INTERVENÇÃO DGSIS NA 6ª CONFERÊNCIA TERRORISMO CONTEMPORÂNEO- "CIBERTERRORISMO- DESAFIOS, AMEAÇAS E CONSEQUÊNCIAS GEOPOLITICAS"

28ABRIL 2022

Permitam-me, que inicie a minha intervenção com a atual conjuntura geopolítica internacional.

Há relativamente pouco tempo, fiz uma intervenção pública em que disse: "No atual ambiente estratégico, o factor incerteza tende a agravar-se em face da debilitação dos vínculos transatlânticos, das divergências entre os parceiros europeus, da aproximação oportunista entre a China e a Rússia, do ressurgimento dos nacionalismos, do protecionismo económico e das ameaças aos sistemas democráticos".

Hoje já não poderia fazer exatamente a mesma afirmação, embora parte dela ainda seja atual. Com efeito, a guerra na Ucrânia alterou quase tudo. Os vínculos transatlânticos reforçaram-se. A NATO demonstrou quer a sua vitalidade quer que, afinal, não estava em estado comatoso. A invasão catalisou nações e governos a unirem-se para romper os laços

financeiros e comerciais com a Rússia e a imporem sanções quase por unanimidade. As relações entre a Rússia e a China parecem cada vez mais consistentes e desafiadoras da ordem internacional que perdurou nos últimos 75 anos.

O Ocidente, que apresentava fortes sinais de debilidade perante outros atores, parece querer sobrepor a força moral dos regimes democráticos nas relações internacionais.

A União Europeia deu mostras de coordenação e de liderança, abriu as portas aos refugiados e aprovou um novo documento estratégico na área da segurança e defesa, a denominada Bússola Estratégica. Em simultâneo, presenciamos mudanças estratégicas brutais na área da política externa e de defesa, como foi o caso da Alemanha. Estamos a assistir ao surgimento de um novo sistema de alianças.

Os fundamentos que garantiram a paz na Europa estão novamente ameaçados. As consequências desta guerra na Ucrânia não se limitam à Europa Oriental e sobrepõem-se aos efeitos da crise pandémica que já teve efeitos profundos, nem todos ainda visíveis, na política, na economia e na sociedade. O impacto destes acontecimentos recentes

repercutir-se-ão nas próximas décadas de maneiras que ainda não podemos prever.

Nos últimos 30 anos, vivemos num contexto global de relativa paz e assistimos à expansão da globalização. A paz e a prosperidade foram fenómenos indissociáveis. Estas foram alavancas poderosas que aceleraram o comércio internacional, aumentaram o crescimento económico, interconectaram as economias e ajudaram a reduzir drasticamente a pobreza das nações em redor do mundo.

Porém, a invasão russa da Ucrânia veio desferir um rude golpe no processo de globalização e disparar o risco da confrontação militar. Estamos a assistir a uma mudança drástica na ordem mundial que poderá antecipar a fragmentação do mundo em blocos geopolíticos e agravar a rivalidade entre as potências liderantes desses blocos. Neste contexto, os reajustamentos no processo de globalização far-se-ão em zonas de influência político-militar ou de tutela geoeconómica, como afirmou há dias o novo economista chefe do FMI.

As tendências que se vislumbram em consequência desta guerra acarretam um nível de incerteza sem precedentes na vida das

populações, em particular das mais vulneráveis, e uma perspetiva de dificuldade na resposta à crise económica.

Poderemos estar perante a "tempestade perfeita" que agravará as ameaças contra o modelo político e socioeconómico das nossas democracias e há fatores que se constituem fertilizantes para os fenómenos resultantes da polarização, do extremismo político e da violência do terrorismo.

Enfrentaremos uma nova vaga de terrorismo de matriz política e com patrocínio estatal? Iremos ter novamente que prevenir atos de sabotagem e de subversão política e social com génese no confronto de blocos geopolíticos?

Como disse o Prémio Nobel da Física de 1922, o dinamarquês Niels Bohr, "fazer predições é muito difícil, especialmente, se forem sobre o futuro"

Os decisores europeus não acreditaram que uma potência nuclear como a Rússia, iniciasse uma guerra nas fronteiras da Europa; a interconetividade económica e a dependência energética não chegaram

para conter os ímpetos expansionistas da Rússia; o que poderá acontecer no domínio da corrida ao armamento de destruição em massa?

A este conjunto complexo de tendências e cenários, acrescem as ameaças resultantes do confronto geopolítico e económico que exigirão mais investimento nos sectores da defesa e da segurança, quando se tornam vitais os esforços financeiros para conter as alterações climáticas e avançar com a transição energética.

Os dilemas são numerosos e o risco de não ser possível resolvê-los atempadamente estão associados à volatilidade e à imprevisibilidade do futuro próximo. Porém, se o cenário de fragmentação geopolítica se corporizar, dificilmente se recuperará a prosperidade e a paz em que vivemos nos últimos 30 anos.

*****

Nós, nas informações, lidamos com o Mundo tal como ele é e não como gostaríamos que fosse. Corremos contra o tempo, pressionados pela necessidade de lidar, em simultâneo, com as velhas ameaças e com os

efeitos de um conjunto de fenómenos que as transmutam, num ambiente estratégico instável e imprevisível.

Neste quadro complexo, os serviços de informações enfrentam desafios e têm que tomar decisões. Procuram combinar a experiência da produção de intelligence com a exploração de novas tecnologias para enfrentar os adversários; sentem necessidade de aproximar as relações na comunidade das informações entre as informações civis e as militares, as de segurança e as estratégicas e os diversos departamentos do Estado; criam metodologias de trabalho inovadoras, novos centros especializados de acompanhamento das ameaças envolvendo as várias valências internas, de análise e técnicas e trabalham em conjunto com os parceiros internacionais numa unidade de ação, como em tempo algum se verificou; e estabelecem novas parcerias com as empresas privadas e a Academia;

com um só objetivo final: o de detetar, identificar e disromper atividades que ameaçam os pilares das nossas sociedades livres e democráticas, proteger e garantir a segurança dos nossos cidadãos e da nossa economia e bem-estar, através de informações independentes.

As ameaças com que lidamos diariamente, a par das crescentes capacidades tecnológicas dos adversários, sejam eles de natureza estatal ou não estatal, exigem serviços de informações modernizados, com condições de atrair e fixar recursos humanos de qualidade e dotados de legislação adaptada à evolução tecnológica do mundo virtual e às ameaças atuais. Importa aprender com a história recente e não adiar o que tem de ser feito para lidar com a reconfiguração das ameaças que os serviços, em democracia, acompanham.

****

O tema da Conferência é o ciberterrorismo; um conceito complexo cuja definição ainda não reúne consenso. Existem genericamente duas perspetivas sobre o conceito de ciberterrorismo que norteiam o debate: por um lado, quando a tecnologia é o *alvo*, isto é, o ciberterrorismo como a destruição de sistemas e redes informáticas através de acções ideologicamente motivadas com o propósito de alcançar um impacto relevante nos cidadãos e instituições; e, por outro lado, quando a tecnologia é a *ferramenta* usada para conduzir acções violentas no ciberespaço com o objectivo último de gerar violência e destruição e alterar a ordem política e o modelo social. Isto é, acções disruptivas da

infra-estrutura tecnológica de suporte ao ciberespaço ou acções disruptivas do ciberespaço em si mesmo.

Mas, na verdade, a perspectiva dos serviços de informações, isto é, o olhar da *intelligence* ou o nosso conceito operativo para a ciberameaça no domínio do terrorismo , e que quero partilhar convosco, é diferente. Mais do que um alvo ou uma ferramenta, o ciberespaço é indissociável do mundo real e constitui-se um meio facilitador da ação terrorista.

Mais do que dominar as definições dos diversos tipos de terrorismo, o importante é garantir que os modelos de análise e as grelhas interpretativas são válidos. Os conceitos que usamos são o mapa, mas o mapa não é o território e esta ideia tem que estar sempre presente no nosso trabalho.

Há dois conceitos essenciais no modelo do pensamento crítico que constituem uma espécie de vacina contra o erro ou a compreensão errada de uma situação. Isto tanto se aplica ao terrorismo como à guerra. Um é o conceito de **desvinculação moral** ou seja a desumanização do outro em razão da raça, cultura, economia, religião ou política. Este processo cognitivo de desvinculação moral alimenta as

narrativas de ódio ao outro, ao que é diferente. Isto é viral quando feito online, seja no terrorismo seja no actual conflito.

O outro é a **comparação vantajosa**, que é um processo cognitivo aplicado para fazer parecer um ato negativo aceitável quando é uma resposta a atos cometidos por outros. Perante uma percepção de injustiça, matar outros pode parecer aceitável. Estes são conceitos em que assentamos como vacina contra a desinformação, a manipulação, contra a radicalização e o recrutamento para os extremismos.

***

As duas dimensões da ameaça terrorista – radicalização e recrutamento/propaganda e inspiração – são especialmente relevantes ao nível da fusão do ciberespaço com o mundo real e da consolidação e expansão da ameaça. Naquilo que é a competência exclusiva do SIS em matéria de contraterrorismo e no quadro da orientação estratégica das autoridades nacionais e internacionais, a missão não é diferente no ciberespaço do que é no mundo real. Todavia, é muito mais complexa e enforma-se de dificuldades acrescidas.

A detecção precoce de potenciais ameaças por parte dos serviços de informações – o primeiro pilar da estratégia de combate ao terrorismo – será tanto mais eficaz quanto mais expressivos forem os meios e capacidades disponíveis. Do ponto de vista constitucional e legal, de alguma forma, fez-se um esforço de transição de um mundo analógico de ameaças para o mundo digital, mas falta ainda percorrer com sucesso o caminho para o mundo virtual, nomeadamente ao nível do acesso à encriptação de dados das comunicações.

No caso português, falta quase tudo o que diz respeito às comunicações. Continuamos como o único país da Europa sem autorização legal para aceder aos dados de comunicações por parte dos serviços de informações.

Ao nível da prevenção – em particular da radicalização – muito tem sido feito ao nível nacional e internacional, na identificação e partilha de páginas, perfis e *sites* promotores das narrativas do terrorismo. De forma regular e sistemática, estas são eliminadas ou o acesso é bloqueado, através dos mecanismos de cooperação estabelecidos entre as entidades nacionais e internacionais de combate ao terrorismo e os *providers* daqueles serviços. Mas estes processos podem ser mais

rápidos e mais ágeis, reduzindo o tempo de exposição *online* de conteúdos extremistas.

Ao nível da proteção e segurança das infra-estruturas críticas e pontos sensíveis, eventualmente onde o termo ciberterrorismo se pode manifestar e gerar impactos relevantes e significativos, os serviços de informações e as demais entidades nacionais com competência nesta matéria dispõem de mais um aliado: os responsáveis pela cibersegurança destas entidades que são a primeira linha de protecção dos sistemas e redes informáticas e de resposta em caso de incidente. A cooperação e partilha de informação relativamente a incidentes registados, tentativas de intrusão, disseminação de código malicioso será sempre um contributo relevante para elaborar a avaliação de ameaça que impende sobre estas infraestruturas.

Relativamente à perseguição das actividades terroristas – o quarto pilar da estratégia – importa igualmente destacar os sucessos obtidos ao nível da cooperação internacional entre serviços de informações, possibilitando a identificação e caracterização de redes de contactos *online* que se estendem por múltiplos países, incluindo Portugal. Mas, citando Platão, também há coisas que *sabemos que não sabemos* e outras que *não sabemos que não sabemos* – como referi, o ciberespaço não está

confinado geograficamente e oferece oportunidades infinitas de ocultação.

Por fim, o último pilar da estratégia nacional de combate ao terrorismo define a resposta em caso de atentado. Felizmente, e nas últimas décadas, Portugal não foi palco da estratégia violenta de organizações terroristas ou extremistas. Os serviços de informações e as demais forças e serviços de segurança estão a cumprir a sua missão. Mas serei absolutamente claro: o momento actual encerra demasiadas incertezas securitárias que irão inevitavelmente alterar o quadro actual.

***

A abordagem da *intelligence* é sempre uma abordagem dinâmica, que se detém sobre os sinais de mudança que se vão desenhando diariamente e denunciando alterações aos contornos das ameaças acompanhadas. Todo o trabalho dos serviços assenta em obter informação verdadeira e não cair nos enganos gerados pela manipulação de outros. Num mundo fortemente tecnológico todas as ameaças foram amplificadas o que exige constante ADAPTABILIDADE.

Pela frente temos muitos futuros e nunca desistiremos! Os serviços de informações estão focados em monitorizar os impactos diretos e indiretos das crises sucessivas e a trabalhar para apoiar o decisor

político a entender como navegar nesse novo ambiente geopolítico e geoeconómico e ajudá-lo a decidir. Navegamos juntos a incerteza, ainda sem terra firme à vista. E ao mesmo tempo que esperamos pelo fim deste conflito, vamos desenhando os cenários que irão configurar as ameaças futuras à segurança global – e à segurança do nosso país. Compete à intelligence PREVENIR ameaças e para isso temos de estar atentos aos momentos de viragem (turning points), designadamente no terrorismo para minimizar surpresas e incertezas que ponham em causa a nossa segurança.

Desejo um bom trabalho a todos os participantes nesta 6ª Conferência Internacional sobre Terrorismo Contemporâneo.

Muito obrigada.