FACULDADE DE DIREITO UNIVERSIDADE NOVA DE LISBOA

CEDIS CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

DIREITO, SEGURANÇA E DEMOCRACIA

AS AMEAÇAS HÍBRIDAS – UMA ABORDAGEM CONCEPTUAL NO QUADRO DA OTAN E DA UE

Hybrid threats - A conceptual approach in the EU and NATO frameworks

JOÃO PEREIRA
Doutorando em Direito e Segurança

RESUMO

Atendendo à crescente preocupação dos países da UE e da OTAN perante um novo quadro de ameaças proporcionado pela interconetividade e informatização da vida moderna, as ameaças híbridas têm vindo a causar apreensão pelo potencial subversivo que acarretam para o Estado de direito democrático. A dificuldade de definição concetual das ameaças híbridas tem afetado a compreensão deste fenómeno e, consequentemente, a capacidade de prevenção e resposta dos países visados, tendo, recentemente, a UE e a OTAN colaborado na elaboração e implementação de uma estratégia coordenada destinada, por um lado, à compreensão do fenómeno e, por outro, à preparação de uma capacidade de resposta. Caracterizadas por ações multidimensionais coordenadas e sincronizadas, as ameaças híbridas empregam um

leque amplo de meios que tendem a explorar os limiares da deteção e da autoria, explorando, também, os limites da paz e da guerra, procurando afetar os interesses estratégicos dos países visados.

PALAVRAS-CHAVE

Ameaças híbridas, segurança, OTAN, UE, estratégia

ABSTRACT

Given the growing concerns of the EU and NATO regarding the new framework of threats that arise from the interconnectivity and the digitation of modern life, hybrid threats have been raising major apprehensions to the rule of law and democratic States in consequence of the subversive potential they carry. The difficulties associated to the conceptual definition of hybrid threats have been affecting the understanding of this phenomenon and, consequently, the capacity of prevention and response of the affected countries. To that end, the EU and NATO have been collaborating to the elaboration and implementation of a strategy aimed at understanding the phenomenon and preparing a response capacity. Hybrid threats are multidimensional, coordinated and synchronized actions that use a wide range of means that tend to exploit the limits of detection and authorship, as well as limits of peace and war, seeking to undermine the strategic interests of the targeted countries.

KEYWORDS

Hybrid threats, security, NATO, EU, strategy

Índice

1. Introdução

No passado dia 13 de Junho de 2018, a Alta Representante para a União Europeia e os Negócios Estrangeiros e para a Política de Segurança, em conjunto com a Comissão Europeia, publicou uma comunicação conjunta intitulada "*Joint Communication to the European Parliament, the European Council and the Council: Increasing resilience and bolstering capabilities to address hybrid threats*"[1], na qual se definem as linhas de ação estratégica para combater as ameaças híbridas.

[1] Comissão Europeia e Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança. 2018. Joint Communication to the European Parliament, the European Council and the Council: *Increasing resilience and bolstering capabilities to address hybrid threats* JOIN(2018) 16 Final. *European Union External Action - Press and Media - Documents*. [*Online*] 13 de Junho de 2018. Acedido a 23 de Agosto de 2018, em https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf.

Este documento representa o culminar de um longo processo de definição do conceito de ameaças híbridas, cuja definição se verá mais adiante, traduzindo ainda a estratégia das instituições comunitárias para atender este fator de condicionamento securitário. Conforme este trabalho se propõe demonstrar nas páginas que se seguem, aquele documento representa também o resultado da cooperação com outras instituições, como a Organização do Tratado do Atlântico Norte (OTAN), principal precursora do conceito, evidenciando, também, a necessidade de colaboração interinstitucional que esta temática requer.

Num mundo de elevada e crescente interconetividade, o conceito de ameaças híbridas tem vindo a ganhar maior amplitude, compreendendo a cada vez mais significativa complexidade dos tempos modernos e contribuindo para enformar as políticas de segurança dos Estados-Membros da União Europeia e da OTAN.

Neste sentido, e face ao acima exposto, o vertente trabalho propõe-se a, numa primeira parte, definir o conceito de ameaças híbridas, atendendo-se em particular ao sentido que lhe é atribuído pela OTAN e pela União Europeia (UE), para, numa segunda parte, identificar os principais tipos de ameaças híbridas. Antes de concluir este trabalho, as páginas seguintes propõem-se, numa terceira parte, a caracterizar tipologicamente as ameaças híbridas e, numa quarta parte, a expor e a analisar as linhas de orientação estratégica da União Europeia e da OTAN para combater este fenómeno.

2. As ameaças híbridas – Definição concetual

2. 1 Origem do conceito de ameaças híbridas

Segundo os dados disponíveis, o conceito de ameaças híbridas foi formalmente referido em Junho de 2015, na sequência da reunião dos Ministros da Defesa da Organização do Trato do Atlântico Norte (OTAN), em Bruxelas, que emitiram uma declaração, na qual, no seu ponto 7, se estatui o seguinte: "*To enhance the ability to respond quickly and effectively to any contingency, we have significantly adapted our advance planning. We have also adapted our decision making procedures to enable the rapid deployment of our troops. We have set the key elements for an effective response to hybrid threats. We will seek close coordination and coherence with the European Union's*

efforts in this field. We have also agreed concrete steps for NATO's adaption to the growing challenges and threats emerging from the south".[2]

Até àquela ocasião, a expressão usada era "guerra híbrida" (do inglês, *hybrid warfare*) – que, de resto, se mantém –, que, inicialmente, segundo Jan J. Andersson e Thierry Tardy, no Issue Brief 32 do Instituto de Estudos de Segurança da União Europeia de 2015[3], terá sido sugerida em 2002, na tese de William J. Nemeth (*Future War and Chechnya: a Case for Hybrid Warfare*)[4]. O conceito de guerra híbrida, conforme proposto por Nemeth, remetia para a natureza híbrida das sociedades, aparentemente menos estruturadas e menos socioeconomicamente desenvolvidas, como era o caso da Chechénia, na altura, e que, devido à assimetria dos meios disponíveis, principalmente comparado com os meios políticos, económicos, tecnológicos e militares convencionais das sociedades Ocidentais, desenvolveram formas de confronto híbridas para colmatar a sua inferioridade naqueles campos, recorrendo, entre outros meios, a campanhas de desinformação e táticas de guerrilha que não obedecem ao Direito Internacional (como seja o caso das Convenções de Genebra e das Convenções da Haia sobre o Direito da Guerra) e às formas ditas convencionais de confronto armado.

O termo "guerra híbrida" terá sido posteriormente utilizado[5], em 2005 e 2006, para descrever as estratégias desenvolvidas pelo Hezbollah, no âmbito da Guerra do Líbano, para descrever a combinação de meios convencionais e não-convencionais, regulares e irregulares, abertos e encobertos que foram empregues naquele conflito.

Ganhando tração, o conceito de guerra híbrida terá também sido mencionado, ainda que de forma indireta, no documento produzido de preparação para a Cimeira da OTAN de Lisboa, em 2010, designado *NATO 2020: assured security; dynamic*

[2] OTAN. 2015. Statement by NATO Defence Ministers. Bruxelas, 25 de Junho de 2015. Acedido em 20 de Agosto de 2018, em https://www.nato.int/cps/en/natohq/news_121133.htm?selectedLocale=en.
[3] ANDERSSON, Jan J. e TARDY, Thierry, 2015. *Hybrid: what's in a name?*: European Union Institute for Security Studies, Outubro de 2015. ISSUE Briefs, Vol. 32. ISSN 2315-1110.
[4] NEMETH, William J. 2002. Future war and Chechnya: a case for hybrid warfare. Monterey, California, EUA, Junho de 2002. Tese de mestrado no âmbito do Programa de Mestrado em Assuntos de Segurança Nacional da Naval Postgraduate School de Monterrey, California (EUA).
[5] VAN PUYVELDE, Damien. 2015. *Hybrid war – does it even exist?* NATO Review Magazine. [*Online*] 07 de Maio de 2015. Acedido a 24 de Agosto de 2018, em https://www.nato.int/docu/review/2015/also-in-2015/hybrid-modern-future-warfare-russia-ukraine/en/index.htm.

engagement[6], em que são mencionadas as "variações híbridas" das ameaças que enfrentam os países membros da OTAN e a necessidade de os Países da Aliança reverem a sua conceção das ameaças que se vislumbram. Nesse relatório[7], concluiu-se ainda o seguinte:

- *"Conventional military aggression against the Alliance or its members is unlikely but the possibility cannot be ignored"*.
- "*The most probable threats to Allies in the coming decade are unconventional. Three in particular stand out: 1) an attack by ballistic missile (whether or not nuclear-armed); 2) strikes by international terrorist groups; and 3) cyber assaults of varying degrees of severity. A host of other threats also pose a risk, including disruptions to energy and maritime supply lines, the harmful consequences of global climate change, and financial crisis*".
- "*The danger posed by unconventional threats has obvious implications for NATO preparedness, including its definition of security, its conception of what constitutes an Article 5 attack, its strategy for deterrence, its need for military transformation, its ability to make decisions rapidly, and its reliance for help on countries and organisations from outside the Alliance*".

Já na Cimeira da OTAN de 2014, no País de Gales, o conceito de guerra híbrida ganhou maior densidade, tendo sido referido de forma expressa na Declaração Final, para caracterizar as ameaças que ora se apresentam aos países da Aliança no século XXI, que as "ameaças de guerra híbrida" ("*hybrid warfare threats*") se constituem como um conjunto amplo de medidas, encobertas e abertas, militares, paramilitares e civis, utilizadas de forma altamente integrada ("*a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design*"")[8]. Esta

[6] ALBRIGHT, Madeleine e VAN DER VEER, Jeroen et al. 2010. *NATO 2020: assured security; dynamic engagement - Analysis and recommendations of the group of experts on a new strategic concept for NATO.* NATO Public Diplomacy Division. Bruxelas, 2010. Documento elaborado com vista à preparação da Cimeira da OTAN de Lisboa, em 2010, e à revisão do Conceito Estratégico da OTAN. Acedido a 24 de Agosto de 2018, em https://www.nato.int/strategic-concept/expertsreport.pdf.

[7] ALBRIGHT, Madeleine e VAN DERR VEER, Jeroen et al. 2010. *NATO 2020:* … cit..

[8] OTAN. 2014. Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. NATO, e-Library, Official texts. [*Online*] 05 de Setembro de 2014. Acedido a 26 de Agosto de 2018, em https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

formulação procurava traduzir, de forma ainda frágil, um novo modelo de ameaças globais, refletindo um novo panorama securitário mundial, sem que a sua delimitação concetual estivesse consolidada, deixando antever aquilo que viria a ser o conceito de ameaças híbridas efetivamente adotado pela OTAN.

2. 2 Definição do conceito de ameaças hibridas

O conceito de ameaças híbridas, conforme acima exposto, registou uma evolução ao longo dos últimos quinze anos, acompanhando a evolução proporcionada pelas inovações tecnológicas no mundo das telecomunicações, no meio cibernético e da consequente interconetividade galopante que marcou o século XXI.

Depois da reunião dos Ministros da Defesa da OTAN, em Julho de 2015, importa referir que foi proposta a criação do Centro Europeu de Excelência para Combater as Ameaças Híbridas (*European Centre of Excellence for Countering Hybrid Threats*)[9], no passado dia 06 de Abril de 2016, constando da *Comunicação conjunta ao Parlamento Europeu e ao Conselho, Quadro comum em matéria de luta contra as ameaças híbridas, Uma resposta da União Europeia*[10], tendo esta proposta sido posteriormente apoiada, em 06 de Dezembro de 2016, pelo Conjunto de propostas comuns para a implementação da Comunicação Conjunta pelo Presidente do Conselho Europeu, o Presidente da Comissão Europeia e o Secretário-Geral da OTAN [11] (*Common set of proposals for the implementation of the Joint Declaration by the President of the European Council, the*

[9] Sedeado na Finlândia, o *European Centre of Excellence for Countering Hybrid Threats* foi criado com o patrocínio institucional da UE e da OTAN, sendo ainda participado pelos Governos de República Checa, Dinamarca, Estónia, Finlândia, França, Itália, Alemanha, Letónia, Lituânia, Holanda, Noruega, Polónia, Espanha, Suécia, Reino Unido e Estados Unidos. A participação no Centro encontra-se aberta a todos os membros da UE e da OTAN (European Centre of Excellence for Countering Hybrid Threats. *About us. European Centre of Excellence for Countering Hybrid Threats*. [*Online*] Acedido a 5 de Setembro de 2018, em https://www.hybridcoe.fi/about-us/).

[10] Comissão Europeia. 2016. *Comunicação conjunta ao Parlamento Europeu e ao Conselho, Quadro comum em matéria de luta contra as ameaças híbridas, Uma resposta da União Europeia JOIN(2016) 18 final*. Bruxelas, 06 de Abril de 2016. Acedido a 25 de Agosto de 2018, em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52016JC0018&from=EN.

[11] 2016. *Common set of proposals for the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization*. 06 de Dezembro de 2016. Acedido a 31 de Agosto de 2018, em https://www.hybridcoe.fi/wp-content/uploads/2017/08/Common-set-of-proposals-for-the-implementation-of-the-Joint-Declaration-2.pdf.

President of the European Commission and the Secretary General of the North Atlantic Treaty Organization).

Nestes dois documentos supracitados, não foi definido o conceito de ameaças hibridas, já que uma das missões do Centro de Excelência, sedeado na Finlândia, será precisamente o de estudar o fenómeno e definir novos conceitos para que este fenómeno possa ser melhor entendido. Com efeito, o conceito de ameaças híbridas voltou a ser abordado na Cimeira de Chefes de Estado, em Varsóvia, em Julho de 2016, figurando expressamente no Comunicado emitido na sequência daquele evento, no qual se menciona o conceito de ataques híbridos (ponto 5)[12] e a necessidade do acordo celebrado, entre os Aliados, de definir uma estratégia para combater a guerra híbrida no quadro da OTAN (ponto 37)[13]. Nesse mesmo documento, é mencionado, no ponto 72[14], o combate à guerra híbrida, levada a cabo por meio de ameaças híbridas, que a OTAN aparenta definir como "uma combinação ampla, complexa e adaptável, de meios convencionais e não-convencionais e de medidas militares, paramilitares e civis, encobertas e abertas, utilizadas de forma integrada por atores estatais e não estatais para alcançar os respetivos objetivos ("a *broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, are employed in a highly integrated design by state and non-state actors to achieve their objectives*").

Conforme mencionado[15] por Andersson e Tardy, uma das principais dificuldades associadas à definição do conceito de ameaças híbridas prende-se precisamente com a

[12] OTAN. 2016. Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. *OTAN, e-Library, Official texts*. [*Online*] 09 de Julho de 2016. Acedido a 29 de Agosto de 2018, em https://www.nato.int/cps/ic/natohq/official_texts_133169.htm.

[13] OTAN. 2016. Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. *OTAN, e-Library, Official texts*. [*Online*] 09 de Julho de 2016. Acedido a 29 de Agosto de 2018, em https://www.nato.int/cps/ic/natohq/official_texts_133169.htm.

[14] OTAN. 2016. Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. *OTAN, e-Library, Official texts*. [*Online*] 09 de Julho de 2016. Acedido a 29 de Agosto de 2018, em https://www.nato.int/cps/ic/natohq/official_texts_133169.htm.

[15] ANDERSSON, Jan J. e TARDY, Thierry, 2015. *Hybrid: what's in a name?*: European Union Institute for Security Studies, Outubro de 2015. ISSUE Briefs, Vol. 32. ISSN 2315-1110.

sua delimitação material, já que a destrinça entre uma ameaça considerada convencional e outra considerada híbrida é particularmente ténue, não sendo evidentes as diferenças:

"(…) *a key element of this is establishing a clear understanding of what exactly hybrid threats are, i.e. how they differ from 'non-hybrid' ones. Simply put, for a threat to be of a 'hybrid' nature it needs to be the product of multiple ways to threaten or attack its intended target – much as a hybrid species is produced by combining different breeds or varieties. It is therefore the mix of different methods – conventional and unconventional, military and non-military – which makes a threat hybrid*."[16]

Neste sentido, e em consonância com o acima exposto, poderá afirmar-se que o que contribui para definir o conceito de ameaça híbrida reside precisamente na natureza variada e difusa das ameaças utilizadas, unidas pela cúpula de um objetivo comum e usadas de forma sistemática, conforme sublinham Andersson e Tardy:

"*In this sense, not all contemporary threats are hybrid. For example, a terrorist group which mainly plants bombs or makes use of suicide bombers does not, in and by itself, constitute a hybrid threat.*

It is only if and when such an outfit combines such tactics with, for example, the launching of military campaigns, systematically spreading disinformation or running criminal activities that the threat mutates into a hybrid one. Terrorism, cybercrime, trafficking and extortion are not per se hybrid in nature; they may become so depending on how (and to what extent) they are pursued using multiple tactics simultaneously."[17]

Assim, não será pela verificação da concretização de uma ameaça que se poderá determinar estar-se perante ameaças híbridas, mas, antes, pela verificação de diversas ameaças combinadas, de forma sistemática, pelos mesmos perpetradores, na prossecução de um objetivo específico.

Neste quadro, e face à evidente densidade concetual que carateriza as ameaças híbridas, será de destacar que, a nível institucional, designadamente no atinente à União Europeia, a OTAN e o Centro de Excelência Europeu para Combater as Ameaças

[16] ANDERSSON, Jan J. e TARDY, Thierry, 2015. *Hybrid: what's in a name*…, cit. pp 1.
[17] ANDERSSON, Jan J. e TARDY, Thierry, 2015. *Hybrid: what's in a name*…, cit. pp 1.

Híbridas (*European Centre of Excellence for Countering Hybrid Threats*) criado por aquelas duas organizações, tem-se frequentemente definido o conceito de ameaças híbridas procurando-se descrever o fenómeno em vez de definir concretamente a sua delimitação concetual. Esta situação decorre da complexidade da realidade que se procura compreender nestas páginas, decorrendo ainda da multiplicidade dos atores que poderão estar envolvidos, não sendo ainda o fenómeno das ameaças híbridas suficientemente estudado para ser conhecido com a abrangência que possivelmente implica. Paralelamente, a atribuição da autoria das referidas ameaças terá alguma relevância na sua identificação, bem como na classificação da sua natureza híbrida, densificando o conceito e dificultando a sua apreensão.

Não obstante, o *European Centre of Excellence for Countering Hybrid Threats*, incumbindo pela UE e pela OTAN de aprofundar o conhecimento sobre as ameaças híbridas [18] , define-as como "ações coordenadas e sincronizadas que visam deliberadamente afetar as vulnerabilidades dos Estados democráticos e das suas instituições, empregando um leque particularmente amplo de meios políticos, económicos, militares, civis e de informação"[19].

O centro avança ainda que os autores das ameaças híbridas tendem a explorar os limiares da deteção e autoria, operando, frequentemente, nas zonas de indefinição da autoria, explorando, também, os limites da paz e da guerra. Com esta forma de procedimentos, o centro defende que os autores das ameaças híbridas procuram influenciar o processo de tomada de decisão (*decision-making*), nomeadamente político e institucional, a nível local, regional ou nacional, procurando, ainda, afetar os interesses estratégicos dos visados[20].

[18] European Centre of Excellence for Countering Hybrid Threats. *About us. European Centre of Excellence for Countering Hybrid Threats*. [*Online*] Acedido a 5 de Setembro de 2018, em https://www.hybridcoe.fi/about-us/.
[19] European Centre of Excellence for Countering Hybrid Threats. *Hybrid Threats. European Centre of Excellence for Countering Hybrid Threats*. [*Online*] Acedido a 05 de Setembro de 2018, em https://www.hybridcoe.fi/hybrid-threats/.
[20] European Centre of Excellence for Countering Hybrid Threats. *Hybrid Threats. European Centre of Excellence for Countering Hybrid Threats*. [*Online*] Acedido a 05 de Setembro de 2018, em https://www.hybridcoe.fi/hybrid-threats/.

A verificação de ameaças híbridas, segundo o *European Centre of Excellence for Countering Hybrid Threats*, implica, assim: i) o envolvimento de atores estatais e não-estatais; ii) o desafio à ordem estabelecida, caracterizando os visados como ameaças, opositores ou concorrentes; iii) o recurso a um amplo leque de métodos e atividades; iv) o aproveitamento das vulnerabilidades dos seus opositores; v) vulnerabilidades que podem ser reais ou criadas, podendo derivar do aproveitamento de memórias históricas, falhas legais, práticas consuetudinárias, fatores geoestratégicos, polarização da sociedade, desvantagem tecnológica ou diferenças ideológicas, entre muitas outras possibilidades; e vi) a escalada da gravidade das ameaças híbridas nos níveis de violência, caso os objetivos pretendidos não sejam imediatamente alcançados.

3. Caracterização tipológica das ameaças híbridas

Conforme resulta do acima exposto, as ameaças híbridas assumem uma natureza particularmente complexa e caracterizada por uma multiplicidade de meios, sendo, não raras as vezes, difícil determinar que tipo de ocorrências podem ser efetivamente classificadas de híbridas. Não obstante, as próximas páginas deverão dedicar-se a essa tarefa, procurando identificar e caracterizar algumas das ameaças consideradas híbridas que poderão ser tidas em consideração no contexto proposto.

Seguindo o acima exposto, as ameaças híbridas combinam atividades convencionais e não-convencionais, militares e não militares, utilizadas de forma coordenada por atores estatais e não-estatais, recorrendo ainda a campanhas multidimensionais que combinam medidas coercivas e subversivas, com vista ao alcance de objetivos políticos. Assim, e atendendo a definição de ameaças híbridas seguida no presente trabalho, torna-se evidente a dificuldade em fazer a destrinça entre o rol de potenciais ameaças que poderão estar incluídas ou excluídas deste quadro, já que, sob a alçada do conceito proposto, poderá caber a quase totalidade das realidades bélicas.

As ameaças híbridas poderão assim, neste quadro, abranger desde as campanhas mediáticas à utilização de armas químicas, biológicas, radiológicas e nucleares, passando por ciberataques contra os sistemas informáticos de infraestruturas estratégicas ou pela utilização de meios de subversão da paz social ou da ordem económica.

A maioria das táticas abaixo identificadas não serão particularmente novas, mas encontram-se exponencialmente mais acessíveis e fáceis de utilizar graças às novas

tecnologias e à interconetividade do séc. XXI, que proporcionam meios consideravelmente mais eficientes e eficazes de alcançar os objetivos a que se propõem os autores das ameaças híbridas, sendo também de mencionar, a este propósito, a rápida propagação dos efeitos que aquelas mesmas tecnologias propiciam[21]. Entre o rol de ameaças que têm vindo a ser identificadas como híbridas, serão de destacar, entre outras possíveis, as seguintes[22]:

- **Propaganda**

A propaganda representa um dos casos de meios empregues no quadro das ameaças híbridas que não são novos, constituindo-se como a instrumentalização da informação com o propósito de influenciar a perceção das populações dos países visados e dos seus líderes através de campanhas mediáticas, quer nos meios convencionais de comunicação social, como os jornais e as televisões, quer, na atualidade, nas redes sociais. Devido à massificação do acesso à Internet e à proliferação de meios de comunicação, esta ameaça representa hoje um instrumento particularmente acessível e barato de disseminar ideias e veicular ideologias. Acresce, neste quadro, que a elevada competitividade dos meios de comunicação social e das redes sociais para reforçarem as suas quotas de mercado, bem como a celeridade considerável com que circula a informação, têm contribuído, também, para a sua mais fácil instrumentalização, já que a capacidade de verificação dos factos noticiosos e a ocupação imediata dos tempos de antena não se coadunam com o tempo da reflexão crítica e da verificação factual.

- **Meios noticiosos estatais ou paraestatais**

À semelhança do caso anterior, este meio será já bem conhecido, constituindo-se como os meios noticiosos direta ou indiretamente financiados pelos Estados que os apoiam – podendo também ser meios noticiosos com elevada afinidade política com o regime no poder –, beneficiando de uma visibilidade e credibilidade sustentada na

[21] TREVERTON, Gregory F., et al.. *Addressing Hybrid Threats*. Estocolmo, Swedish Defence University, 2018. ISBN 978-91-86137-73-1. Acedido em 25 de Agosto de 2018, em https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf.
[22] TREVERTON, Gregory F., et al.. *Addressing Hybrid Threats*…, cit., pp. 45 a 61.

proximidade ao Estado, como sejam a *Russia Today* ou *Sputnik News*, no caso da Rússia, ou da *Xinhua*, no caso da China. Estes meios noticiosos, reputados sérios, veiculam as ideias e as opiniões oficiais dos regimes que apoiam e apresentam as notícias e os factos naquela perspetiva, recorrendo, não raras as vezes, à distorção da veracidade dos factos para coincidir com a retórica pretendida. Esta situação será já amplamente do conhecimento do público melhor informado, surtindo efeitos mais moderados sobre os decisores, pese embora contribua, ainda que parcialmente, para a desinformação em massa e para a penetração na opinião pública das ideias dos respetivos regimes.

- **Redes sociais**

O potencial para alcançar em massa as populações por via das redes sociais tem vindo a ser consideravelmente explorado no domínio das ameaças híbridas, já que possibilitam a disseminação rápida e em larga escala de ideias e notícias de forma praticamente gratuita, possibilitando um imediatismo e sensacionalismo exponenciais face aos dois casos anteriores acima expostos. Por outro lado, as redes sociais possibilitam o anonimato das mensagens veiculadas, dificultando a identificação da sua origem, bem como, frequentemente, da sua veracidade. Acresce que o reencaminhamento das notícias, factos, ideias e ideologias por via das redes sociais permite a propagação de campanhas mediáticas à escala global num curto período de, por vezes, horas. De entre as redes socias que mais se têm destacado, neste campo, cumpre referir o *Twitter* e o *Facebook*, cuja instalação simples e rápida nos equipamentos privados de telecomunicação, como os *smartphones*, possibilita que os cidadãos sejam imediatamente alcançáveis por esta via. A este propósito, segundo estudos, designadamente do *Pew Research Center*[23], em 2016, cerca de 67% dos adultos norte-americanos recebiam as suas notícias via *Twitter* e *Facebook*, contrastando com uma percentagem de 62%, no ano anterior, evidenciando o amplo alcance que aquelas duas redes sociais potenciam, bem como uma tendência de crescimento daquele fenómeno. A título exemplificativo, Treverton [24] menciona que centenas de jovens russos foram empregados por *troll farms*, em São Petersburgo, incumbidos da missão de multiplicar-se

[23] TREVERTON, Gregory F., et al.. *Addressing Hybrid Threats*…, cit., pp. 47 a 48.
[24] TREVERTON, Gregory F., et al.. *Addressing Hybrid Threats*…, cit., pp. 47 a 48.

em publicações e comentários nas redes sociais na Internet, preferencialmente nas páginas de audiência norte-americana, para favorecer a opinião pública sobre a candidatura de Donald Trump às eleições Presidenciais dos Estados Unidos, em 2016[25].

- **Notícias falsas ou *fake news***

Na sequência do que vem sendo exposto, será também de sublinhar o conceito de notícias falsas ou, mais popularmente conhecido como *fakes news*, cujo propósito, como o nome indica, é a disseminação de notícias falsas, que distorcem a realidade. Este fenómeno será relativamente novo e terá sido identificado aquando da campanha para as eleições presidenciais norte-americanas, procurando alegadamente favorecer a eleição de Donald Trump[26]. As *fake news*, quando não absolutamente falsas, usarão de uma base parcialmente verídica, sendo distorcida e publicada em meios reputados e prestigiosos de informação, nas redes sociais e na comunicação social, na esperança que, com a celeridade da circulação da informação, os designados *mainstream media* as aceitem como verdadeiras e as redifusem por sua vez, sem verificação[27]. As notícias tendem a ser de consumo rápido e de fácil compreensão, recorrendo a preconceitos e *clichés* de forma a facilitar a sua penetração na opinião pública e nos decisores políticos, contribuindo para a propagação em massa de ideais populistas. Paralelamente, outro dos objetivos das *fakes news* é de amplificar fenómenos mediáticos e causar danos

[25] As *troll farms* constituem-se como empresas politicamente ativas e próximas dos regimes que as patrocinam ou apoiam para empregar pessoas que se dedicam, em exclusivo, à publicação de mensagens politizadas e enviesadas nas redes sociais e de publicar comentários exagerados de apoio ou rejeição às notícias publicadas de outras fontes nas mesmas redes (LEE, Dave, BBC News, 16 de Fevereiro de 2018. *The tactics of a Russian troll farm*: https://www.bbc.com/news/technology-43093390, acedido em 08 de Setembro de 2018.

[26] GAURON, Roland, Le Figaro, 07 de Março de 2017. *«Fake news», un même terme pour plusieurs réalités*: http://www.lefigaro.fr/actualite-france/2017/03/06/01016-20170306ARTFIG00187-fake-news-un-meme-terme-pour-plusieurs-realites.php, acedido a 08 de Setembro de 2018.

[27] CUDDY, Alice, Euronews, 06 de Setembro de 2018. *1 in 3 news articles shared about Sweden election are fake, finds study*: http://www.euronews.com/2018/09/06/1-in-3-news-articles-shared-about-sweden-election-are-fake, acedido em 08 de Setembro de 2018.

reputacionais ou causar uma falsa impressão generalizada de discórdia e descontentamento público.

- **Fugas estratégicas de informações**

A fuga estratégica de informações traduz-se na publicação de documentos oficiais – ou oficiosos – de personalidades ou instituições relevantes da vida pública e política, visando a sua descredibilização e causar danos reputacionais consequentes, minando a confiança pública nas instituições ou personalidades políticas de relevo. Um dos casos mais recentes deste tipo de ameaças verificou-se aquando da campanha presidencial francesa, quando, 48h antes do dia das eleições, naquilo que viria a ser conhecido como o *MacronLeaks*, em 2017, foram divulgados *e-mails* de Emmanuel Macron e documentos alegadamente comprometedores da sua idoneidade [28], procurando, por esta via, influenciar o curso das eleições presidenciais francesas. Os documentos teriam sido alegadamente obtidos por via da ciberespionagem, explorando as vulnerabilidades do seu sistema de segurança informática e foram publicados no *Twitter*, uma rede social que se tornou numa importante ferramenta para o jornalismo e para a vida política Ocidental.

- **Financiamento de organizações**

O financiamento, direto ou indireto, de organizações por parte de Estados tem-se constituído como uma prática relativamente comum e já bem conhecida, sobretudo no caso de organizações de índole político ou académico, procurando-se, por esta via, a influência da opinião pública, do discurso político e do decurso da vida política dos países visados junto das elites intelectuais [29]. Entre as organizações que têm sido privilegiadamente escolhidas para este tipo de ação, destacam-se os *think tanks*, os partidos políticos ou outras entidades da sociedade civil que possam ter uma visibilidade e alguma capacidade de influência no país.

---

[28] MARTINS, Alexandre, Público, 06 de Maio de 2017. *Os emails de Macron podem ser inofensivos, mas este jogo chama-se "suspeita"*: https://www.publico.pt/2017/05/06/mundo/noticia/os-emails-de-macron-podem-ser-inofensivos-mas-este-jogo-chamase-suspeita-1771195, acedido em 08 de Setembro de 2018.

[29] TREVERTON, Gregory F., et al.. *Addressing Hybrid Threats*…, cit., pp. 50 a 51.

A título de exemplo, refira-se o caso do *Institute for China-American Studies*, em Washington, nos Estados-Unidos, um *think tank* criado em 2015 e diretamente financiado pelo Governo chinês[30], com o propósito de favorecer a imagem da China nos Estados-Unidos e no Ocidente, contribuindo, ainda, para a divulgação da cultura chinesa e da perspectiva política da China sobre o mundo.

Também a título de exemplo, refira-se a possibilidade de financiamento indireto de partidos políticos, como terá alegadamente sido o caso com o partido francês de Marine Le Pen, o *Front National*, que, durante a campanha eleitoral para as presidenciais francesas, terá recebido capitais russos para financiar a sua atividade[31] e influenciar o resultado das eleições. Também de salientar, neste contexto, as alegadas interferências russas em Itália, tendo o Kremlin alegadamente apoiado campanhas de desinformação e de protesto contra os movimentos migratórios dos refugiados e fomentar uma maior recetividade do povo italiano aos ideais de extrema-direita[32].

Merece também destaque o apoio dado a movimentos de protesto, separatistas ou de subversão, como terá sido alegadamente o caso na Bulgária, em que Moscovo terá apoiado protestos contra a exploração e produção de gás de xisto (*shale gas*) naquele país, naquilo que terá sido um boicote velado aos esforços de um Estado-Membro da UE de reduzir a sua dependência dos fornecimentos de gás russo[33], resultando no

---

[30] FISH S., Isaac. 2016. Beijing Establishes a D.C. Think Tank, and No One Notices. *Foreign Policy*. 07 de Julho de 2016. Acedido a 25 de Agosto, em https://foreignpolicy.com/2016/07/07/beijing-establishes-washington-dc-think-tank-south-china-sea/.

[31] *Quels sont les liens troubles entre le Front national et le Kremlin?* HADDAD, Marie-Pierre. RTL. 2018. 14 de Março de 2018. RTL. Acedido a 08 de Setembro de 2018, em https://www.rtl.fr/actu/politique/quels-sont-les-liens-troubles-entre-le-front-national-et-le-kremlin-7792607362.

[32] *How Russian networks worked to boost the far right in Italy.* ALANDETE, David, VERDÚ, Daniel. El País. 2018. 01 de Março de 2018. Acedido a 03 de Setembro de 2018, em https://elpais.com/elpais/2018/03/01/inenglish/1519922107_909331.html.

[33] *Russian Money Suspected Behind Fracking Protests*. HIGGINS, Andrew. 2014. The New York Times. 30 de Novembro de 2014. Acedido a 10 de Setembro de 2018, em https://www.nytimes.com/2014/12/01/world/russian-money-suspected-behind-fracking-protests.html.

cancelamento da licença atribuída à empresa norte-americana Chevron para aquele efeito.

- **Instrumentos cibernéticos**

As ameaças de natureza cibernética têm vindo a ganhar uma nova projeção no panorama securitário global, tendo vindo a ser cada vez mais recorrentes os ataques associados à era da informática e da híper-conetividade. Assim, serão de mencionar, entre as principais ameaças cibernéticas conhecidas, a ciberespionagem, os ciberatques e a cibermanipulação.

Relativamente à ciberespionagem, cabe referir que os objetivos são, na prática, semelhantes em quase tudo à espionagem convencional, designadamente a recolha de informações que, de outra forma não seriam acessíveis, sem o conhecimento do seu detentor. Em 2016, aquando da campanha eleitoral para as presidenciais norte-americanas, foram várias as notícias sobre os possíveis ciberataques russos contra organizações políticas dos Estados-Unidos [34], nomeadamente para favorecer a candidatura de Donald Trump.

Já no que diz respeito aos ciberataques, será de destacar o *Stuxnet*, que consiste num *malware* que, para além do roubo de informações, causou danos físicos aos sistemas informáticos e aos equipamentos por estes controlados, tendo visado as centrais nucleares iranianas, em 2009. Embora a autoria do vírus não será conhecida, existem notícias aventando suspeitas sobre os Estados-Unidos e Israel[35].

Quanto à ciber-manipulação, que consiste na infiltração dos sistemas informáticos para manipular ou alterar os dados neles armazenados, cumpre destacar que a sua ocorrência será, de momento, ainda pouco comum, pese embora os casos conhecidos tenham causado prejuízos avultados na economia dos países visados. A título de exemplo, recorde-se o caso dos *hackers* sírios que, em 2013, penetraram na conta de *Twitter* da agência noticiosa *Associated Press*, publicando uma notícia falsa sobre uma

[34] *Russia, Trump, and the 2016 U.S. Election*. MASTERS, Jonathan. 2018. Council on Foreign Relations. 26 de Fevereiro de 2018. Acedido a 10 de Setembro de 2018, em https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.

[35] *The rise of the cyber-mercenaries*. ZILBER, Neri. 2018. Foreign Policy. 31 de Agosto de 2018. Acedido a 10 de Setembro de 2018, em https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/.

explosão na Casa Branca que teria ferido o então Presidente Obama. A notícia foi prontamente desmentida, mas não deixou de causar uma situação de pânico nos mercados financeiros, tendo provocado perdas estimadas em cerca de US$136 mil milhões nas bolsas[36]. Este tipo de ataques tem vindo a causar alguma apreensão pelo facto de ser dificilmente detetável e a sua autoria dispersa nos meios cibernéticos, sendo que as consequências, nas circunstâncias referidas, podem ser consideravelmente danosas para a sociedade, a economia e a ordem financeira global[37].

- **Pressão económica**

À semelhança de outras ameaças híbridas, o exercício de pressão económica sobre países ou organizações públicas ou empresariais constitui um instrumento também já bem conhecido, sobretudo no mundo Ocidental, existindo sob diversas formas, sendo de recordar, neste contexto, os recentes casos das sanções internacionais contra o Irão[38] e a Rússia[39], que visaram os interesses económicos daqueles países, em consequência da violação das regras do Direito Internacional.

A pressão económica verifica-se também noutras circunstâncias, podendo consubstanciar-se, entre outros: i) na concessão de empréstimos de um país a outro para criar um ascendente financeiro; ii) na celebração de acordos de venda de matérias-primas energéticas ou agrícolas a preços inferiores aos praticados nos mercados internacionais para granjear apoios políticos na esfera internacional; iii) na proibição de venda de matérias-primas estratégicas, nomeadamente energéticas, agrícolas ou minerais, para condicionar o posicionamento político internacional de países dependentes daqueles fornecimentos; e iv) no aumento considerável dos preços de matérias-primas, também

[36] *'Bogus' AP tweet about explosion at the White House wipes billions off US markets*. FOSTER, Peter. 2013. The Telegraph. 23 de Abril de 2013. Acedido a 10 de Setembro de 2018, em https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.

[37] TREVERTON, Gregory F., et al.. *Addressing Hybrid Threats*…, cit., pp. 50 a 51.

[38] *International Sanctions on Iran*. LAUB, Zachary. 2015. 15 de Julho de 2015, Council on Foreign Relations. Acedido a 10 de Setembro de 2018, em https://www.cfr.org/backgrounder/international-sanctions-iran.

[39] *This time, sanctions on Russia are having the desired effect*. KEATINGE, Tom. 2018. 13 de Abril de 2018, Financial Times. Acedido a 10 de Setembro de 2018, em https://www.ft.com/content/cad69cf4-3e40-11e8-bcc8-cebcb81f1f90.

para condicionar o posicionamento político internacional de países dependentes daqueles fornecimentos.

A título de exemplo, refira-se o caso da venda de gás russo à Ucrânia, que tem vindo a ser recorrentemente utilizada por Moscovo, mediante a prática de preços abaixo do valor de mercado, como forma de coagir Kiev[40], bem como o caso das sanções económicas da China contra a Coreia do Sul após Seoul ter acordado a instalação de sistemas antimíssil norte-americanos no seu território[41].

Porém, será de salientar que a eficácia da aplicação de sanções económicas ou de outros mecanismos de pressão económica de um país sobre outro dependerá, em grande medida, da vulnerabilidade da economia deste último. Com efeito, no caso da pressão económica russa sobre Kiev, será de salientar a importante dependência dos fornecimentos de gás russo que a Ucrânia apresenta, bem como a sua elevada dependência do tecido empresarial russo na sua economia. Já no caso das sanções económicas chinesas à Coreia do Sul, a sua eficácia resultou do peso que a China representa na economia sul-coreana, constituindo-se como o seu principal parceiro comercial, económico e industrial, sendo também de sublinhar, neste quadro, a assimetria da dimensão da economia sul-coreana face à chinesa.

- **Plataformas alternativas de confronto / *proxies***

As plataformas alternativas de confronto e os *proxies* representam igualmente uma forma de confronto já conhecida, sendo de recordar, a este propósito, os vários casos verificados aquando da Guerra Fria, nomeadamente no caso afegão em que, nos anos 70, a União Soviética e os Estados-Unidos se confrontaram por grupos interpostos[42]. A natureza dos confrontos e a sua concretização pode variar em grande medida, em função

[40] COLLINS, Gabriel. 2017. Russia's Use of the "Energy Weapon" in Europe. Issue brief no. 07.18.17. Rice University's Baker Institute Center for Energy Studies. 07 de Julho de 2017. Acedido a 10 de Setembro de 2018, em https://www.bakerinstitute.org/media/files/files/ac785a2b/BI-Brief-071817-CES_Russia1.pdf.

[41] A Coreia do Sul terá acabado por ceder à pressão económica exercida por Pequim, tendo as sanções aplicadas constrangido o desempenho económico dos grandes grupos empresariais sul-coreanos. *China wins its war against South Korea's US THAAD missile shield – Without firing a shot*. VOLODZKO, David J. 2017. 18 de Novembro de 2017, South China Morning Post. Acedido em 10 de Setembro de 2018, em https://www.scmp.com/week-asia/geopolitics/article/2120452/china-wins-its-war-against-south-koreas-us-thaad-missile.

[42] Encyclopaedia Britannica. *Soviet invasion of Afghanistan*. Encyclopaedia Britannica. Acedido a 10 de Setembro de 2018, em https://www.britannica.com/event/Soviet-invasion-of-Afghanistan.

dos interesses que se encontram em disputa, podendo consubstanciar-se numa competição na área científica, conforme se verificou durante a Guerra Fria, em que os Estados-Unidos e a União Soviética competiam pela conquista do Espaço, podendo consubstanciar-se, também, num conflito armado protagonizado por atores interpostos.

No caso dos conflitos armados, este tipo de ameaças consiste, principalmente, na instrumentalização de tensões e conflitos regionais por potências estrangeiras para a projeção dos seus respetivos interesses e extensão da sua esfera de influência naquele espaço, não raras as vezes, de forma oculta e não assumida, sendo ainda frequente os verdadeiros interesses das potencias estrangeiras não coincidirem com os dos protagonistas efetivos dos confrontos[43].

- **Organizações paramilitares**

O financiamento de grupos paramilitares tem também vindo a constituir-se como um dos instrumentos na panóplia de ameaças híbridas, sendo de referir, em modo de exemplo, o caso dos russos *Night Wolves*, que, sob a forma de um clube de motociclismo, defende ideais extremistas e ultranacionalistas, tendo vindo a ser alegadamente utilizados pelo regime russo para intimidar civis em questões socialmente fracturantes. Este tipo de ameaça, pelo facto de não estar diretamente associado a um Estado dificulta a aplicação do Direito Internacional e do Direito da Guerra, não sendo possível responder de forma legal e legítima com o uso da força armada, nomeadamente no quadro da OTAN[44].

4. Linhas de orientação Estratégica da UE e da OTAN para combater as ameaças híbridas

Conforme acima exposto, e atendendo à natureza das ameaças híbridas, a luta contra este fenómeno afigura-se relativamente complexa, já que é de difícil deteção. Não obstante, e face à evolução do conhecimento sobre as ameaças híbridas no seio da UE e da OTAN, estas duas organizações têm vindo a conciliar os seus esforços para delinear uma estratégia comum para responder a este novo vetor de ameaça.

[43] TREVERTON, Gregory F., et al.. *Addressing Hybrid Threats*…, cit., pp. 58 a 59.
[44] TREVERTON, Gregory F., et al.. *Addressing Hybrid Threats*…, cit., pp. 59.

Assim, será de salientar a estratégia apresentada pela Alta Representante para a União Europeia e os Negócios Estrangeiros e para a Política de Segurança, em conjunto com a Comissão Europeia, no passado dia 13 de Junho de 2018, intitulada "*Joint Communication to the European Parliament, the European Council and the Council: Increasing resilience and bolstering capabilities to address hybrid threats*"[45], na qual se definem as linhas de ação estratégica para combater as ameaças híbridas.

No seu comunicado de imprensa, a Alta Representante declarou o seguinte:

"*In times of new challenges around the world, we are reinforcing our work within the European Union to counter hybrid threats – be it in the field of cyber, on disinformation or counter intelligence. Together with our Member States and partners, such as NATO, we are working to strengthen our capabilities to address these challenges and build up our resilience to chemical, biological, radiological and nuclear-related risks, to effectively protect our citizens.*"

Por um lado, estas palavras evidenciam o importante desafio que se apresenta à UE e aos países da Aliança. Por outro lado, evidenciam que a capacidade de resposta reside essencialmente numa capacidade de resiliência conjunta e numa capacidade de identificação dos fenómenos para prevenir e reagir em conformidade.

Assim, a estratégia apresentada defende que o combate às ameaças híbridas deverá assentar, primordialmente, em quatro pilares, nomeadamente os seguintes:

i) **Consciência situacional**: A UE criou, em 2017, o *Hybrid Fusion Cell*[46], que funciona no âmbito do *EU Intelligence and Situation Centre structure*

[45] Comissão Europeia e Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança. 2018. Joint Communication to the European Parliament, the European Council and the Council: *Increasing resilience and bolstering capabilities to address hybrid threats* JOIN(2018) 16 Final. *European Union External Action - Press and Media - Documents*. [*Online*] 13 de Junho de 2018. Acedido a 23 de Agosto de 2018, em https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf.

[46] Comissão Europeia. 2017. JOINT REPORT TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the Joint Framework on countering hybrid threats - a European Union response JOIN/2017/030 final. Comissão Europeia. [Online] 19 de Julho de 2017. [Citação: 12 de Setembro de 2018.] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0030:FIN.

e do Serviço Europeu de Ação Externa, tendo por missão a recolha, processamento e análise de informações sobre as ameaças híbridas, devendo incluir agora as ameaças Químicas, Biológicas, Radiológicas e Nucleares, a contra-espionagem e as ciberameaças;

ii) Comunicação estratégica: Um dos vetores de potencial sucesso das ameaças híbridas reside na falta de comunicação e no isolamento dos países visados, que, frequentemente, por receio de divulgar as suas vulnerabilidades, não comunicam as ocorrências detetadas. Para remediar a esta situação, a Alta Representante propõe reforçar a comunicação estratégica, sistemática e interativa entre as estruturas da UE, os Estados-Membros e organizações aliadas, como a OTAN;

iii) Reforçar a resiliência e capacidade de contenção no setor da cibersegurança: Para este efeito, a UE tem vindo a envidar esforços no sentido de reforçar a segurança cibernética europeia, nomeadamente com vista à formação e capacitação no domínio dos ciberataques para uma mais célere deteção, tendo, para tal, proposto a criação de um certificado de cibersegurança, o reforço das competências da Agência Europeia para a Cibersegurança[47], um quadro reforçado de cooperação entre Estados-Membros e as agências da UE em caso de ciberataque[48], bem como o conjunto de instrumentos de ciberdiplomacia[49].

iv) Reforço da resiliência perante atividades hostis de espionagem: A UE reconhece, neste domínio, a essencialidade da cooperação e coordenação entre os Estados-Membros e as organizações internacionais, sobretudo com a OTAN, procurando, por esta via, conter as atividades hostis de espionagem contra as instituições europeias, pretendendo, neste quadro,

[47] Comissão Europeia. 2017. *ENISA and a new cybersecurity act. Briefing, EU Legislation in Progress*. Acedido a 12 de Setembro de 2018, em http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf.

[48] Comissão Europeia. 2017. *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises C/2017/6100*. 13 de Setembro de 2017. Acedido a 10 de Setembro de 2018, em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.239.01.0036.01.ENG.

[49] Conselho Europeu. 2017. *Ciberataques: UE pronta a responder com uma série de medidas, incluindo* sanções. 19 de Junho de 2017. Acedido em 10 de Setembro de 2018, em http://www.consilium.europa.eu/pt/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

melhorar a capacidade do *EU Hybrid Fusion Cell* no campo da contraespionagem.

A Alta Representante mencionou também a necessidade de incrementar a preparação e capacidade de resposta da UE perante as ameaças Químicas, Biológicas, Radiológicas e Nuclear, para atender casos como o recente ataque de Salisbury, no Reino Unido, em que um alegado ex-agente dos serviços de informações russo terá sido envenenado com recurso a substâncias químicas, neste caso o agente químico Novichok[50]. Entre as medidas que a Comissão Europeia pretende adotar para combater este tipo de ameaças, cumpre destacar a elaboração de uma lista de substâncias químicas que possam ser utilizadas no contexto mencionado, encetar um diálogo com potenciais fornecedores deste tipo de substâncias para prevenir a sua utilização hostil, melhorar a detecção de ameaças de natureza química, capacitar as forças e serviços de segurança para melhorar a sua capacidade de resposta perante ocorrências semelhantes, bem como elaborar um inventário do armazenamento de medicamentos e tratamentos contra armas químicas para mapear a sua disponibilidade rápida na UE.

Já no que diz respeito à OTAN, cabe destacar que a *Joint Intelligence and Security Division*, instalada na sede da OTAN, em Bruxelas, tem vindo, desde 2015, a desenvolver um trabalho de recolha, processamento e análise de informações sobre ameaças híbrida, visando capacitar aquela Organização perante este novo vetor de ameaças, proporcionando informações aos decisores políticos dos Aliados sobre aquela matéria. Segundo a declaração resultante da Cimeira dos Chefes de Estado e de Governo da OTAN, nos passados dias 11 e 12 de Julho de 2018[51], resultou o reconhecimento de que a responsabilidade principal no combate às ameaças híbridas recai sobre cada Estado,

[50] Recorde-se que Sergei Skripal, ex-agente dos serviços de informações russos, e a sua filha, terão sido alegadamente envenenados por dois agentes dos serviços de informações militares russos, recentemente identificados, recorrendo ao agente nervoso Novichok. *Salisbury novichok suspects say they were only visiting cathedral*. ROTH, Andrew e DODD, Vikram. 2018. The Guardian. 13 de Setembro de 2018. Acedido a 13 de Setembro de 2018, e https://www.theguardian.com/uk-news/2018/sep/13/russian-television-channel-rt-says-it-is-to-air-interview-with-skripal-salisbury-attack-suspects.

[51] OTAN. 2018. Brussels Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018. *OTAN, e-Library, Official texts*. [*Online*] 11 de Julho de 2018. Acedido a 13 de Setembro de 2018, em https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21.

em primeiro lugar (ponto 21.), já que são os principais visados, sobrando à OTAN, um papel de apoio e preparação dos Aliados neste âmbito.

A OTAN disponibiliza assim um conjunto de mecanismos de cooperação e colaboração para aprofundar o conhecimento sobre as ameaças híbridas, gerando *expertise* naquele domínio, apoiando ainda os países da Aliança a: i) preparar respostas eficazes perante acidentes envolvendo armas Químicas, Biológicas, Radiológicas e Nuclear, ii) proteger as infraestruturas críticas, ii) desenvolver uma comunicação estratégica, iii) proteger a população civil, iv) defender a cibersegurança e a segurança energética, bem como v) combater o terrorismo[52]. Este esforço de apoio da OTAN concretiza-se, também, na formação, treino e capacitação dos Estados-Membros para reagir perante ocorrências de ameaças híbridas, incluindo mecanismos de resposta militar e não militar, em cooperação com outras entidades, como a UE.

A Declaração da Cimeira dos Chefes de Estado e de Governo da OTAN de 2018 recorda também que a Aliança se mantém disponível para intervir sempre que for ameaçada a integridade territorial e a segurança de qualquer Aliado, conforme estipulado no artigo 5º do Tratado de Washington, não se excluindo que esta afirmação possa ser interpretada, ainda que de forma extensiva, como a possibilidade de uma ameaça híbrida poder vir a ser considerada uma forma de agressão que possa permitir uma resposta militarizada.

5. Conclusões

Atendendo ao acima exposto, cumpre sublinhar que o conceito de ameaças híbridas ainda se encontra em construção, pese embora o reconhecimento desta nova realidade e uma melhor compreensão deste fenómeno tenham vindo a possibilitar não apenas uma definição concetual cada vez mais precisa, como, também, uma apreensão mais abrangente deste novo vetor de condicionamento securitário.

[52] OTAN. 2018. Brussels Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018. *OTAN, e-Library, Official texts*. [*Online*] 11 de Julho de 2018. Acedido a 13 de Setembro de 2018, em https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21.

Resulta, assim, das páginas anteriores, que as ameaças híbridas se caracterizam por ações coordenadas e sincronizadas que visam deliberadamente afetar as vulnerabilidades dos Estados democráticos e das suas instituições, empregando um leque particularmente amplo de meios políticos, económicos, militares, civis e de informação, combinando atividades convencionais e não-convencionais, militares e não militares, de forma coordenada, levadas a cabo por atores estatais e não-estatais, recorrendo ainda a campanhas multidimensionais que combinam medidas coercivas e subversivas, com vista ao alcance de objetivos políticos.

Por outro lado, os autores das ameaças híbridas tendem a explorar os limiares da deteção e autoria, operando, frequentemente, nas zonas de indefinição da autoria, explorando, também, os limites da paz e da guerra, o que, perante o actual quadro legal internacional, dificulta a aplicação das medidas previstas no Direito Internacional, configurado para situações convencionais, e mina a capacidade de resposta dos países regidos por regimes de Estado de Direito Democrático.

Acresce que as ameaças híbridas visam ainda influenciar o processo de tomada de decisão político e institucional, a nível local, regional ou nacional, procurando, também, afetar os interesses estratégicos dos visados, recorrendo frequentemente à subversão mediática ou outros métodos, como a propaganda, a instrumentalização das redes sociais, dos meios noticiosos estatais ou paraestatais, as *fake news*, as fugas estratégicas de informações, a ciberespionagem ou a pressão económica, entre outros.

Face a sua elevada complexidade e multidimensionalidade, não será de somenos importância concluir este trabalho recordando que, face ao acima exposto, o que distingue as ameaças híbridas das restantes ameaças reside, cumulativamente, na dificuldade da sua identificação e atribuição da autoria, a sua utilização sistemática, coordenada e sincronizada com um amplo leque de acções hostis, cobertas e encobertas, civis, militares e paramilitares, em prol de um objetivo específico, num período indefinido de tensão entre o estado de paz e de guerra. Na eventualidade das características acima mencionadas não se verificarem cumulativamente, dificilmente se poderá considerar estar perante ameaças híbridas, residindo precisamente nesta questão a complexidade do combate às ameaças híbridas, a sua definição concetual e, por conseguinte, a sua identificação, requerendo a sua prevenção e combate um elevado nível de coordenação e cooperação interinstitucional e internacional, nomeadamente no seio da UE e da OTAN.

Referências Bibliográficas

- *1 in 3 news articles shared about Sweden election are fake, finds study.* **CUDDY, Alice. 2018.** 06 de Setembro de 2018, Euronews.
- **ALBRIGHT, Madeleine e VAN DERR VEER, Jeroen et al. 2010.** *NATO 2020: assured security; dynamic engagement - Analysis and recommendations of the group of experts on a new strategic concept for NATO.* NATO Public Diplomacy Division. Bruxelas, 2010. Documento elaborado com vista à preparação da Cimeira da OTAN de Lisboa, em 2010, e à revisão do Conceito Estratégico da OTAN.
- **ANDERSSON, Jan J. e TARDY, Thierry . 2015.** *Hybrid: what's in a name?* European Union Institute for Security Studies, Outubro de 2015. ISSUE Briefs, Vol. 32. ISSN 2315-1110.
- *'Bogus' AP tweet about explosion at the White House wipes billions off US markets.* **FOSTER, Peter. 2013.** 23 de Abril de 2013, The Telegraph.
- *China wins its war against South Korea's US THAAD missile shield – Without firing a shot.* **VOLODZKO, David J. 2017.** 18 de Novembro de 2017, South China Morning Post.
- **COLLINS, Gabriel. 2017.** Russia's Use of the "Energy Weapon" in Europe. *Issue brief no. 07.18.17. Rice University's Baker Institute Center for Energy Studies.* 07 de Julho de 2017.
- **Comissão Europeia. 2016.** *Comunicação conjunta ao Parlamento Europeu e ao Conselho, Quadro comum em matéria de luta contra as ameaças híbridas, Uma resposta da União Europeia JOIN(2016) 18 final.* Bruxelas, 06 de Abril de 2016.
- **Comissão Europeia e Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança. 2018.** Joint Communication to the European Parliament, the European Council and the Council: Increasing resilience and bolstering capabilities to address hybrid threats JOIN(2018) 16 Final. *European Union External Action - Press and Media - Documents.* [*Online*] 13 de Junho de 2018. Acedido a 23 de Agosto de 2018, em https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf.

- **Comissão Europeia. 2017.** JOINT REPORT TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the Joint Framework on countering hybrid threats - a European Union response JOIN/2017/030 final. *Comissão Europeia.* [*Online*] 19 de Julho de 2017. Acedido a 12 de Setembro de 2018, em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0030:FIN.
- **2016.** *Common set of proposals for the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization.* 06 de Dezembro de 2016.
- **Encyclopaedia Britannica.** Soviet invasion of Afghanistan. *Encyclopaedia Britannica.* [*Online*] Acedido a 10 de Setembro de 2018, em https://www.britannica.com/event/Soviet-invasion-of-Afghanistan.
- **European Centre of Excellence for Countering Hybrid Threats.** About us. *European Centre of Excellence for Countering Hybrid Threats.* [*Online*] Acedido em 5 de Setembro de 2018, em https://www.hybridcoe.fi/about-us/.
- **—.** Hybrid Threats. *European Centre of Excellence for Countering Hybrid Threats.* [*Online*] Acedido a 05 de Setembro de 2018, em https://www.hybridcoe.fi/hybrid-threats/.
- **FISH S., Isaac. 2016.** Beijing Establishes a D.C. Think Tank, and No One Notices. *Foreign Policy.* 07 de Julho de 2016.
- *How Russian networks worked to boost the far right in Italy.* **ALANDETE, David e VERDÚ, Daniel. 2018.** 01 de Março de 2018, El País.
- *International Sanctions on Iran.* **LAUB, Zachary. 2015.** 15 de Julho de 2015, Council on Foreign Relations.
- **NEMETH, William J. 2002.** Future war and Chechnya: a case for hybrid warfare. Monterey, California, EUA, Junho de 2002. Tese de mestrado no âmbito do Programa de Mestrado em Assuntos de Segurança Nacional da Naval Postgraduate School de Monterrey, California (EUA).
- *Os emails de Macron podem ser inofensivos, mas este jogo chama-se "suspeita".* **2017.** Lisboa, 06 de Maio de 2017, Público.
- **OTAN. 2015.** *Statement by NATO Defence Ministers.* Bruxelas, 25 de Junho de 2015.

- **—. 2014.** Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. *NATO, e-Library, Official texts.* [*Online*] 05 de Setembro de 2014. Acedido a 26 de Agosto de 2018, em https://www.nato.int/cps/en/natohq/official_texts_112964.htm.
- **—. 2016.** Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. *OTAN, e-Library, Official texts.* [*Online*] 09 de Julho de 2016. Acedido a 29 de Agosto de 2018, em https://www.nato.int/cps/ic/natohq/official_texts_133169.htm.
- *Quels sont les liens troubles entre le Front national et le Kremlin?* **HADDAD, Marie-Pierre. 2018.** 14 de Março de 2018, RTL.
- *Russia, Trump, and the 2016 U.S. Election.* **MASTERS, Jonathan. 2018.** 26 de Fevereiro de 2018, Council on Foreign Relations.
- *Russian Money Suspected Behind Fracking Protests.* **HIGGINS, Andrew. 2014.** 30 de Novembro de 2014, The New York Times.
- *The rise of the cyber-mercenaries.* **ZILBER, Neri. 2018.** 31 de Agosto de 2018, Foreign Policy.
- *This time, sanctions on Russia are having the desired effect.* **KEATINGE, Tom. 2018.** 13 de Abril de 2018, Financial Times.
- **TREVERTON, Gregory F., et al. 2018.** *Addressing Hybrid Threats.* Swedish Defence University. Estocolmo, 2018. ISBN 978-91-86137-73-1.
- **VAN PUYVELDE, Damien. 2015.** Hybrid war – does it even exist? *NATO Review Magazine.* [*Online*] 07 de Maio de 2015. Acedido a 24 de Agosto de 2018, em https://www.nato.int/docu/review/2015/also-in-2015/hybrid-modern-future-warfare-russia-ukraine/en/index.htm.