China, 5G e Segurança da Aliança após as Cimeiras da OTAN de 2021/22

Este resumo apresenta os pontos-chave retirados de uma mesa redonda organizada pelo GMF e realizada sob o domínio da Chatham House, que reuniu peritos da Europa e dos Estados Unidos para explorar a amplitude das questões em torno da China, 5G, resiliência e infra-estruturas críticas que estavam a ser abordadas no contexto da OTAN. A mesa redonda foi realizada em 2021, mas as conclusões e análises foram actualizadas na sequência da invasão da Ucrânia e da Cimeira de Madrid da OTAN de 2022.

- A invasão da Ucrânia por parte da Rússia sublinha o papel fundamental da NATO na garantia da segurança dos aliados europeus, ao passo que o anúncio de uma parceria "sem limites" da China com a Rússia veio demonstrar o espectro mais alargado de ameaças a que a NATO tem de estar atenta. Além disso, reforça a obrigação imperiosa de a NATO estar bem adaptada a todas as dimensões do novo ambiente de segurança com que se defronta.
- Nas principais cimeiras realizadas em torno da visita do presidente Biden à Europa durante o verão de 2021, ficou claro que a China irá ocupar um papel central na relação transatlântica nos próximos anos. A China está agora presente na agenda da NATO de várias formas, constituindo agora como nunca uma parte muito mais relevante do debate. Embora a NATO não esteja num conflito militar com a China, este país continua a ser um grande concorrente geopolítico do Ocidente visto em conjunto. Além disso, os Estados Unidos encaram a China como uma ameaça direta à segurança nacional e existem várias contingências plausíveis que podem levar as duas partes a um confronto militar. Ainda que existam vozes dissonantes na Europa em relação a esta matéria, os aliados europeus da NATO têm tradicionalmente assumido parte da agenda de segurança e defesa dos EUA a troco de garantias de segurança. No entanto, a China também representa um conjunto de riscos especificamente europeus. Refira-se, em particular, a resiliência e infraestrutura crítica, tendo em conta a forte dependência da tecnologia chinesa que se verifica na infraestrutura digital europeia. Atualmente, debate-se se a NATO é a plataforma ideal para estes temas, se a UE deve assumir um papel mais ativo ou se existe uma divisão de responsabilidades adequada entre estas duas organizações.
- As telecomunicações foram identificadas pela NATO como uma nova área de interesse. Para levar a cabo a sua missão principal de defesa coletiva, a NATO necessita de infraestruturas mais robustas para resistir a interferências de natureza híbrida. Contudo, na maioria dos países europeus as infraestruturas são detidas por privados. Isto torna-as suscetíveis a interferências externas e motivas decisões económicas que podem secundarizar aspetos de segurança nacional, caso não haja uma regulamentação legal clara. A Rússia é um estado que recorre a vários tipos de táticas híbridas no território da NATO. No entanto, a China também começou a usar várias táticas sofisticadas de natureza política e não militar face à NATO no seu conjunto e a países específicos, com vista a disseminar a sua influência política e económica.
- Para a resiliência ser o catalisador de maior cooperação entre a NATO e a UE, é necessário alcançar um equilíbrio em que os papéis de ambas as organizações estejam claramente definidos. Atualmente, a NATO está a adotar um enquadramento mais robusto, incluindo na dimensão não militar. A NATO visa principalmente a coordenação e a consulta política, a gestão de crises e a defesa coletiva, bem como a interoperabilidade. A UE, por seu lado, dispõe de um conjunto de instrumentos regulamentares, desde o conjunto de instrumentos para a cibersegurança das redes 5G ao Plano de Ação para a Democracia Europeia, que abordam algumas das questões mais vastas de resiliência. Como tal, deve ser apurada uma plataforma comum e responsabilidades partilhadas entre a UE e a NATO. Devem também ser estabelecidas ligações mais estreitas entre o planeamento da capacidade militar

tradicional e os requisitos de resiliência, pois este será um dos pilares fundamentais para o futuro da cooperação entre a NATO e a UE.

- Subsiste incerteza se a proteção de infraestruturas civis na Europa estaria abrangida pela NATO. Por outras palavras, um ciberataque a infraestruturas civis na Europa acionaria o Artigo 5. Caso não acione, é uma competência da UE? Além disso, nem sempre são claras as linhas que separam infraestruturas civis e militares, especialmente no que toca a telecomunicações.

- As telecomunicações estão a ganhar importância no funcionamento das nossas sociedades e economias, sendo também a base e o futuro da inovação. Estas duas dimensões, por sua vez, estão ligadas à corrida por supremacia tecnológica. A tecnologia tem sido um elemento essencial de dissuasão e defesa, e continuará a ser. O domínio tecnológico é essencial para se ter supremacia no campo de batalha, mas também fora dele. Para este domínio, é essencial uma base industrial robusta e em constante evolução, que integre inovação civil e militar, investigação e desenvolvimento. São necessárias iniciativas conjuntas de inovação transatlânticas para manter e reforçar as capacidades críticas, tanto dentro como fora do campo de batalha. Para isto, são necessárias ligações melhores e mais eficientes entre as indústrias civis e militares. A NATO precisa de começar a encontrar formas inteligentes de integrar as dimensões económicas subjacentes a determinados elementos das suas políticas de segurança, em particular numa altura em que a estratégia industrial está mais uma vez a ocupar um lugar de destaque na Europa e nos Estados Unidos. É necessário criar novos canais políticos para facilitar essa integração, para fortalecer a resiliência da aliança e manter a sua vantagem competitiva.

- Para já, a NATO não parece estar a ter qualquer tipo de dificuldade com este papel. Por isso, é necessária grande precisão na identificação e categorização dos problemas que se encontram sob o seu âmbito de atuação. Um primeiro passo para os políticos é a definição de parâmetros claros em áreas nas quais relações comerciais com a China não colocam em causa a segurança nacional. A NATO é também uma plataforma natural para trocas de pontos de vista em matéria de segurança entre várias instituições, entidades não estatais e parceiros da NATO com experiência em relações com a China, como o Japão ou a Coreia do Sul. Por conseguinte, a NATO deve continuar a dar prioridade à infraestrutura digital (5G/comunicações avançadas, cabos submarinos, etc.) e à China, mantendo-os em primeiro plano na sua agenda.

- Tendo em conta que as ciberameaças há muito que são uma área que preocupa a NATO, as redes 5G tornaram-se naturalmente um objeto de interesse nos debates da NATO, ainda que as dimensões de defesa destas redes tenham demorado a ser incluídas na agenda. Além disso, o processamento e armazenamento de dados são uma área de segurança prioritária que não deve ficar esquecida. O cerne da questão está em proteger o nosso setor público e as nossas indústrias, bem como garantir que as nossas empresas, cidadãos e instituições públicas possam enviar tráfego até ao destino sem passar por uma rede chinesa. Nas redes 5G, por exemplo, a infraestrutura de nuvem terá um papel muito importante. Ao abrigo da legislação chinesa, o governo daquele país pode solicitar e obter acesso aos dados de qualquer empresa privada na China, colocando em risco todos os dados existentes numa rede 5G chinesa. Na Bélgica, por exemplo, a infraestrutura de telecomunicações estava integralmente assente em equipamento chinês, incluindo as comunicações móveis usadas pelas administrações da UE e da NATO. Situação semelhante observa-se na Alemanha e em Portugal, onde há equipamento chinês nas redes nacionais, o que significa que o tráfego de dispositivos móveis de todas as tropas estacionadas na NATO passa, em algum momento, por redes dependentes de tecnologia chinesa. Estes países começam a ser observados como parceiros de risco dentro da Aliança. A nova lei alemã em matéria de segurança das TI faz uma justa referência às necessidades de segurança da NATO no que toca à avaliação da fidedignidade dos fornecedores. Contudo, mostra também que podem existir grandes divergências entre as ambições e a aplicação prática da lei: desde que a nova legislação entrou em vigor, no ano passado, a quota da Huawei na rede 5G da Deutsche Telekom (DT) aumentou para bem mais de 60%. Também em Portugal a utilização da Huawei em redes 5G tem continuado a acontecer. Em 2020, a nuvem da DT, criada e gerida pela Huawei, tem o centro de investigação nuclear (CERN) na Suíça como principal cliente de referência à

data do lançamento. Por outras palavras, o principal centro de investigação nuclear armazena dados numa nuvem chinesa. Um requisito mínimo deve, portanto, ser que as redes que sirvam funções de redes governamentais, a indústria da defesa e a segurança interna não estejam assentes em equipamento chinês. Além disso, as redes que sirvam funções críticas para a sociedade, como o setor de serviços de abastecimento público e a indústria farmacêutica, cuidados de saúde, bancos, transportes e comunicações também não devem ser comprometidas.

- Os aliados da NATO na Europa Oriental têm, até agora, mostrado relutância em reforçar a atenção que a NATO dedica à China, pois estão preocupados com a distração da ameaça russa. As últimas semanas têm mostrado o que a NATO tem de fazer: lidar com as ameaças da Rússia e da China. Na realidade, as duas estão interligadas. A guerra contra a Ucrânia comprovou, de forma drástica, o perigo iminente de agressão por parte do regime russo. Por outro lado, os laços cada vez mais estreitos entre a China e a Rússia, o apoio aberto da China em relação à postura que a Rússia adotou perante a NATO, a utilização maciça dos seus serviços de propaganda em favor das posições de Moscovo e a iminência de cedência de apoio económico por parte de Pequim – ou mesmo de armamento – reforçam o facto de que a cooperação sino-russa "sem limites" significa, essencialmente, cooperação contra o Ocidente. A NATO deve ter presente que as capacidades conjuntas sino-russas podem ser dirigidas contra objetivos russos na Europa, objetivos chineses na Ásia e interesses conjuntos noutras partes do mundo.
- Isto representa um agravamento muito significativo do risco de segurança decorrente da utilização de equipamento de telecomunicações chinês nas redes dos países aliados da Europa Central e Oriental. À medida que a NATO reforça as capacidades de defesa militar na sua fronteira oriental face à ameaça russa, as redes de telecomunicações na Polónia, na Roménia e noutros países continuam fortemente dependentes de equipamento chinês. Com efeito, nenhum destes países garante a remoção de fornecedores não fidedignos nos próximos anos. As regras mais exigentes até ao momento limitam a implementação de equipamento adicional de origem chinesa, mas aceitam o risco de equipamento mais antigo e não fidedigno até meados da década, ou mesmo mais, o que é uma abordagem que dificilmente se pode considerar aceitável. A possibilidade de, em caso de conflito, a China poder dar acesso à Rússia a redes de telecomunicações polacas através da Huawei ou ZTE, por exemplo, é bem real e tem consequências dramáticas.
- O custo de substituição da infraestrutura de telecomunicações chinesa na Europa não será proibitivo: à medida que as operadoras forem atualizando as redes de 4G para 5G, todo o equipamento anterior acabará por ser substituído. Por conseguinte, uma interdição total de novo equipamento da Huawei na Europa poderia durar "naturalmente" cerca de seis anos, até a base de equipamento não fidedigno instalada ser pura e simplesmente desativada por obsolescência. Contudo, a questão mais premente é garantir uma transição mais célere para tecnologia fidedigna por motivos de segurança nacional, cujo ritmo não deve ser determinado por considerações de curto prazo relacionadas com os prazos de obsolescência. Outro mito recorrente é os fornecedores chineses possuírem tecnologia mais avançada do que os fornecedores europeus. Os Estados Unidos e a Coreia do Sul são considerados líderes na implementação de redes 5G e nestes países a infraestrutura foi implementada sem recurso a equipamento chinês, tendo ambos apostado principalmente em tecnologia europeia. No que toca a preços, os fornecedores europeus também conseguem concorrer com as empresas chinesas, mas não conseguem concorrer com o Estado chinês. Os subsídios que a China atribui às suas empresas com operações nos mercados globais, assim como a preferência dada às empresas chinesas no mercado interno, continuam a distorcer a concorrência. A questão torna-se mais grave para as operadoras mais pequenas na Europa, América Latina e Ásia, que têm menor capacidade creditícia e, por isso, se veem obrigadas a recorrer a empréstimos chineses, a não ser que sejam oferecidos mecanismos de financiamento alternativos. Uma abordagem que tem vindo a ser apresentada como alternativa é a Open-RAN. Contudo, na prática, a presença e a influência da China nas estruturas de desenvolvimento deve levantar algumas questões e exige uma avaliação de risco completa.
- O conjunto de instrumentos da UE para a cibersegurança das redes 5G é um bom ponto de

partida para os próximos passos. No entanto, uma vez que é uma iniciativa voluntária, permite diferentes interpretações e implementações nos Estados-Membros da UE, o que pode criar vulnerabilidades. Um dos próximos passos poderia ser uma garantia de implementação mais rigorosa do conjunto de ferramentas em toda a UE. No entanto, o conjunto de instrumentos da UE para a cibersegurança das redes 5G apenas pode ser o ponto de partida. As redes que fazem a ligação de recursos críticos através de fibra ótica, cabos de transporte e cabos submarinos carecem do mesmo escrutínio e implementação rigorosa das salvaguardas a que o acesso via rádio e a rede de base estão sujeitos. Pode prever-se o desenvolvimento partilhado de conjuntos de instrumentos para estes perímetros de rede.

- Não obstante a linguagem com nuances adotada nas cimeiras da OTAN de 2021/02, os aliados concordaram que o comportamento da China interfere nos nossos princípios democráticos e segurança nacional. Por conseguinte, o desafio sistémico que a China representa tornou-se um elemento central da agenda da NATO e foi amplificado com a intensificação da colaboração entre a Rússia e a China. A política da Aliança em relação à China foi concretizada no Conceito Estratégico adoptado na Cimeira de Madrid. O maior desafio para a NATO será encontrar uma resposta simultânea para as numerosas e diversas ameaças que enfrenta: dissuasão híbrida, tecnologias emergentes e disruptivas, e infraestruturas críticas vulneráveis. Devido ao panorama de segurança em rápida mudança e ao desenvolvimento acelerado da tecnologia, ter a capacidade de atingir a excelência em todas as frentes será essencial para continuar a garantir o sucesso da NATO.