mas, não obstante,

interessa-nos promover a capacidade da indústria nacional para que possamos obter um grau de soberania cibernética, sem perdermos de vista que se falamos de empresas falamos não de capacidades do Estado, mas antes de entidades que de um momento para outro podem ter novos proprietários.

A implantação da *NATO Communications and Information Academy* (NCIA) em Portugal e que será inaugurada ainda este ano, é uma oportunidade para desenvolvermos melhor as nossas capacidades neste domínio, e temos de saber aproveitar sobretudo as potenciais sinergias com as nossas universidades e as nossas empresas, criando núcleos tecnológicos e humanos capazes de liderar nas respostas às ameaças potenciais no ciberespaço e cujos efeitos se fazem sentir, seja no âmbito civil, seja no âmbito militar.

Na Cimeira de Gales e em momentos subsequentes, a Aliança Atlântica tem dado sinais claros no sentido de incentivar os seus Estados membros a desenvolver capacidades de ciberdefesa, criando recursos na área da formação, educação e treino operacional, de que Portugal tem, aliás, beneficiado. A proteção dos sistemas de comunicação da NATO e dos seus parceiros é um objetivo central desta abordagem. De forma semelhante, também no âmbito da União Europeia estamos a desenvolver passos na área da cibersegurança e ciberdefesa – naturalmente articulados com a NATO, sempre que relevante. A estratégia da UE para a cibersegurança inclui também uma dimensão de ciberdefesa e de desenvolvimento de capacidades para a Política Comum de Segurança e Defesa, a par das preocupações com os princípios de abertura da economia europeia. Sendo que as mulheres e os homens das nossas Forças Armadas participam em missões das duas organizações, a sua segurança tem de ser uma prioridade, e nós contribuímos também para essas dimensões da segurança coletiva.

Sublinharia ainda, como parte integrante da nossa política de Defesa Nacional, a integração de questões de ciberdefesa na cooperação bilateral e multilateral, incluindo no âmbito da CPLP. Na Estratégia Digital, de 2018, assumíamos com todos os nossos parceiros da CPLP, a cibersegurança e ciberdefesa como uma prioridade.[5] Continuamos a trabalhar para expandir boas práticas nesta matéria para outros contextos geográficos e para a articulação de uma visão comum.

Diria, pois, que Portugal está a dar passos sólidos de criação de meios para a sua ciberdefesa e que esta é uma parte integrante da cibersegurança nacional.

5 https://www.cplp.org/Admin/Public/Download.aspx?file=Files%2FFiler%2F1_CPLP%2FComunicacoes%2FAgendaDigitalCPLP-2018.pdf.

Minhas senhoras e meus senhores,

Apesar destes esforços significativos, há um imenso espaço de incerteza, que tem de ser reconhecido. Lidamos com avanços tecnológicos exponenciais, e inovações tecnológicas que estão na sua infância. As vulnerabilidades a que procuramos dar resposta são por isso também exponenciais e de difícil previsão. Precisamos de presumir a inevitabilidade das falhas, ao mesmo tempo que reforçamos a resiliência dos sistemas.

Procuramos soluções para problemas que muitas vezes ainda não existem, ou existem apenas hipoteticamente. Decidimos com base em modelos abstratos e cenários imaginados, que nos servem de guia, mas que devem deixar espaço à adequação necessária se e quando nos confrontarmos com experiências reais.

Estamos a trabalhar todos os dias para ganhar capacidade e para estarmos no centro das boas práticas internacionais nesta matéria. É preciso também gradualmente ir construindo um espaço de diálogo cooperativo, ao nível internacional, onde medidas de criação de confiança possam ser implementadas. Isso é crucial para evitar uma escalada de ameaças que deixe, à semelhança do foi a realidade nuclear da Guerra Fria, o planeta paralisado. Não conhecemos as consequências de uma guerra cibernética e, no que me diz respeito, gostaria de continuar a não conhecer. Trabalhemos, pois, para a tornar impraticável, através da cooperação e através da dissuasão – dois instrumentos tradicionais que nos servem de guia nas nossas aventuras do século XXI.

Muito obrigado!