REPÚBLICA PORTUGUESA

GABINETE DO MINISTRO DA ADMINISTRAÇÃO INTERNA

Exmo. Senhor
Chefe do Gabinete
de S. Exa. a Ministra Adjunta e dos Assuntos Parlamentares
Palácio de São Bento
1249-068 Lisboa

SUA REFERÊNCIA	SUA COMUNICAÇÃO DE	NOSSA REFERÊNCIA	DATA
1584	29-11-2022	Nº: 326/2023 ENT.: 194/2023 PROC. Nº: 868.01	05-01-2023

ASSUNTO: Pergunta n.º 911/XV/1.ª de 29 de novembro de 2022

Em resposta à pergunta n.º 911/XV/1ª cumpre informar:

O espaço geostratégico próximo da UE caracteriza-se no presente por uma forte instabilidade geopolítica e geoeconómica determinada pela invasão da Ucrânia, que agravou sobremaneira as consequências já sentidas pela pandemia de Covid-19. A profundidade geostratégica da guerra é geradora de fenómenos estratégicos conexos com grande impacto no sistema de segurança europeia, nas suas dimensões interna e externa, designadamente os respeitantes a instrumentos de guerra híbrida e aos ciberataques.

As ameaças e riscos contra interesses críticos da UE tendem a registar um aumento de complexidade e interdependência que requerem uma compreensão, avaliação e análise integrada, coordenada e executada pelos Estados-membros, como um todo.

Neste contexto, as ameaças com que nos deparamos comportam efeitos na segurança humana em consequência de migrações forçadas e dos movimentos de refugiados, no contexto da atual guerra da Ucrânia, mas também das tensões e crises de guerra e humanitárias num largo arco que interfere no ambiente estratégico da UE,

que inclui África, o Médio Oriente e a Ásia Central. Refira-se, ainda a este propósito, que durante a pandemia de Covid-19, as restrições à circulação impactou nos fluxos migratórios, que, no atual contexto, estão a ser retomados e reavivados sobretudo devido à degradação das condições económicas, políticas e sociais nos Estados de origem, que são o resultado, nomeadamente, de três fatores: a pandemia Covid-19, a guerra de agressão à Ucrânia e as alterações climáticas.

Paralelamente, estamos confrontados com ameaças e desafios emergentes transnacionais. Estes, pela que pela sua natureza, amplitude e profundidade impõem uma resposta política e operacional da UE, através das suas instituições e estruturas nas áreas da Defesa, Justiça, Assuntos Internos e Proteção Civil.

Como enuncia a Bússola Estratégica da UE, o terrorismo e o extremismo violento em todas as suas formas e independentemente da sua origem continuam a evoluir de modo persistente e constituem uma grave ameaça para a paz e a segurança, dentro e fora da UE. Incluem uma combinação de terroristas endógenos, combatentes estrangeiros regressados, atentados dirigidos, encorajados ou inspirados no estrangeiro, bem como a propagação de ideologias e crenças que conduzem à radicalização e ao extremismo violento.

A proliferação de armas de destruição maciça e dos seus vetores constitui uma ameaça persistente, tal como ilustram nomeadamente os programas nucleares da RPDC e do Irão, a utilização repetida de armas químicas e o desenvolvimento e recurso a novos mísseis balísticos, de cruzeiro e hipersónicos avançados. Tanto a Rússia, como a China, estão a expandir o seu arsenal nuclear e a desenvolver novos sistemas de armamento.

Há intervenientes estatais e não estatais que estão a recorrer a estratégias híbridas, a ciberataques, a campanhas de desinformação, à interferência direta nas nossas eleições e nos nossos processos políticos, à coerção económica e à instrumentalização dos fluxos de migração irregular.

A crescente utilização abusiva da lei para alcançar objetivos políticos, económicos e militares é também uma preocupação cada vez maior. Os nossos adversários não hesitam em utilizar tecnologias emergentes e disruptivas para obterem vantagens estratégicas e aumentar a eficácia das suas campanhas híbridas.

As alterações climáticas, a degradação ambiental e as catástrofes naturais terão também repercussões sobre o nosso panorama de segurança ao longo das próximas décadas e são fatores comprovados de instabilidade e conflito em todo mundo.
As crises sanitárias mundiais podem também exercer pressões consideráveis sobre as sociedades e as economias, com implicações geopolíticas de grande alcance. A pandemia de COVID-19 veio alimentar rivalidades internacionais e mostrar que as perturbações das principais rotas comerciais podem colocar as cadeias de abastecimento críticas sob pressão e afetar a segurança económica.

Este quadro de análise sobre as ameaças e riscos que pendem sobre os interesses estratégicos e de segurança da UE está bem presente no Quarto Relatório de Implementação da Estratégia de Segurança da UE, que elenca algumas das medidas organizacionais e operacionais que os Estados-Membro da UE estão a adotar de forma combinada e gradual

Tem-se intensificado a coordenação e o intercâmbio de informações com redes de cibersegurança, como a Cyber Crises Liaison Organisation Network (CyCLONe), que inclui as agências nacionais de cibersegurança, a Comissão e a ENISA. Para refletir esta abordagem internamente nas instituições da UE, existe um mecanismo de coordenação, o Grupo de Trabalho para a Crise Cibernética, que permite que a informação seja partilhada entre todos os serviços relevantes e organismos e agências, incluindo a ENISA, o Centro Europeu de Cibercrime da EUROPOL e o CERT EU. São necessários esforços constantes para garantir canais de comunicação entre os níveis político, operacional e técnico, bem como para reforçar a cooperação com a Segurança Informática Rede de Equipas de Resposta a Incidentes (CSIRT).

Em 22 de março de 2022, a Comissão propôs novas regras para estabelecer medidas comuns de cibersegurança e segurança da informação em todas as instituições, organismos e agências da UE (EUIBA). Estas regras reforçarão a resiliência e a capacidade da administração da UE para responder a ameaças e incidentes cibernéticos. Ao colocar estas atividades num quadro comum, a cooperação interinstitucional será reforçada e a exposição aos riscos será minimizada. A proposta de regulamento de cibersegurança para o EUIBAs reforçará o mandato do CERT-UE e conduzirá à criação de um novo Conselho Interinstitucional de Cibersegurança, impulsionando as capacidades de cibersegurança.

Movimento forçado das populações e efeitos no espaço da UE. A guerra de agressão da Rússia contra a Ucrânia forçou milhões de pessoas a abandonarem as suas casas, aumentando consideravelmente os movimentos através das fronteiras externas da UE. A UE tem procurado prestar o acolhimento mais rápido e flexível aos que fogem da guerra, sem comprometer a segurança da UE.

A UE tomou medidas sem precedentes para oferecer aos que fogem da guerra proteção temporária e está empenhada em lidar com todos os recém-chegados sem discriminação. Ao mesmo tempo, os riscos potenciais que podem surgir de tantas pessoas em movimento não podem ser negligenciados, e a UE, com forte apoio das agências competentes da UE continua vigilante quanto aos novos desenvolvimentos na criminalidade organizada e no terrorismo.
Vigilância e coordenação. Uma cooperação mais forte em matéria de aplicação da lei entre os Estados-Membros e com países terceiros é fundamental para garantir a sensibilização para as ameaças criminosas e terroristas emergentes e para a ação em matéria de redes criminosas e indivíduos que podem tentar aproveitar-se da guerra contra a Ucrânia. Os Estados-Membros e os parceiros operacionais estão a partilhar ativamente informações relevantes disponíveis e informações criminais com a Europol, que cruzam e analisam as informações e a transformam em notificações de inteligência operacional, tais como notificações de alerta precoce e avaliações de ameaças, que são partilhadas com parceiros.

A UE tem sido rápida e enérgica ao assegurar uma resposta coordenada a esta ameaça real às pessoas que precisam da ajuda da UE. As orientações operacionais, incluindo sobre o desafio do tráfico de seres humanos, foram rapidamente estabelecidas pelos Estados-Membros que implementam a Diretiva relativa à proteção temporária para apoiar aqueles que fogem da guerra na Ucrânia. Um Plano Comum para a prevenção do tráfico de seres humanos e ajudar as vítimas, foi desenvolvido pelo Coordenador Anti-Tráfico da UE, em cooperação com Agências da UE.

Também o Conselho JAI de 13 e 14 de outubro de 2022 definiu um conjunto de prioridades para 2022-2025, no plano da definição de ameaças e riscos à UE e seu combate, a saber:

- Redes criminosas de alto risco;
- Ciberataques e cibercriminalidade;
- Tráfico de seres humanos;
- Exploração sexual de crianças;
- Introdução clandestina de migrantes;
- Tráfico de droga;
- Fraude, criminalidade económica e financeira;
- Crime organizado contra a propriedade;
- Criminalidade ambiental.

A operacionalização destas prioridades de segurança coletiva da UE é realizada segundo a perspetiva da segurança integrada da UE. i.e. os Estados-Membro coordenam a sua cooperação intra-EU seguindo os mecanismos e processos já em funcionamento, com recurso transversal , designadamente às estruturas da Europol, Frontex e INTCEN.

As ameaças já identificadas no seio da UE, o seu combate e minimização, requerem ,convirá sublinhar novamente ,uma abordagem comum, pois a sua complexidade e alcance não são compagináveis com respostas exclusivas de cada Estado, salvaguardadas que estejam a existência de especificidades próprias. A coordenação política, a cooperação técnico-operacional entre agências, FSS e serviços de informações, e também o reforço das parcerias extra- UE, em especial na cooperação nas áreas do contraterrorismo e da gestão das fronteiras externas da UE, são a resposta aos problemas de segurança global e regional que se colocam no contexto da UE.

A ameaças sistémicas, deverá corresponder uma resposta sistémica por parte da UE, com recurso aos instrumentos disponíveis, sem embargo do seu necessário aperfeiçoamento legislativo e operativo.

Em síntese:

A nova realidade com que nos confrontamos lança enormes desafios à segurança dos Estados e das sociedades, numa amplitude e profundidade sem paralelo potenciando vulnerabilidades como causa-efeito daqueles ajustamentos, que têm expressão:

- No terrorismo transnacional, que assumindo diferentes modus operandi continua a demonstrar capacidades para atuar na Europa;
- No extremismo violento e na radicalização ideológica, que registam um recrudescimento;
- No alto crime organizado, cuja natureza transnacional também tem vindo a acentuar-se;
- Nas redes de migração irregular, que têm vindo a diversificar origens e destinos;
- Na proliferação de armamento e no enfraquecimento gradual da arquitetura de controlo de armas;
- Nas ciber-ameaças (em especial o cibercrime e o ciberterrorismo), que registam um crescimento exponencial, com capacidade para vulnerabilizar o funcionamento de infraestruturas críticas;
- Na desinformação e em operações "híbridas," envolvendo movimentos e grupos inorgânicos com grande capacidade de mobilização, cujo potencial efeito de rutura é suscetível de, em certas circunstâncias, gerar entropias no Estado e na sociedade;
- Na criminalidade económico-financeira transnacional;
- No efeito indutor de conflitos de baixa, média e elevada intensidade no arco geopolítico próximo da UE, para além da guerra da Ucrânia, gerando a pobreza e a deslocação em massa das populações.

O atual ambiente geostratégico (Estados frágeis, potências revisionistas, ameaças assimétricas- terrorismo, ciber-ameaças, guerra híbrida) , gera aquilo que designamos por "gestão contínua de crises", levando a um desgaste dos pilares de segurança dos Estados e das sociedades.

O ambiente de "gestão de crises" demonstra o crescente desafio que é colocado à tomada de decisão política, especialmente na confluência entre segurança interna e segurança externa, considerando os efeitos de "surpresa estratégica" com que os governos cada vez mais se confrontam.

No caso de Portugal importa salientar a coordenação que existe no âmbito das atividades e do SSI, do SIRP e no âmbito das atribuições das FSS em matéria de segurança pública e de avaliação das ameaças à segurança interna, que decorrem das suas atribuições orgânicas próprias.

Como já foi identificado pela própria UE, a Rússia desenvolve ações contrárias aos interesses estratégicos e de segurança da UE, com diferentes graus de ameaças.
Está identificado o seu modus operandi em matéria de operações híbridas e de ciberataques contra alvos económicos e políticos no espaço da UE. A coordenação no seio da UE tem possibilitado mitigar e neutralizar as ações conduzidas direta e indiretamente por agentes afetos ao governo russo.

No atinente a ameaças a infraestruturas críticas, Portugal possui uma arquitetura de caraterização, avaliação e resiliência enquadrada na posição da UE nessa matéria.
A atual legislação, em especial o Dec. Lei 43/2020, de 21 de Julho (cria o Sistema Nacional de Planeamento Civil de Emergência e dentro deste cria o Conselho Nacional de Planeamento Civil de Emergência), e o Dec. Lei 20/2022, de 28 de Janeiro, (aprova os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias) possibilita a criação de condições políticas, institucionais, organizacionais e operacionais que permitem uma avaliação e resposta a potenciais ameaças e riscos em conexão com o disposto na Lei de Segurança Interna, na Estratégia Nacional de Combate ao Terrorismo, na Estratégia Nacional de Segurança no Ciberespaço, no Regime Jurídico da Segurança do Ciberespaço, e no Conceito Estratégico de Defesa Nacional

No plano organizacional e operacional o Conselho Nacional do Planeamento Civil de Emergência, tem um procedimento organizado em quatro fases distintas. Quando uma infraestrutura é considerada critica, o operador tem o dever de ter um plano de segurança da mesma, bem como uma avaliação de risco e de ter contra-medidas para superar o ataque. O plano de segurança de tal infraestrutura é submetido a um parecer prévio do Conselho Nacional do Planeamento Civil de Emergência, sendo a aprovação final da responsabilidade do secretário-geral do sistema de segurança interno.

As infraestruturas críticas são registadas numa plataforma de registo de informação de IEC, como está previsto no artigo 22º do Decreto-Lei n.º 20/22. Essa plataforma, que é criada pelo SG do SSI, permite de forma expedita o acesso a um conjunto de elementos informacionais, em caso de necessidade.

A natureza das informações respeitantes à identificação das infraestruturas críticas impõe uma natural confidencialidade e sua partilha restrita.

Com os melhores cumprimentos,

O Chefe do Gabinete

Vítor Teixeira de Sousa

/mr