

TERRORISMO E VIOLÊNCIA POLÍTICA

GEORGE JOFFÉ TRANSNATIONAL TERRORISM REGENERATED SOFIA DE VASCONCELOS
CASIMIRO LIBERDADE E SEGURANÇA NO COMBATE AO TERRORISMO: *QUIS CUSTODIET
IPSOS CUSTODES?* UMA PERSPETIVA JURÍDICA JÚLIO PEREIRA VIGILÂNCIA VÍDEO,
INTERCEÇÃO PREVENTIVA DE COMUNICAÇÕES E CONTRATERRORISMO HUGO FRANCO
TERRORISMO E PROPAGANDA NOS *MEDIA* PAULO MONIZ TERRORISMO E VIOLÊNCIA
POLÍTICA: COMO COMBATER O CIBERTERRORISMO E A RADICALIZAÇÃO LUÍS ELIAS O
TERRORISMO TRANSNACIONAL CONTEMPORÂNEO: SEGURANÇA, JUSTIÇA E COOPERAÇÃO

TERRORISMO E VIOLÊNCIA POLÍTICA

GEORGE JOFFÉ TRANSNATIONAL TERRORISM REGENERATED SOFIA DE VASCONCELOS
CASIMIRO LIBERDADE E SEGURANÇA NO COMBATE AO TERRORISMO: *QUIS CUSTODIET
IPSOS CUSTODES?* UMA PERSPETIVA JURÍDICA JÚLIO PEREIRA VIGILÂNCIA VÍDEO,
INTERCEÇÃO PREVENTIVA DE COMUNICAÇÕES E CONTRATERRORISMO HUGO FRANCO
TERRORISMO E PROPAGANDA NOS *MEDIA* PAULO MONIZ TERRORISMO E VIOLÊNCIA
POLÍTICA: COMO COMBATER O CIBERTERRORISMO E A RADICALIZAÇÃO LÚÍS ELIAS O
TERRORISMO TRANSNACIONAL CONTEMPORÂNEO: SEGURANÇA, JUSTIÇA E COOPERAÇÃO

NAÇÃO E DEFESA

Revista Quadrimestral – P.V.P. 8,50 €

Diretor

Vitor Rodrigues Viana

Editor

Luís Cunha

Conselho Editorial

Ana Santos Pinto, António Horta Fernandes, António Paulo Duarte, António Silva Ribeiro, Armando Serra Marques Guedes, Bruno Cardoso Reis, Carlos Branco, Carlos Mendes Dias, Daniel Pinéu, Francisco Proença Garcia, Isabel Ferreira Nunes, João Leal, João Vieira Borges, José Luís Pinto Ramalho, José Manuel Freire Nogueira, Luís Leitão Tomé, Luís Moita, Manuel Ennes Ferreira, Maria do Céu Pinto, Maria Helena Carreiras, Mendo Castro Henriques, Miguel Monjardino, Nuno Brito, Paulo Jorge Canelas de Castro, Paulo Viegas Nunes, Raquel Freire, Rui Mora de Oliveira, Sandra Balão, Teresa Vicente Rodrigues, Vasco Rato, Victor Marques dos Santos, Vitor Rodrigues Viana.

Conselho Consultivo

Abel Cabral Couto, António Martins da Cruz, António Vitorino, Carlos Gaspar, Diogo Freitas do Amaral, Fernando Carvalho Rodrigues, Fernando Reino, João Salgueiro, Joaquim Aguiar, José Manuel Durão Barroso, Luís Valença Pinto, Luís Veiga da Cunha, Manuel Braga da Cruz, Maria Carrilho, Nuno Severiano Teixeira, Pelágio Castelo Branco.

Conselho Consultivo Internacional

Bertrand Badie, Christopher Dandeker, Christopher Hill, George Modelski, Josef Joffe, Jurgen Brauer, Ken Booth, Lawrence Freedman, Robert Kennedy, Todd Sandler.

Antigos Coordenadores Editoriais

1983/1991 – Amadeu Silva Carvalho. 1992/1996 – Artur Baptista dos Santos. 1997/1999 – Nuno Mira Vaz. 2000/2002 – Isabel Ferreira Nunes. 2003/2006 – António Horta Fernandes. 2006/2008 – Isabel Ferreira Nunes. 2009/2010 – João Vieira Borges. 2011/2018 – Alexandre Carriço.

Núcleo de Edições

António Baranita

Colaboração

Lúisa Nunes

Capa

Nuno Fonseca/nfdesign

Normas de Colaboração e Assinaturas

Consultar final da revista

Propriedade e Edição

Instituto da Defesa Nacional

Calçada das Necessidades, 5, 1399-017 Lisboa

Tel.: 21 392 46 00

Fax.: 21 392 46 58

E-mail: idn.publicacoes@defesa.pt

www.idn.gov.pt

Composição, Impressão e Distribuição

Pentaedro, Lda.

Praceta da República, 13 • 2620-162 Póvoa de Santo Adrião – Portugal

Tel.: 218 494 141/43

Fax.: 218 492 061

E-mail: pentaedro@mail.telepac.pt

ISSN 0870-757X Publicação Electrónica ISSN 2183-9662

Depósito Legal 54 801/92

Tiragem 750 exemplares

Anotado na ERC

Registada na Latindex – Sistema Regional de Informação em Linha para Revistas Científicas da América Latina, Caraíbas, Espanha; MIAR, RedAlyC e JSTOR.

Disponível no RCAAP – Repositório Científico de Acesso Aberto de Portugal

O conteúdo dos artigos é da inteira responsabilidade dos autores

Editorial	5
Terrorismo e Violência Política	
Transnational Terrorism Regenerated <i>George Joffé</i>	8
Liberdade e Segurança no Combate ao Terrorismo: <i>Quis Custodiet Ipsos Custodes? Uma Perspetiva Jurídica</i> <i>Sofia de Vasconcelos Casimiro</i>	23
Vigilância Vídeo, Interceção Preventiva de Comunicações e Contraterrorismo <i>Júlio Pereira</i>	39
Terrorismo e Propaganda nos <i>Media</i> <i>Hugo Franco</i>	48
Terrorismo e Violência Política: Como Combater o Ciberterrorismo e a Radicalização <i>Paulo Moniz</i>	58
O Terrorismo Transnacional Contemporâneo: Segurança, Justiça e Cooperação <i>Luís Elias</i>	78
Extra Dossiê	
Uma Nova Visão da Sustentabilidade da Marinha de Duplo-Uso <i>Teresa Vicente Rodrigues</i>	114
O Conceito de Emprego das Forças Armadas em Matérias de Segurança Interna <i>Nuno Imperial</i>	137

Este número da revista *Nação e Defesa* tem por base os textos elaborados pelos conferencistas convidados para o seminário internacional “Terrorismo e Violência Política”, organizado pelo Instituto da Defesa Nacional entre janeiro e outubro de 2018.

Trata-se de revisitar, atualizando, um tema já abordado em edições anteriores da *Nação e Defesa*, números 143 e 148, novamente pela mão de conhecidos especialistas nacionais e estrangeiros.

O terrorismo – do Latim *terrere* ou “assustar, causar medo” – é um conceito de difícil conceptualização. Historicamente apresenta-se como um fenómeno complexo e de grande abrangência, tendo vindo a sofrer uma evolução interpretativa condicionada por conjunturas ideológicas. Um estudo especializado referido na obra *História do Terrorismo* (eds. Gérard Chaliand e Arnaud Blin) contabiliza 108 formulações distintas para o conceito de “terrorismo”, o que diz bem da polissemia reinante para as derivações do vocábulo.

O terrorismo não é um fenómeno novo. O que muda são os objetivos, métodos e meios utilizados e, nesse sentido, o seu impacto estratégico. O terrorismo transnacional, que os atentados perpetrados nos últimos anos voltaram a evidenciar, ilustra bem esta mudança. O objetivo é provocar alterações no quadro de valores e no modo de vida das sociedades democráticas e fomentar o terror e o medo, através da violência em larga escala e potencial capacidade de atuação a nível global.

Nenhum país está, portanto, imune a esta ameaça e a sua prevenção e combate exige cooperação internacional reforçada, serviços de informações eficazes e o emprego de estratégias integradas por parte dos Estados e das organizações internacionais.

É esse novo enquadramento, legal, político, securitário e até psicológico, no âmbito do combate a um fenómeno mutável, mas perene, que os colaboradores desta edição da *Nação e Defesa* abordam nas suas análises especializadas.

O conjunto de textos abre com o artigo assinado por George Joffé, abordando as táticas e estratégias levadas a efeito na ofensiva contraterrorista, que resultaram na desocupação territorial do Daesh.

Sofia de Vasconcelos Casimiro dá-nos uma reflexão sobre os desafios do combate ao terrorismo num Estado de Direito. Como salienta, um dos principais desafios do combate ao terrorismo consiste em ser eficaz sem colocar em causa os princípios que sustentam o próprio Estado de Direito.

Numa visão complementar, Júlio Pereira aborda a importância da videovigilância e intervenção preventiva de comunicações no prosseguimento da estratégia nacional de combate ao terrorismo. Deixando claro que o problema da videovigilância é sempre o do equilíbrio entre o valor da segurança e o respeito pelos direitos constitucionais, o autor não deixa de frisar que a segurança, não sendo o direito mais importante, é o palco onde se exercem todos os outros direitos.

Hugo Franco escreve sobre as novas formas de propaganda do grupo jihadista Daesh e o respetivo impacto nos *media*. Evocando casos concretos, coloca em causa a gestão – ética deontológica e profissional –, da ofensiva terrorista na comunicação social ocidental. Conclui que a falta de organização nos *media* contribuiu, de algum modo, para a projeção do autodenominado Estado Islâmico.

Por seu turno, Paulo Moniz avança com uma análise tendente à compreensão dos fenómenos de radicalização, terrorismo e violência política no contexto do ciberespaço, propondo estratégias de atuação para o seu combate.

Por último, Luís Elias debruça-se sobre o papel das Forças e Serviços de Segurança, Serviços de Informações, Forças Armadas e Justiça – a par das universidades e *think tanks* – na resposta multidisciplinar ao terrorismo.

Com a oportuna contribuição destes peritos, a *Nação e Defesa* proporciona aos seus leitores uma visão panorâmica, qualificada e heterogénea, sobre o fenómeno do terrorismo nas suas múltiplas dimensões.

Vítor Rodrigues Viana

Terrorismo e Violência Política

Transnational Terrorism Regenerated

George Joffé

University of Cambridge. Research Fellow and Visiting Professor of Geography at Kings College, London University. Specialist in the Middle East and North Africa. Currently engaged in a project studying connections between migrant communities and trans/national violence in Europe.

Abstract

Now that Da'ish's territorial construct has been dismantled, a new version of violent Islamic extremism is confidently predicted. Its form and ideological content is, as yet, undefined but the fact that it will emerge is considered inevitable as extremism follows what is assumed to be a linear progression into becoming the basic challenge facing the hegemonic secular political order, whether liberal or autocratic in nature. This comment is intended to question this conclusion by suggesting that extremism of this kind may be ideologically static or even in regression as it fragments and begins to confront mirror-images of itself that also operate outside the confines of the formal state. It is a fragmentation that has also been accelerated by the sustained anti-terrorist containment tactics of the West which have cut into its efficacy in terms of ideological regeneration and territorial control. Western tactical and strategic mistakes, however, have given it the means to postpone its ultimate defeat and, even, to recuperate from much of its past losses.

Resumo

Terrorismo Transnacional Regenerado

Agora que a construção territorial do Da'ish foi desmantelada, pode prever-se uma nova versão do extremismo islâmico violento. O autor coloca em causa as táticas sustentadas de contenção antiterrorista do Ocidente. Os erros táticos e estratégicos ocidentais têm adiado a derrota final do Da'ish.

By the end of 2017, the territorial reification of the *Islamic State* (ISIS, *Da'ish*) – its ‘caliphate’ in Syria and Iraq, with outliers in Sinai, Libya and latterly Afghanistan – seemed to have become little more than a palimpsest of ungoverned space awaiting the reappearance of a state to be etched out upon its surface. Most commentators appeared to believe that *Da'ish* itself would transmute into a new type of structure and emerge yet again, phoenix-like, from its ashes as it had seven years before after American and Iraqi forces had dismembered it inside Iraq (Joffé, 2016a, p. 7). The ‘virtual caliphate’ that they anticipated would replace it was also expected to develop new ideological forms by which to justify its actions. Just as *al-Qa'ida* had sidelined its objective of confronting the ‘far enemy’¹ and replaced it by the new aim of ‘good governance’ as it entrenched itself in Yemen and Libya, so *Da'ish v.2*, as it came to be known, was expected to adopt new strategies and tactics as it adjusted to the loss of its embryonic universal state.

A year later, however, this did not appear to have happened. Instead the movement had regressed back to the pattern of sporadic attacks within the confines of the states in which it remained and where it now fragmented into isolated but still-active groups. Its targets remained the same – the institutions of the state, whether security forces or administrations, if they existed; antagonistic militias and violent competitors if they did not; individuals who actively opposed it and religious competitors (the Shi'a in particular) even if they did not challenge it. Nor had its essential ideology changed, beyond the fact of its territorial loss with the resulting irrelevance of the administrative and extractive infrastructure it had created. It still irrationally believed in a rigid application in the most brutal way of its salafi-jihadi vision and in the need to destroy the ‘gray zone’, that arena of social interaction between Muslim and non-Muslim populations which was to be replaced by antagonistic and agonistic separation.²

Of course, this may yet change but there is no evidence that this will be the case. Beyond this, too, despite the fragmentation of *Da'ish*, the core of its leadership still remained. Its putative caliph, Abu Bakr al-Baghdadi, still seemed to hold on to its nominal leadership, albeit concealed in the ungoverned spaces along the Syrian-Iraqi border.³ Its rank-and-file, too, particularly its foreign fighters, seemed largely undiminished in their enthusiasm for the movement wherever they had not been dispersed, killed or detained. In Europe, as well, its acolytes turned back to the practice of ‘leaderless jihad’ – self-motivated extremism against the wider popula-

-
- 1 The non-Muslim Western states that were perceived to support and tolerate the repressive autocracies of the Middle East and North Africa in order to preserve regional stability, regardless of the consequences for the populations concerned or for their cultural and religious values.
 - 2 In terms of Adorno’s ‘theodicity of conflict’ in the critical sense that it is irreconcilable with majority sentiment and society which it must, therefore, seek to destroy (Adorno, 1951, p. 52).
 - 3 There have recently been reports that he, together with most of the remaining core of *Da'ish*, has fled to the tribal areas of Pakistan along the Afghan-Pakistan border (Anon., 2018a).
-

tion, as encouraged by as-Suri in his study, *The global Islamic resistance call* (Lia, 2008). Their ostensible purpose was to cause antagonism and hatred between its Muslim and non-Muslim communities or simply to estrange host communities from engagement with the wider Muslim world preparatory to aggressively confronting them with its aim of ultimate victory.⁴ Da'ish had become, in short, the archetypal chiliastic movement it always ultimately sought to be, despite its loss of control over the physical reality of Dabiq and the territorial caliphate.⁵

Alternative Agendas

Quite apart from any regression or reversion to type within Da'ish's strategy as a result of the destruction of its territorial caliphate, there have been other directions in which the extremist salafi-jihadi agenda has evolved. Ironically enough, the non-Muslim world has become habituated to extremist violence and therefore tends to ignore the day-to-day reality of its existence unless its gratuitous brutality becomes impossible to overlook – one of the main reasons, apart from its success at recruiting foreigners to fight in its ranks and its staggering initial success in confronting the Iraqi and Syrian states, that Da'ish had attracted so much attention in the West. Another irony appears to be that part of its membership relocated to Afghanistan and Pakistan, allegedly having enjoyed safe passage through Iran to do so; a trajectory originally followed by its founder, Abu Musab al-Zarqawi, in 1999 and a further irony because of his detestation of Shi'a Islam, a sentiment subsequently adopted by the organisation he created, *al-Qa'ida fi'l-Iraq* (Joffé, 2016a, p. 6). It is a sentiment typical of the wider salafi movement, too, but adopted with particular vehemence by Da'ish.

The third irony, however, is that as Da'ish appears to have regressed in terms of media prominence and ideological innovation in recent years, it has been al-Qa'ida and the other organisations claiming affiliation to it that have progressed. The irony here is that, shortly after the emergence of Da'ish, the movement tried to assert its leadership of the global jihadi movement against al-Qaida on the grounds that leadership should be the prerogative of those directly engaged in the struggle, not of those isolated in the mountain fastnesses of Afghanistan or tribal Pakistan and

4 See Lia (2008, pp. 102, 313-316 and 347-484) and Naji (2006). Naji's major vision, as expressed in *The Administration of Savagery*, is discussed in Brachman (2009, pp. 94-95) and in Ryan (2013, pp. 148 and 168-178). It should be noted that the original book is also sometimes entitled *The Management of Savagery*. See also Kaplan (2008) for a description of what Da'ish has become: "Chiliastic in nature, deeply religious with eclectic or syncretic religious tropes assembled and interpreted by the leaders in support of a millenarian dream to be realized through a campaign of apocalyptic violence". Cited in George Joffé (2017, p. 12).

5 Dabiq is the town in Northern Syria where the final millennial battle between Islam triumphant and its non-Muslim opponents would be fought out that would mark the advent of 'the end of time' – al-Qaymah, the Day of Judgement.

thus removed from the field of action (Joffé, 2016b, pp. 807-808). It has continued to maintain this position, particularly through its project for the caliphate in Syria and Iraq until it was forced out of Mosul and Raqqa (Maher, 2018, pp. 10-12). Yet, in reality, it has been al-Qa'ida which had adapted its agenda to changed circumstances in ways that Da'ish apparently could not.

There have been several reasons for Al-Qa'ida's new-found flexibility and Da'ish's doctrinal and organisational rigidity. Firstly, al-Qa'ida had become a brand, rather than a unitary organisation, to which other autonomous groups sought affiliation, being prepared to accept shared ideology, strategy and tactics, and it also expanded its ideological horizon as well, moving away from its original concern solely with confronting the 'far enemy' – non-Muslim states supporting corrupt regimes in the Muslim world which it considered degenerate – 'jahili' (Gerges, 2005, pp. 44-49). Thus the remnants of the extremist groups which had participated in the Algerian civil war between 1992 and 1999, which had moved from Kabylia and the surrounding regions along Algeria's Mediterranean coast into the Sahara and the Sahel after 2003, rebranded themselves as *Tanzim al-Qa'ida fi'l-Bilad al-Maghribi al-Islami* (al-Qa'ida in the Islamic Maghrib – AQIM) with al-Qa'ida's explicit agreement in 2006. Secondly, networks have now begun to emerge, tying such affiliated groups together. Thus AQIM has proliferated into at least three, if not four related groups; AQIM itself continues but now as a predominantly Algerian group still linked its origins in Kabylia. Alongside it, *Mujao* (*Jamā'at at-tawhīd wa'l-jihād fi'l-gharb al-'afrīqīyā; Mouvement pour l'unicité et le jihad en Afrique de l'Ouest*) emerged in 2011 as a predominantly Sahelian group primarily led by Mauritians seeking its ideological inspiration from African, rather than Arab, religious leaders such as Usman Dan Fodio, an eighteenth century jihadi leader from Northern Nigeria. In 2013, one of its factions merged with a dissident AQIM group, led by Mokhtar Belmokhtar called *Al-Mulathamīn* to create *Al-Mourabitoun*, a group avowedly loyal to al-Qa'ida (Counter Extremism Project, 2018). It has even been prepared to embrace other similar groups elsewhere in Africa as its loose links with *Boko Haram* in Northern Nigeria, in the Lake Chad region and in Cameroon attest.

In addition, al-Qa'ida was prepared to accommodate, even collaborate, with other similar groups; something which Da'ish would not consider under any circumstances, unless the group concerned espoused its doctrines and leadership in all respects, as was to be the case in November 2014 with *Ansar al-Bayt Maqdis* in Sinai, now renamed as *Ad-Dawla al-Islamiyya fi'l-Iraq wa'sh-Sham: Wilayat Sinai* (Kirkpatrick, 2014). AQIM, on the other hand is a very good example of this alternative approach adopted by al-Qa'ida-affiliated groups, for it sought affiliation with al-Qa'ida as early as 2003, an affiliation which was accepted by the parent organisation three years later. Al-Qa'ida's relationship with the *Nusra Front* in Syria, now renamed *Jabhat Fatah ash-Sham*, is another, for the Nusra Front was originally derived from the Iraqi-based movement that was to become Da'ish after the Syrian

civil war broke out. However, it rejected Da'ish's demand that Al-Qa'ida recognise its leadership, remaining faithful to Usama bin Ladin's original movement instead, even at the cost of a rupture with its own parent organisation (Maher, 2018, pp. 10-12). The original al-Qa'ida movement has also re-forged links with extremist groups in South East Asia, such as *Jemaah Islamiyyah* in Indonesia and similar groups in Mindanao in the Philippines (Singh, 1917, pp. 5-8). It has also reached out to similar groups in Africa and Central Asia (Cummings, 2017).

Furthermore, Al-Qa'ida's flexibility is also demonstrated by the way it has allowed its ideology and objectives to change. Its old agendas of confronting the 'far enemy' either through pre-emption, as was the case in Washington and New York in September 2001, or by the kind of direct engagement it practiced in Afghanistan against the Soviet Union between 1980 and the Soviet departure in 1989 or even through 'nomadic jihad', as occurred in Bosnia-Herzegovina or Chechniya in the late 1980s – have evolved in the last decade (Joffé, 2016b, pp. 803-804). *Al-Qa'ida in the Arabian Peninsula (Tanẓīm al-Qā'ida fī'l-Jazīrat al-'Arab)* was able, during the last decade, to develop a new approach, aiming at 'good governance' instead and thereby at ensuring popular support. It has, as a result, been able to spread its influence throughout the Yemeni Hadramaut since 2015 and its success there has been replicated in Western Libya and Tunisia within a new movement adopting similar ideological patterns in the form of *Ansar al-Shar'ia*. Other movements have developed their own agendas – Boko Haram, for example, ostensibly attacking the influence of Western culture to justify its own bestiality towards local populations. Da'ish, on the other hand, has shown no such flexibility in the face of Western attacks upon it. It has, instead, merely undergone a tactical evolution, forced upon it by its loss of territorial control and its organisational fragmentation.

Western Responses

Yet Da'ish remains the primary target and concern of the Western response.⁶ Indeed, that response to the terrorism of recent decades is also an aspect of the problem, for it has not only been a response but also a progenitor of extremist violence itself. Its primary response, certainly since September 11, 2001, has been the so-called 'war on terror', an American-inspired initiative bringing together a loose alliance of Western states against the manifestation of extremist violence arising primarily in the Middle East. The alliance has been committed to using a spectrum of responses against such violence, dominated by military force as its dominant principle in five major geographic arenas – Afghanistan, Iraq, Syria, Yemen and Somalia together with Mali and the Sahel since 2011 – supplemented by initiatives designed to undermine the financial viability and social cohesion of the movements involved.

6 Viz. United Nations Security Council (2018).

It has been an extremely costly undertaking which, by 2020 is expected to have cost its major members – predominantly the United States – between \$1.8 trillion and \$5.5 trillion (Trotta, 2011).⁷ It has also involved significant loss of life: an estimated 65,800-to-88,600 extremists worldwide up to the end of 2015 as the result of military action, together with 7,008 American military deaths and a further more than 3,000 civilian deaths (Anon., 2015). Overall civilian deaths in Western states and in the five principle arenas of military activity have been variously estimated to have been between 480,000 and 507,000 (Anon., 2018b) and 1.3 million-to-2 million.⁸

The problem is that, quite apart from the massive costs involved in terms of wealth and loss-of-life, there have been other losses that raise serious questions about the efficacy of the initiative introduced by the George W. Bush administration after the horrific attacks on New York and Washington in September 2001. Accompanying legal measures, such as the Patriot Act in the United States and terrorist legislation in most Western countries have resulted in abuse of human rights and a reduction of civil liberties, thus undermining the very principles for which the ‘war on terror’ was supposed to be the defensive bulwark. Perhaps the most egregious examples of this have been the CIA’s ‘special rendition’ programme and the extra-legal detention of terrorist suspects in the prison created at Guantanamo Bay and elsewhere – outside the reach of the American legal system.

More sinister, perhaps, has been the gradual shredding of civil rights of assembly and expression for the populations concerned within Europe and the United States, despite the arguments of the governments concerned that they are endeavouring to achieve the reverse outcome. And even worse has been the intellectual acceptance and unconscious incorporation of these developments on the grounds of necessity and intellectual co-option within the West. Popular protest at their curtailment has been gradually replaced by a tacit acceptance, even on occasion active endorsement, of the necessity to restrict them by elites and populace alike. This has been reflected in the conventional media-induced hysteria over the threat of extremism to the Western ideal which is increasingly reflected in social media as well. It has been partnered by the growing neglect of responses to extremism based on the rule-of-law and the definition of extremism in terms of its criminal dimensions, rather than as a hard security threat, equivalent to war.⁹

7 The estimates are derived from two sources, as shown below:

	Congress	Brown
Financial year 2001-2011	1,283.2	2,662.1-3,057.3
Financial year 2012-2020	454.1	2,043.1-2,388.1
Total	1,737.3	4,705.2-5,445.4

Congress: United States Congressional Research Service.

Brown: Watson Institute, Brown University, United States.

8 This is an estimate made by three humanitarian groups: *International Physicians for the prevention of Nuclear War*, *Physicians for Social Responsibility* and *Physicians for Global Survival* (Wilkins, 2015).

9 See Chouet (2008).

The greatest irony, though, is the fact that the development of such attitudes perfectly mirrors the objective of destroying the 'Grey Zone' sought by Da'ish and its intellectual progenitors (see footnote [2] above)! This is manifest in the growing clamour against immigration in both Europe and the United States, albeit for different reasons in each case. Parallel to this has been the generalisation of Islamophobia within Western societies and the demand for the revival of the supposedly social and ethnic homogeneity of an idealised – and, thus, defunct – society of an imagined past. These sentiments are exacerbated by the economic victimisation of large sections of Western societies caused by neo-liberal economic globalisation. It also lies behind the growing populist objection in Europe to the inclusion of Turkey within the Union – a project that was seen as central to its growth a decade ago. This complex array of factors is, ironically enough, manifest in such apparently unrelated phenomena as Britain's crisis over membership of the European Union and its growing popular endorsement of Islamophobia and thus, by implication, of Da'ish's agenda as well.

Da'ish's objective in this respect, after all, has been disaggregate Muslim and non-Muslim populations by intensifying their mutual hatreds through exemplary violence, whether this was achieved through 'lone-wolf' attacks or by planned extremism against Western states or populations. In this respect, of course, it mirrored the original objectives of al-Qa'ida and its associates as well but differed from them in both believing that it should direct such a struggle, not al-Qa'ida, and in refusing to alter its techniques and objectives in the face of the Western onslaught against it. Nor, apparently, does it intend to do so now, despite the loss of its territorial desideratum, the caliphate. The irony, then, resides in the fact that such an unchanged strategy which should have led to its oblivion has, through the 'war in terror'¹⁰, led to its revitalisation because of the unconscious cultural consequences which the alleged war has induced, both in re-legitimising Da'ish's strategy and tactics and in reinforcing the antiphonal antagonism that both sides in this 'war' now manifest.

In the popular and media imaginary, the 'war on terror' has, in effect, appropriated Samuel Huntington's vision of future war as cultural and civilisational in nature, rather than, as in the past, being based in state security and national interest (Huntington, 1993). The consequence is that Islam itself is now popularly seen as intrinsically responsible for contemporary extremist violence – whether those

10 Although the label was abandoned by the Obama Administration in 2009, being replaced by the more anodyne term 'Overseas Contingency Operation', the objectives and techniques did not significantly change except insofar as the use of targeted drone warfare and aerial warfare replaced the use of main, land-based force. The British government had abandoned the use of the term two years earlier since, as Eliza Manningham-Buller, the former head of MI5, pointed out in 2011, it under-valued the criminal nature of the extremism it was supposed to counter by dignifying it as a 'war' (Norton-Taylor, 2011). Other critics have pointed out that extremism is a tactic of struggle, not a conventional hard security entity equivalent to a state which could therefore engage in a formal war.

involved are Muslim or not! This, of course, naturally feeds into the dominant Western popular narrative of identity politics and populism as Europe and America come to rely on the vision of the West as the domain of a Judeo-Christian cultural tradition and thus reify a traditional Christian-Muslim confrontation (Malik, 2011). It is, however, a far cry from the European (and American) self-image as the repository of Enlightenment values of liberalism and democracy, a discrepancy which, if not evident to the West, is certainly clear to the wider non-Western world. However, in a further irony, that experience is also reflected in Da'ish's paradigm of the contemporary caliphate rooted, as it is in practice, in violence towards non-Muslim minorities, rather than in an inclusive rule-of-law.

The reality of such values in practice, in the experience of the Muslim world, has been quite different and has been profoundly and adversely affected by the 'war on terror'. It is a distinction that reflects the difference between timeless synchronic and historically-evolving diachronic appreciations of social reality in the context of contemporary political extremism and of the history of its evolution. For the developing world, the thick substratum of the colonial experience persists as a basis of its understanding of Enlightenment values imposed upon it during and at the end of the colonial period and as constantly renewed in the rhetorical dialogue about development that has persisted thereafter (Bellaigue, 2017; Robinson, 2009). For the Muslim world, in particular, these values, whether welcomed or seen as an oppressive imposition, are nevertheless contrasted with its own cultural and social ideal of a social and political order derived from Islamic principles (Joffé, 2007).

The 'war on terror', then, has had as its primary consequence, a deepening of the distrust and dislike of the principles it is supposed to protect within the cultural domain – the Muslim world, particularly in the Middle East, and Muslim minority communities in Europe – to which it has been predominantly applied. It has also underlined Muslim perceptions of the 'double standards' and hypocrisy that many in the developing world believe to characterise Western policy, in terms, for example, of Western attitudes towards sensitive issues such as Israel and the Palestinian problem, as well as Western rhetoric over governance through popular participation compared with the reality of Western preferences for the illusory stability associated with autocratic governance in the Middle East and North Africa.

In addition, this sense of growing anger in the Muslim world engendered by the seemingly endless struggle encompassed by the 'war on terror' has been reflected in the growth of popular intolerance of Islam inside Europe and the United States. This, of course, has been coupled with the growth of right-wing populism in the Western world, itself in part a consequence of the political failure of neo-liberalism and economic globalisation stimulated by the economic and financial collapse after 2007. But it has also been driven by factors promoted by the 'war on terror', not least by its social and economic costs, and by the cynicism that it has involved. Thus indigenous resentment has been inflamed by the evidence of Western partnership

with obscurantist and corrupt elite elements of the regimes held responsible for indigenous repression. Perhaps the statistics that most starkly reveal this emerged at the end of 2018 in a report published by the Center for Security and International Studies in Washington. Its summary revealed two key points that are germane to the argument being developed here:

- The number of Salafi-jihadists in 2018 declined somewhat from a high in 2016, but is still at near peak levels since 1980. To put this into historical perspective, the high estimate of fighters in 2018 is 270 percent greater than in 2001 when the 9/11 attacks occurred.
- The regions with the largest number of fighters are the Middle East, North Africa, and South Asia. Other regions, such as Southeast Asia, have fewer fighters (Jones *et al.*, 2018).

In other words, the ‘war on terror’ appears to have dramatically worsened global security. There are now estimated to be between 114,500 and 249,500 militant extremists in the five major arenas of activity now, compared with between 30,000 and 70,000 in 2001, distributed amongst 67 discrete groups of which 44 groups (67 per cent) are not affiliated with either Al-Qa’ida or Da’ish. In 2001, there were 25 such groups; now extremist groups worldwide have been augmented 180 per cent.¹¹ These figures need to be set against the other reality; that of an unrelenting Western attempt to fragment and eliminate extremism through military action, and underlines the fact that, despite military success, widespread resentment of Western interference has, nonetheless fed the pool of committed opponents to the Western project. By any standard, this represents a monumental failure in achieving security at immense cost, with the added irony – as suggested above – that it has also served the purpose of those opposed to Western objectives by radically disaggregating the ‘gray zone’ in which Western populism has become a tacit accomplice. As Senator Elizabeth Warren made clear in a speech at the American University in Washington on November 29, 2018:

“Despite America’s huge investment, these wars have not succeeded even on their own terms. Seventeen years later [since 2001], the Middle East remains in shambles. US counterterrorism efforts have often undermined other efforts to reinforce civilian governance, the rule of law, and human rights abroad. We have partnered with countries that share neither our goals nor our values. In some cases, as with our support for Saudi Arabia’s proxy war in Yemen, US policies risk generating even more extremism. Widespread migration of millions of people seeking safety from war-torn regions has allowed right-wing demagogues to unfairly blame the newcomers for the economic pain of working people at home”.

11 See Jones *et al.* (2018, pp. 23-26). These groups, except for *Ahrar ash-Sham* in Syria, are located primarily in Afghanistan or South Asia and take their inspiration from the Deobandi movement, rather than Wahhabi Islam.

This strategic failure is accompanied by a failure of interpretation as well. As I have suggested in a companion article (Joffé, 2017), the widespread assumption that the cause of Islamic extremism is buried within the Islamic theological and ideological corpus is misplaced. Rather than just having religious roots, the drivers for extremism are manifold and also arise from geopolitical, political, psychological and sociological factors as well. Indeed, in many, if not most cases, ideology plays a subordinate role, becoming simply a means of legitimising or camouflaging quite different causes instead. And, in a final irony, right-wing non-Muslim violent extremists have begun to ape the tactics of their supposed antagonists, particularly in 'lone wolf' attacks in Europe and the United States!

New Transnational Terrorism?

If indeed the campaign against violent extremism is failing despite its apparent military successes and despite the intellectual, organisational and ideological rigidity of one of its major opponents – Da'ish – this would suggest a new form of transnational terrorism has, in fact, emerged which we need to understand. Our understanding of the new extremist environment that we now confront would also have to take into account that the new form has emerged despite the lack of intellectual, strategic or tactical innovation that part of the new movement may manifest and that, instead, its success may be as much a consequence of the errors of its antagonists rather than of its own innate principles. In other words, the 'war on terror' may have been a significant contributor to the successful mutation of the opponent it was meant to destroy! And that, in turn, may be crucial to the future design of strategies that could achieve that original goal.

And that, also in turn, may require a review of what that original goal might have been and an understanding of what violent extremism really represents. Violent extremism – usually categorised as 'terrorism', although there is no generally-accepted definition of the term¹² – is a tactic through which a dominant narrative, usually that of a state, is challenged. Despite the difficulty of defining precisely what it is, such extremism does have certain unique characteristics which allow us to distinguish it from other tactical categories of violence through which dominant narratives are contested. Firstly, it tends to be a tactic adopted by groups that perceive themselves as being far weaker than their antagonists, although states may also make use of the tactic as a convenient form of unconventional or hybrid warfare.¹³

12 The definition that is used here is that proposed by Paul Wilkinson who argues that 'terrorism is the systematic use of coercive intimidation, usually to service political ends' (Wilkinson, 2006, p. 15).

13 The term 'hybrid warfare' is a term used to describe a range of tactics "widely understood to blend conventional/unconventional, regular/irregular, and information and cyber warfare". It first appeared around 2006 in reference to Hizbullah's tactics in its war in that year against Israel. See Puyvelde (2016).

Secondly, the term is permeated by moral ambiguity, in that the antagonists – usually states – consider such activities to be criminal since terrorism usually involves civilian deaths and, conventionally, only states can legitimise murder by its citizens (or others in its employ) or of them in pursuit of the wider goals of the state through warfare. However, to the perpetrators of violent extremism, it is their own actions that are inherently moral, for the state has delegitimized itself by its own violence towards its opponents. This is a feature that can also provide a certain specificity towards a phenomenon which is otherwise apparently ideologically neutral. In this respect, salafi-jihadism has an immediate relevance for it provides both a moral framework and the guidelines for a structure through which it can be articulated.

In addition, it is generally considered that extremist violence is indiscriminate in nature and unbounded, for its targets are often apparently innocent civilians and bystanders who have no direct connection with the events in question. The classic response to this is to be found in the “testament” of Emile Henry, an anarchist who in February 1894 bombed a café in Paris – the Café Terminus in Gare St Lazare – which was frequented by the French bourgeoisie. His actions were predicated against the bourgeoisie precisely because of their class-identity and their role, in Emile Henry’s eyes, in exploiting the French working-class. His testament, in the form of a statement to the jury whose verdict enabled his sentence of death – he was executed in May 1894 – is a detailed and reasoned exposition of this argument.¹⁴

Thus the apparently indiscriminate nature of terrorist violence in fact has a certain specificity about it, for there are groups of people who are considered legitimate targets precisely because they are members of the group, not because of their individual actions or responsibilities. The principle, of course can have much wider ramifications but, in the case of terrorism, it is an integral part of the process itself and, almost by definition, means that innocent individuals will be the intended targets and not simply unfortunate incidental victims. It also emphasises, of course, that only certain groups of people can be considered as legitimate targets, thus showing that extremist violence is not necessarily unbounded.

There are many other features that characterise terrorist violence as well,¹⁵ but for our purposes, it is the fact that extremist violence is a tactic, a mode of action to achieve a specified political purpose, not an organisation as such, with a specific

14 See Henry (1894). The specific reason for his choice of the Café Terminus was the execution of Auguste Vaillant, another anarchist who had bombed the French national assembly, injuring twenty-two deputies the previous December in protest over the corruption rife in France for which Emile Henry held the bourgeoisie responsible. Tradition has it that, after his capture in the immediate aftermath of the bombing, Henry was asked why he had tried to kill so many innocent people (only one person actually died, although twenty others were injured) and he replied, “Nobody is innocent!” In reality, he had said, “There are no innocent bourgeois!” thus emphasising the importance of group-identity in determining appropriate targets.

15 Fuller reviews are provided in Joffé (2004 and 2010).

and well-defined ideology to legitimise its actions that is important although the actual nature of the legitimising ideology is not. The one exception to this is epiphenomenal terrorism or extremism in which violence, in itself, is the objective, not the political outcome sought as a consequence of the violence. There is, perhaps a further condition for, as a tactic alone, violent extremism of this kind is also antiphonal in nature; it depends on a defined antagonist with which it can engage on parallel terms and which can and does engage (albeit unwittingly) with it. The 'war on terror' has fulfilled this role to perfection and has thus become a driver for the expansion of extremism, rather than its nemesis, as it had been supposed to be.

Responses

In this respect, therefore, the rigidity that Da'ish now demonstrates is of little consequence for its power of attraction resides in the moral ambiguity it exploits and in its ability to engage with codified and structured Western hostility. In that respect, it differs little from Al-Qa'ida despite the latter's flexibility and innovative ideological evolution, as described above. The new wave of transnational terrorism, in short, is in reality reactive, not innovative, as was its predecessor, and reflects long-standing agonistic tensions between two separate cultural domains. An aspect of its renewed vitality and viability is its relevance as a means of authenticating a cultural reality, however distorted and brutal it may appear to a disinterested observer; that of an innately authentic Muslim social order. Yet its weakness in those terms is the distortion and violence it has created in its interpretation of that ideal. In the long term, therefore, it will be doomed to failure.¹⁶

Yet the longevity of its survival is partly predicated on the nature of the response to it, as the failure of the 'war on terror' has demonstrated. The final question, therefore, must be what the new strategy and tactics to hasten the demise of this 'new transnational terrorism' should be. In terms of tactics, there seems little doubt that, since the military approach has failed, it would be wise to return to the alternative of treating violent extremism as an inherently criminal enterprise. Quite apart from the movement's inherent violence, whatever the justification, nearly all the groups involved use techniques of financing their activities which are illicit or illegal, whether through *hawala*,¹⁷ smuggling, theft, fraud or violence.

16 As Rapoport has pointed out, violent extremism has been a constant concomitant of the established international order and of the state as an expression of those individuals and groups who have felt excluded from the international community and the state ever since the French revolution at the end of the eighteenth century. The consequent and repeated waves of violence, each dominated by an hegemonic ideological vision to legitimise it, have tended to last for up to forty-to-forty-five years (Rapoport, 2002).

17 As Charles Tripp points out, *hawala* "[relies] on interpersonal transnational networks of trust, which avoid the formal banking institutions associated with the dominant global capitalist economy..." (Tripp, 2006, p. 6). See also Ballard (2003) and Jost and Sandhu (n/d).

However, this approach alone will be insufficient to eliminate the threat because of the moral ambiguity in which violent extremism is located and the historical justifications for its sense of resentment and victimhood. In many respects, this is a far greater challenge for it will involve challenging and countering the populism and Islamophobia that have been entrenched in the Western image of Islam during the past two decades. It will also involve the incorporation of Muslim minority communities within Europe into the mainstream communities already there, despite their growing resentments at what is increasingly perceived as an alien intrusion into a European cultural space shaped by quite different influences. It remains to be seen whether the West still has the imagination and empathy to be able to do this and whether it has the political and cultural leadership to achieve such an outcome despite the increasingly agonist nature of its confrontation with the Muslim world.

Bibliography

- Adorno, T., 1951. *Minima Moralia: Reflexionen aus dem bechädigten Leben*. Jephcott, E.N.F., trans., 1978, *Minima Moralia: reflections of a damaged life*. London: Verso.
- Anon., 2018a. Afghanistan: the largest number of journalists killed in one year. *Asharq al-Awsat*, London, September 22.
- Anon., 2018b. US 'war on terror' has killed over half a million: study. *Al-Jazeera* [online], November 9. Available at: <https://www.aljazeera.com/news/2018/11/wars-terror-killed-million-people-study-181109080620011.html>
- Anon., 2015. How many terrorists has President Obama actually 'taken out'? Probably over 30,000. *Washington Post*, December 7.
- Ballard, R., 2003. *A Background Report on the Operation of Informal Value Systems (Hawala)*, 6th April. Available at CrossAsia-Repository/University Library of Heidelberg [website] <http://crossasia-repository.ub.uni-heidelberg.de/271/1/hawala.pdf>
- Bellaigue, C., 2017. *The Islamic Enlightenment: the modern struggle between faith and reason*. London: Bodley Head.
- Brachman, J., 2009. *Global Jihadism: Theory and Practice*. London: Routledge.
- Chouet, A., 2008. Le terrorisme: mal du siècle ou art renouvelé de la guerre? In Arpagian, N. and Delbecque, E., eds., *Pour une stratégie globale de sécurité nationale*. Paris: Dalloz/Présaja, chapter 14.
- Counter Extremism Project, 2018. *Al-Qaeda in the Islamic Maghreb (AQIM)*. Counter Extremism Project. London and New York. Available at: <https://www.counterextremism.com/threat/al-qaeda-islamic-maghreb-aqim>
- Cummings, R., 2017. A Jihadi takeover bid in Nigeria? The evolving relationship between Boko Haram and Al Qad'ia. *CTC Sentinel*, 10(11). Available at: <https://ctc.usma.edu/a-jihadi-takeover-bid-in-nigeria-the-evolving-relationship-between-boko-haram-and-al-qaeda/>
- Gerges, F., 2005. *The Far Enemy: why Jihad went global*. Cambridge: Cambridge University Press.

- Henry, E., 1894. *Testament*. Available at: <http://recollectionbooks.com/bleed/AnarchistTimeline2.htm>
- Huntington, S., 1993. The clash of civilizations? *Foreign Affairs*, 72(3), pp. 22-32.
- Joffé, G., 2017. What is the enemy? *Nação e Defesa*, 148, pp. 10-27.
- Joffé, G., 2016a. The fateful phoenix: the revival of Al-Qa'ida in Iraq. *Small Wars and Insurgencies*, 27(1), pp. 1-21.
- Joffé, G., 2016b. Global Jihad and foreign fighters. *Small Wars and Insurgencies*, 27(5), pp. 800-816.
- Joffé, G., 2010. Radicalism, extremism and government in North Africa. In Asaf Siniver, ed., *International Terrorism post 9/11: Comparative Dynamics and Responses*. London: Routledge, Chap. 3.
- Joffé, G., 2007. Confrontational mutual perceptions and images: Orientalism and Occidentalism in Europe and the Islamic world. *International Spectator*, 42(2), pp. 161-177.
- Joffé, G., 2004. Global terrorism. *EuroMeSCo Paper No. 30*, May, IEEI, Lisbon. Available at: <https://www.euromesco.net/wp-content/uploads/2017/10/200405-EuroMeSCo-Paper-1.30.pdf>
- Jones, S., et al., 2018. *The evolution of the Salafi-Jihadist threat: current and future challenges from the Islamic State, Al-Qaeda and other groups* [pdf]. A report of the Center for Security and International Studies (CSIS), November, Washington. Available at CSIS [website] <https://www.csis.org/analysis/evolution-salafi-jihadist-threat>
- Jost, P. and Sandhu, H., n/d.. *The Hawala Alternative Remittance System and its Role in Money Laundering*. Financial Crimes Enforcement Network/Interpol-FOPAC. Available at: <https://www.assetsearchblog.com/wp-content/uploads/sites/197/2013/06/FinCEN-Hawala.pdf>
- Kaplan, J., 2008. Terrorism's Fifth Wave: A Theory, a Conundrum and a Dilemma. *Perspectives on Terrorism*, 2(2), pp. 12-24.
- Kirkpatrick, D., 2014. Militant Group in Egypt Vows Loyalty to ISIS. *The New York Times* [online], 10 November. Available at: <https://www.nytimes.com/2014/11/11/world/middleeast/egyptian-militant-group-pledges-loyalty-to-isis.html>
- Lia, B., 2008. *Architect of Global Jihad: The Life of Al-Qaeda Strategist Abu Mus'ab Al-Suri*. New York: Colombia University Press.
- Maher, S., 2018. The primacy of praxis: clerical authority in the Syrian conflict. *Policy Paper 2018-10*, October, Middle East Institute, New York. Available at Middle East Institute [website] https://www.mei.edu/sites/default/files/2018-11/PP12_MaherCT.pdf
- Malik, K., 2011. Rethinking the idea of 'Christian Europe'. *Pandemonium* [online], August 19. Available at: <https://kenanmalik.com/2011/08/19/christian-europe/>
- Naji, A., 2006. *The Management of Savagery: The Most Critical Stage through Which the Umma Will Pass*. William McCants, trans.. Cambridge: John M. Olin Institute for Strategic Studies, Harvard University Press. Available at: <https://ia800901.us.archive.org/12/items/The-ManagementOfBarbarismAbuBakrNaji/The%20Management%20of%20Barbarism%20-%20Abu%20Bakr%20Naji.pdf>

- Norton-Taylor, R., 2011. MI5 former chief decries 'war on terror'. *The Guardian* [online], September 2, 00.30 BST. Available at: <https://www.theguardian.com/uk/2011/sep/02/mi5-war-on-terror-criticism>
- Puyvelde, D., 2016. Hybrid war – does it even exist? *NATO Review Magazine* [online]. Available at: <https://www.nato.int/DOCU/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm>
- Rapoport, D., 2002. The four waves of rebel terror and September 11. *Anthropoetics: the Journal of Generative Anthropology* [online], 8(1). Available at: <http://anthropoetics.ucla.edu/ap0801/terror/>
- Robinson, F., 2009. Crisis of Authority: Crisis of Islam? *Journal of the Royal Asiatic Society*, 19(3), pp. 339-354.
- Ryan, M., 2013. *Decoding Al Qaeda's Strategy: the deep battle against America*. New York: Columbia University Press.
- Sanderson, T., 2018. From the Fergana Valley to Syria and Beyond: A Brief History of Central Asian Foreign Fighters. *Centre for Strategic and International Studies* [online], January 5, Washington. Available at: <https://www.csis.org/analysis/ferghana-valley-syria-and-beyond-brief-history-central-asian-foreign-fighters>
- Singh, B., 2017. The revival of Al Qaeda's affiliate in South-East Asia: the Jemaah Islamiyyah. *Counter-Terrorist Trends and Analyses*, 9(5), pp. 5-8. Retrieved from <http://www.jstor.org/stable/26351517>
- Tripp, C., 2006. *Islam and the Moral Economy: The Challenge of Capitalism*. Cambridge: Cambridge University Press.
- Trotta, D., 2011. Cost of war at least \$3.7 trillion and counting. *Reuters* [online], June 29, 12:05 PM. Available at: <https://www.reuters.com/article/us-usa-war/cost-of-war-at-least-3-7-trillion-and-counting-idUSTRE75S25320110629>
- United Nations Security Council, 2018. *Sixth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat*. S/2018/80, January 31, 2018, United Nations, New York. Available at: https://www.un.org/en/ga/search/view_doc.asp?symbol=S/2018/80&referer=/english/&Lang=E
- Wilkins, B., 2015. Doctors group says that 1.3 million killed in US 'war on terror'. *Digital Journal* [online], March 25. Available at: <http://www.digitaljournal.com/news/world/study-1-3-million-killed-in-usa-war-on-terror/article/429180>
- Wilkinson, P., 2006. *Terrorism versus democracy: the liberal state response*, 2nd edition. London and New York: Routledge.

Liberdade e Segurança no Combate ao Terrorismo: *Quis Custodiet Ipsos Custodes?* Uma Perspetiva Jurídica*

Sofia de Vasconcelos Casimiro

Professora da Academia Militar. Professora da Faculdade de Direito da Universidade de Lisboa. Advogada e juriconsulta especialista em tecnologias de informação. Coordenadora da formação em Direito, Cibersegurança e Ciberdefesa no projeto Multinational Cyber-defence Education and Training (MNCDE&T) da NATO. Doutorada por Queen Mary, University of London, Intellectual Property Research Institute. Mestre e licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa.

Resumo

Este artigo contém uma reflexão sobre os desafios do combate ao terrorismo num Estado de Direito. Tendo como ponto de partida os valores do Estado de Direito, que consagra os direitos fundamentais à liberdade e à segurança, detém-se sobre o atual equilíbrio deste binómio. Abordam-se três casos de estudo: (i) as condições de detenção e os métodos de tratamento dos presos no Campo de Detenção da Baía de Guantánamo; (ii) o uso de veículos aéreos não tripulados para fins militares; e (iii) a gestão de programas de vigilância das comunicações que abrangem indiscriminadamente militares e civis, em contextos de guerra e de paz. Um dos principais desafios do combate ao terrorismo consiste em ser eficaz nesse combate sem colocar em causa os princípios que sustentam o próprio Estado de Direito. Na eventualidade de o terrorismo visar a subversão do Estado de Direito, e do modo de vida ocidental neste assente, cabe verificar em que medida os meios de combate ao terrorismo poderão, paradoxalmente, destruir ou pelo menos colocar em causa o Estado de Direito que se visa defender. Uma vez que o Estado é o guardião dos valores do Estado de Direito, violados nestes três casos de estudo, há que questionar quem guarda os guardiões: *quid custodiet ipsos custodes?*

Abstract

Freedom and Security in the Fight Against Terrorism from a Legal Perspective: Quid Custodiet Ipsos Custodes? The Particular Case of Cyberterrorism

*This paper contains a reflection on the challenges of fighting terrorism under the rule of law. Having as a starting point the values of the rule of law, which embodies the fundamental rights of freedom and security, the paper tackles the current balance between the two. Three case studies are covered: (i) the detention conditions and methods of treatment of the prisoners in the Guantanamo Bay Detention Camp; (ii) the use of unmanned aerial vehicles for military purposes; and (iii) the management of mass surveillance programs which include military forces and civilians indiscriminately, in context of war and peace. One of the main challenges of fighting terrorism consists in being effective without putting in stake the principles which sustain the rule of law itself. In the event, the terrorism pursues the subversion of the rule of law, and the western lifestyle supported by it, it is important to understand the extent to which the means used in fighting terrorism can, paradoxically, destroy or at least call into question the rule of law that they claim to defend. Since the State is the guardian of the rule of law's values, violated in these three case studies, one should ask who is guarding the guardians: *quid custodiet ipsos custodes?**

* Este artigo foi redigido na sequência da participação, como oradora, numa sessão do Grupo de Estudos “Terrorismo e Violência Política” dedicada ao tema “Liberdade e Segurança no Combate ao Terrorismo”, em 15 de março de 2018, promovido pelo Instituto da Defesa Nacional (IDN). A autora agradece ao Senhor Major-General Vítor Daniel Rodrigues Viana, Diretor do IDN, o convite que lhe foi endereçado para participar nesta iniciativa, que, como muitas outras promovidas por esta instituição, contribuem para o debate, divulgação e avanço no estudo e tratamento de grandes temas de relevância nacional. Ao Senhor Major-General deve-se uma liderança visionária do IDN.

“Because, therefore, we are defending a way of life, we must be respectful of that way of life as we proceed to the solution of our problem. We must not violate its principles and its precepts, and we must not destroy from within what we are trying to defend from without.”

Dwight David Eisenhower, speech before NATO Council,
11/26/51 [DDE's Pre-Pres. Papers, Box 197]

1. Breve Excurso Histórico até às Conquistas do Estado de Direito

As conquistas do Estado de Direito, tipo de Estado dominante no atual panorama internacional, definem a sociedade ocidental e são utilizadas como estandarte que se exhibe orgulhosamente perante outras formas de organização em sociedade.

O Estado de Direito, constitucional ou representativo caracteriza-se por instituir a supremacia do Direito. Todos, sem exceção, encontram-se sujeitos ao Direito, incluindo os órgãos de soberania e mesmo aqueles que criam o Direito. Consagram-se, nas Leis Fundamentais em que se traduzem as constituições modernas, mecanismos vários de proteção dos cidadãos contra o abuso de poder e que se destinam a limitar esse poder, nomeadamente os direitos fundamentais, os princípios da liberdade e da igualdade, a fiscalização da constitucionalidade e da legalidade, a separação de poderes e o equilíbrio de forças entre órgãos detentores do poder, concretizado nos chamados *checks and balances*. Por sua vez, o Direito é uma manifestação da soberania popular, devendo assegurar-se a representatividade da população no poder exercido pelo Estado.

Percorreu-se um longo caminho até chegar ao Estado de Direito. Na tipologia gizada por Georg Jellinek (2005)¹, e adotada por grande parte dos constitucionalistas, os tipos mais antigos de Estado, como o Estado oriental, que teve lugar mais de 3.000 anos antes de Cristo, assim como o Estado grego, romano e medieval comungavam da arbitrariedade no exercício do poder, da estratificação da sociedade, da indefinição, embora em graus variáveis, do corpo legal aplicável.

O Estado oriental caracterizava-se por uma coincidência entre o poder político e o poder religioso, verificando-se geralmente uma divinização do monarca, bem como por uma ordem desigualitária, hierárquica e hierática da sociedade, que atribuía muito poucas garantias às pessoas e que as remetia para um plano secundário. Embora o Estado romano, iniciado por volta de 753 anos antes de Cristo, tenha contribuído grandemente para o reconhecimento de direitos básicos do cidadão, estes não se configuravam ainda como direitos universais. Ademais, com a entrada no Estado medieval, no século X, verificou-se um claro retrocesso na proteção dos cidadãos, agora convertidos em senhores ou vassalos, dentro da cadeia de vínculos contratuais que caracterizava o feudalismo. A passagem do

1 Veja-se, entre outras obras de Jellinek.

Estado medieval para o Estado europeu ou moderno, por volta de meados do século XV, com a tomada de consciência das nações, ou a sua formação, a separação entre o poder político e religioso e a introdução do conceito de soberania, trabalhado por Jean Bodin², conduziu ao acolhimento de algumas das noções imperantes nos dias de hoje e permitiu um grande avanço em relação ao período das trevas medieval. O aumento do conhecimento das populações e o impulsionamento das artes, ciências e filosofia, e de várias outras áreas da sociedade, com o Renascimento, determinaram uma viragem determinante na mentalidade europeia que não mais recuará.

Foi, contudo, com o movimento da revolução francesa, impulsionada pela revolução industrial e pelas mudanças sociais por esta impostas, que se proporcionou a disseminação e a implementação dos novos ideais que representaram as bases do Estado de Direito. As novas correntes filosóficas, como o contratualismo, o iluminismo ou o individualismo, trazem finalmente a pessoa humana para o centro do poder político, enquanto governante, sujeito que exerce o poder político e que deve assumir as rédeas na tomada das decisões, mas também enquanto governado e, assim, sujeito a quem se destinam as decisões³. De entre os principais reflexos desta diversa abordagem, destaca-se a proliferação das declarações de direitos, que reconhecem um limiar mínimo de respeito pela dignidade da pessoa humana. Os direitos fundamentais, agora assumidos como direitos universais e inalienáveis, são acolhidos em vários ordenamentos jurídicos nacionais, criando as condições para que, no rescaldo dos grandes conflitos mundiais, se internacionalizem e sejam cristalizados em instrumentos jurídicos como a Declaração Universal dos Direitos Humanos⁴, a Convenção Europeia dos Direitos Humanos e das Liberdades Fundamentais⁵ e a Carta dos Direitos Fundamentais da União Europeia⁶.

A centralização do poder político na pessoa humana e a consagração dos direitos fundamentais revelam a preocupação de proteger a pessoa face ao Estado. Neste sentido, são implementados vários mecanismos de limitação do poder do Estado e destinados a assegurar a supervisão da sua atuação e a sua conformidade com o

2 Ver obra clássica *Les Six Livres de la République*, reimpressão de 2013.

3 “O iluminismo é a saída do homem da sua menoridade. E menoridade é a incapacidade de se servir do entendimento sem a orientação de outrem. Tal menoridade é por culpa própria...” (Kant, 1988, p. 11).

4 A Declaração Universal dos Direitos Humanos foi adotada pela Organização das Nações Unidas em 10 de dezembro de 1948.

5 A Convenção Europeia dos Direitos Humanos e das Liberdades Fundamentais foi adotada pelo Conselho da Europa, em 4 de novembro de 1950.

6 A Carta dos Direitos Fundamentais da União Europeia foi adotada pelo Parlamento Europeu, pelo Conselho da União Europeia e pela Comissão Europeia em 7 de dezembro de 2000.

Direito vigente⁷. O Estado de Direito é, assim, um tipo de Estado que procura proteger a pessoa perante o Estado através de normas jurídicas que comportam esta preocupação e cuja observância é controlada por vários mecanismos nestas previstos. A proteção da pessoa face ao Estado concretiza-se sobretudo pela atribuição de um conjunto de direitos que apenas poderão ser restringidos em situações devidamente justificadas, devendo esta restrição limitar-se ao estritamente necessário. De entre os direitos atribuídos, existe ainda um núcleo cuja restrição não é admitida. Entre estes direitos, que não podem ser afastados, encontram-se os direitos à vida, à integridade pessoal – incluindo a proibição da tortura ou de penas ou tratamentos cruéis, desumanos ou degradantes, bem como a proibição da escravatura – à identidade pessoal, à capacidade civil e à cidadania, a não retroatividade da lei criminal, o direito de defesa dos arguidos e a liberdade de consciência e de religião. Para além de os direitos encontrarem consagração nos planos nacional e internacional, como já foi referido, as condições da sua restrição encontram-se também previstas nos planos nacional e internacional⁸.

Após uma longa evolução histórica, as características do Estado de Direito apresentam-se como verdadeiras conquistas. Podendo correr-se o risco de as tomar como adquiridas, e de reduzir os mecanismos que controlam a sua efetivação e que asseguram o seu estrito cumprimento, deverá acautelar-se a sua preservação e não desvirtuamento em todos os momentos e contextos.

2. O Terrorismo e os seus Desafios

O terrorismo não é um fenómeno recente (Chaliand e Blin, 2004). A principal razão para o aumento da perceção deste fenómeno no mundo ocidental prende-se com a sua incidência crescente no respetivo território, inflacionada pela grande visibilidade que lhe é dada. Desde os eventos de 11 de Setembro de 2001, com os ataques perpetrados no território dos Estados Unidos da América – nessa altura inconcebíveis, dada a imagem de segurança externa projetada por este Estado –, o sentimento geral de insegurança em relação a ameaças desconhecidas e incontroláveis instalou-se no mundo ocidental.

Acresce ainda que, a par com o terrorismo praticado por meios analógicos, surge

7 As palavras de Jorge Miranda são eloquentes a este propósito, quando explica que o Estado de Direito consiste num “conjunto de princípios, instituições, processos que a tradição e a experiência dos juristas e dos tribunais mostraram ser essenciais para a salvaguarda das pessoas frente ao Estado, à luz da ideia de que o Direito deve dar aos indivíduos a necessária proteção contra qualquer exercício arbitrário de poder” (Miranda, 2014, p. 138).

8 Vejam-se, a nível nacional, os artigos 18.º e 19.º, n.º 6, da Constituição da República Portuguesa, bem como o artigo 2.º, n.º 1, da Lei n.º 44/86, de 30 de setembro. A nível internacional, veja-se, por exemplo, o artigo 4.º do Pacto Internacional sobre os Direitos Civis e Políticos, adotado pela Organização das Nações Unidas em 16 de dezembro de 1966.

agora o terrorismo por meios eletrónicos ou ciberterrorismo. Muito embora tenha sido inicialmente desvalorizada, a verdadeira dimensão das ameaças colocadas pelo terrorismo por meios eletrónicos tem vindo a ser finalmente reconhecida⁹.

O terrorismo transporta consigo vários efeitos nefastos, bem como inúmeros desafios para o Estado de Direito, que nem sempre são evidentes. Um desafio central consiste na capacidade de combater o terrorismo sem colocar em causa os princípios que sustentam o próprio Estado de Direito. Na eventualidade de o terrorismo visar a subversão do Estado de Direito, e do modo de vida ocidental assente no Estado de Direito, cabe verificar em que medida os meios de combate ao terrorismo poderão, paradoxalmente, destruir ou pelo menos colocar em causa o Estado de Direito que se visa defender.

Entre os direitos fundamentais consagrados no seio do Estado de Direito, integram-se os direitos à liberdade e à segurança, ambos de extrema relevância no contexto do combate ao terrorismo. Estes dois direitos fundamentais encontram-se frequentemente em conflito, uma vez que um maior espaço de liberdade representa, por regra, menor segurança e um maior grau de segurança envolve, por regra, uma maior restrição da liberdade. Na Constituição da República Portuguesa, estes dois direitos encontram-se consagrados no artigo 27.º, que tem como epígrafe “Direito à liberdade e à segurança” e que, no seu n.º 1, prevê “Todos têm direito à liberdade e à segurança”.

Paralelamente ao conceito mais restrito da liberdade, respeitante especificamente à liberdade de movimentos, adota-se um conceito mais amplo, vulgarmente correspondente aos designados direitos de liberdade, que compreendem os direitos fundamentais que garantem genericamente o acesso individual a bens de liberdade individual, autonomia pessoal e participação política e que, *grosso modo*, na doutrina mais recente correspondem aos direitos, liberdades e garantias¹⁰, que consis-

9 Apesar de os trabalhos de sensibilização contra estas ameaças estarem a ser desenvolvidos desde há décadas atrás por algumas entidades, como, em Portugal, a Academia Militar, a Competitive Intelligence and Information Warfare Association (CIIWA) e o IDN, contribuíram grandemente para este reconhecimento e divulgação as declarações de altos cargos de direção dos Estados Unidos da América e, mais recentemente, da União Europeia. Vejam-se, por exemplo, as declarações de John Brennan, ex-Diretor da CIA, no programa de televisão “60 minutos”, em 2016, destacando que, de entre todas as ameaças, eram as ameaças de ataques por via eletrónica as que mais o preocupavam e que não o deixavam dormir à noite – CBS, programa 60 Minutes, fevereiro de 2016. De igual forma, no seu discurso anual sobre o estado da União, em 2017, o Presidente da Comissão Europeia, Jean-Claude Juncker (2017), elencou a proteção dos europeus contra ciber-ataques como uma das principais prioridades da União Europeia. Neste discurso, o Presidente da Comissão Europeia declarou que “Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks”.

10 Vide Jorge Reis Novais, *Direitos de Liberdade e Direitos Sociais na Constituição Portuguesa*.

tem na principal categoria de direitos fundamentais. Neste sentido mais amplo, verifica-se também uma constante fricção entre a segurança e os restantes direitos, liberdades e garantias. A segurança exige, quase sempre, uma restrição de outros direitos, liberdades e garantias. Por esta razão, na medida em que o combate ao terrorismo envolve um inevitável reforço da segurança, há que estar atento à observância de critérios de proporcionalidade e à imposição de limites naquela restrição. O ponto de equilíbrio entre segurança e liberdade, considerada nesta segunda aceção, mais ampla, é muito difícil de alcançar. Não há dúvidas de que o entendimento quanto ao que deva ser este ponto de equilíbrio tem conhecido uma ampla oscilação ao longo dos tempos, dependente do pulsar do sentimento geral da sociedade ou, por outras palavras, da opinião pública, influenciada grandemente pelo contexto histórico em que se insere.

Um exemplo paradigmático desta oscilação verifica-se com os referidos eventos de 11 de setembro de 2001. Antes de estes eventos terem lugar, foram apresentadas várias propostas de aprovação de medidas legislativas que reforçavam a segurança interna e externa dos Estados. Estas propostas foram maioritariamente rejeitadas, sobretudo por razões de defesa da liberdade dos cidadãos, onde se inclui a defesa da privacidade. Após o 11 de setembro, aquelas mesmas medidas legislativas, agora fortalecidas com maior pendor securitário, foram aprovadas e implementadas sem qualquer contestação de relevo. Este movimento verificou-se não apenas nos Estados Unidos da América, sendo ilustrativo a este propósito o *USA Patriot Act*¹¹, como ainda em vários outros Estados do mundo ocidental.

O pacote legislativo de reforma do sector das comunicações eletrónicas da então Comunidade Económica Europeia encontrava-se na sua fase final de aprovação no momento em que se verificaram os eventos de 11 de Setembro. Todas as propostas de Diretiva incluídas no referido pacote legislativo foram aprovadas com exceção da proposta de Diretiva relativa à privacidade no sector das comunicações eletrónicas, que foi retida com vista a ponderar a sua melhor adequação aos novos desafios de segurança externa e interna face ao 11 de setembro. A redação original desta proposta robustecia a proteção dos direitos, liberdades e garantias e parecia esquecer as necessidades de segurança, face ao cenário de paz que se fazia sentir até então. Impunha-se agora uma ponderação dos recentes desenvolvimentos despoletados com o 11 de setembro. Como resultado daquela ponderação, inseriu-se na proposta de Diretiva relativa à privacidade no sector das comunicações eletrónicas o polémico artigo 15.º, que prevê a possibilidade de cada Estado-membro restringir várias das proteções conferidas por essa Diretiva para fins de segurança. À luz desta disposição, os Estados-membros poderão restringir essas proteções sempre

11 “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act”, de 2001.

que “essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas”¹².

Algumas das alterações implementadas na vida quotidiana do mundo ocidental após o 11 de setembro demonstram igualmente uma viragem perante o binómio segurança-liberdade. Antes do 11 de setembro, o controlo da segurança nos aeroportos através do *scan* corporal dos passageiros, com a captação de uma imagem mais ou menos detalhada do corpo dos passageiros, parecia inimaginável. Esta medida, sobretudo nas suas formulações iniciais, mais invasivas, parecia manifestamente injustificada e, assim, excessiva. Atualmente, estas e outras medidas são entendidas como necessárias e mesmo desejadas como forma de garantir a segurança dos próprios visados.

É indubitável que o combate ao terrorismo tem justificado restrições à liberdade dos cidadãos no mundo ocidental. Estas restrições surgem como inevitáveis, não tendo sido possível até ao momento alargar o espectro de segurança sem ocupar um espaço que estava antes destinado à liberdade. Liberdade e segurança partilham o mesmo campo de atuação, pelo que estão em contínua competição pela ocupação do respetivo espaço. Antes de compreender os termos em que se processa esta competição, porém, importa perceber melhor em que consiste o terrorismo e qual o correspondente quadro legal nacional.

2.1. Dificuldades de Definição do Terrorismo

O terrorismo não tem uma definição fácil¹³. Podem ser adotados inúmeros critérios para a sua delimitação, quer quanto aos fins, aos meios, aos sujeitos, ou mesmo ao contexto político, entre vários outros. Por esta razão, identificam-se muitas definições possíveis de terrorismo¹⁴.

Esta volatilidade das fronteiras conceptuais do terrorismo não é vantajosa para o seu estudo e posterior enquadramento pelos ordenamentos jurídicos. Uma vez que a prática de atos de terrorismo é qualificada como crime, à luz dos vários ordenamentos jurídicos nacionais, esta volatilidade dificulta a harmonização de

12 Redação original do n.º 1 do artigo 15.º da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas – Diretiva relativa à privacidade e às comunicações electrónicas.

13 Veja-se Wojciechowski (2009) e Schmid (2004).

14 De acordo com Pierre-Marie Dupuy (2004, p. 5), existem pelo menos 109 possíveis definições de terrorismo.

um quadro legal na matéria e a criação de planos transnacionais de combate a este fenómeno. Na eventualidade de se adotar um conceito demasiado amplo, de maneira a integrar várias manifestações dessa realidade e facilitar a conciliação com outros ordenamentos jurídicos, pode mesmo atentar-se contra o princípio da legalidade, que preconiza, num Estado de Direito, a delimitação precisa e prévia das ações e omissões que são qualificadas como crime¹⁵. Vários argumentos aconselham, assim, a convergência numa definição consensual, una e bem delimitada de terrorismo, a nível nacional, regional e internacional.

No espaço da União Europeia, a Diretiva 2017/541¹⁶ procura contribuir para a harmonização das legislações nacionais dos Estados-membros nesta matéria, fixando regras mínimas relativas à definição das infrações penais e das sanções em matéria de infrações terroristas, infrações relacionadas com um grupo terrorista e infrações relacionadas com atividades terroristas, bem como medidas de proteção, apoio e assistência às vítimas do terrorismo.

Mesmo fora destes espaços geográficos onde se tem avançado no sentido de alcançar alguma harmonização, encontram-se alguns pontos de contacto nas várias legislações que contemplam o terrorismo. Por regra, este envolve a prática ou a ameaça de prática de atos de grande violência cometidos para intimidar a população, grupos determinados da população ou o poder político, com vista a provocar mudanças no sistema político ou a conquistar mais poderes ou a independência. Em termos muito simplistas, o terrorismo visa a adoção de um comportamento que favoreça as pretensões do agente. Pode ter fins políticos, religiosos ou ideológicos. Se a definição de terrorismo não é uma tarefa fácil, a integração de uma certa conduta nas definições existentes não oferece menor dificuldade. Para além do grau de complexidade inerente à subsunção dos factos às normas jurídicas, as partes envolvidas avaliam os factos de uma maneira diferente. Como é repetido nos textos sobre a matéria, “one man’s terrorist is another man’s freedom fighter”¹⁷.

2.2. *Quadro Legal Nacional de Combate ao Terrorismo*

No plano nacional, a Estratégia Nacional de Combate ao Terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 7-A/2015, estabelece objetivos estratégicos de combate ao terrorismo e define as linhas de ação através das quais se irão concretizar esses objetivos. Esta Estratégia é delineada de uma forma integrada, sem esquecer as várias vertentes que compõem um combate efetivo ao terrorismo.

15 Cfr. Greene (2017).

16 Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho de 15 de março de 2017 relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho.

17 *Vide*, por exemplo, Alex Schmid (2004, p. 397).

Destaca-se o facto de este documento iniciar pela enunciação do compromisso de, no combate ao terrorismo, respeitar “a Convenção Europeia dos Direitos Humanos e das Liberdades Fundamentais do Conselho da Europa, o direito originário da União Europeia, a Carta dos Direitos Fundamentais da União Europeia, os princípios constitucionais do Estado português, a política de luta contra o terrorismo da União Europeia” e desenvolver-se “na estrita observância dos princípios da necessidade, da adequação, da proporcionalidade e da eficácia, das liberdades cívicas, do Estado de Direito e de liberdade de escrutínio”¹⁸. Conforme se retira desta passagem, o legislador, tendo presente os desafios de conciliação dos vários valores em confronto, tem a preocupação de lembrar as principais balizas de atuação no combate ao terrorismo. Sublinha que este combate não pode, em caso algum, implicar o afastamento ou a restrição desnecessária, desproporcionada ou inadequada dos pilares que caracterizam o Estado de Direito.

Em matéria penal, a Lei de Combate ao Terrorismo, aprovada pela Lei n.º 52/2003, de 22 de agosto¹⁹, dá o seu contributo para a exatidão do conceito do terrorismo. De acordo com este diploma legal, os atos terroristas são aqueles que “visem prejudicar a integridade e a independência nacionais, impedir, alterar ou subverter o funcionamento das instituições do Estado previstas na Constituição, forçar a autoridade pública a praticar um ato, a abster-se de o praticar ou a tolerar que se pratique, ou ainda intimidar certas pessoas, grupos de pessoas ou a população em geral...” e que se integrem na enumeração taxativa do n.º 1 do seu artigo 1.º.²⁰ Na sua grande maioria, os atos enumerados correspondem a atos já criminalizados por outras normas jurídicas. O facto de estes atos serem praticados com finalidades terroristas justifica uma diversa medida da pena, agravada, face àquela que resulta dessas outras normas jurídicas. O agravamento da medida da pena traduz a maior censurabilidade de atos terroristas, face ao impacto que têm na sociedade em geral e aos riscos que colocam ao Estado de Direito.

Com as últimas alterações à Lei de Combate ao Terrorismo, introduzidas já em 2019, criminalizou-se o recebimento de treino em Portugal e no estrangeiro, bem como o ato de viajar ou tentar viajar para um território diferente do seu Estado de residência ou nacionalidade, com vista a receber treino ou outro tipo de apoio para o desenvolvimento de atividades terroristas. Alargou-se ainda o conceito de financiamento ao terrorismo. Procurou-se, por esta forma, colmatar algumas falhas da legislação portuguesa, cobrindo situações que ainda não estavam previstas e que não podem deixar de ser reprimidas criminalmente.

18 Veja-se o n.º 2 da Estratégia Nacional de Combate ao Terrorismo.

19 Esta lei transpõe para a ordem jurídica interna a já referida Diretiva (UE) 2017/541, do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo.

20 Esta definição resulta da conjugação dos artigos 2.º, n.º 1, parte final e 4.º n.º 1, alínea a), ambos da Lei de Combate ao Terrorismo.

3. Os Limites Impostos pelo Estado de Direito

Uma vez identificados os principais traços definidores do Estado de Direito e demonstrados os desafios que o terrorismo pode colocar ao Estado de Direito, cabe apurar se o combate ao terrorismo tem vindo a ter lugar com total respeito do Estado de Direito e dos limites por este impostos.

Isolam-se a este propósito três casos de estudo, polémicos, que se encontram na fronteira deste tema que agora nos ocupa, do respeito do Estado de Direito aquando do combate ao terrorismo. Existiriam muitos outros casos suscetíveis de fazer parte deste elenco. Contudo, não se pretende realizar um tratamento exaustivo destes casos, mas tão somente ilustrar uma realidade que se entende dever ser evidenciada, estudada e, quando necessário, corrigida. Para este escopo, bastará a enunciação destes três casos de estudo.

O primeiro caso relaciona-se com as condições de detenção e os métodos de tratamento dos presos no Campo de Detenção da Baía de Guantánamo. Este campo de detenção consiste numa prisão militar dos Estados Unidos da América, situada numa base militar na ilha de Cuba. Esta prisão militar, que tem vindo a ser utilizada para deter vários suspeitos de terrorismo, foi criada em 2002 pelo Presidente George W. Bush, na sequência dos eventos de 11 de Setembro. Desde a sua criação, vieram a lume vários relatos da prática de tortura e de tratamento cruel, humilhante e degradante dos detidos nesta prisão, por parte das forças militares²¹. Adicionalmente, a grande maioria dos detidos que passou por esta prisão ou que ainda nesta se encontra está presa por período indeterminado, sem ter sido sujeita a julgamento.

Os factos descritos consubstanciam a violação de direitos, liberdades e garantias consagrados em instrumentos jurídicos internacionais, a que se vincularam os Estados Unidos da América. Entre estes instrumentos jurídicos internacionais, destacam-se as Convenções de Genebra e a própria Declaração Universal dos Direitos Humanos (DUDH). O artigo 4.º da DUDH determina que “Ninguém será submetido a tortura nem a tratamentos cruéis, desumanos ou degradantes”. Por sua vez, o artigo 3.º, comum às quatro Convenções de Genebra, e aplicável também a conflitos armados não internacionais, proíbe os assassinatos, mutilações, bem como a tortura, tratamento cruel, humilhante e degradante dos prisioneiros. No que respeita à detenção por período indeterminado, transcreve-se seguidamente o n.º 1 do artigo 11.º da DUDH: “Toda a pessoa acusada de um ato delituoso presume-se inocente até que a sua culpabilidade fique legalmente provada no decurso de um processo público em que todas as garantias necessárias de defesa lhe sejam

21 A primeira notícia veio a lume em 2004, com a divulgação, pelo *The New York Times*, de um relatório confidencial do Comité Internacional da Cruz Vermelha sobre as condições de tratamento dos detidos nessa prisão (Lewis, 2004).

asseguradas". Pode concluir-se facilmente que os direitos, liberdades e garantias não estão a ser devidamente respeitados, como seria suposto no seio de um Estado de Direito.

O segundo caso relaciona-se com o uso de veículos aéreos não tripulados – *unmanned aerial vehicles* –, vulgarmente designados por *drones*, para fins militares²². Em particular, estes veículos são utilizados na chamada guerra contra o terrorismo. No contexto militar, a utilização destes veículos é polémica²³. São frequentemente utilizados para proceder a execuções de combatentes enquanto estes não estão a lutar e não estão, assim, a participar nas hostilidades. São ainda frequentemente utilizados para executar civis que não pertencem às forças armadas do Estado ou da força adversária e que participam, por vezes, nas hostilidades, sendo também executados quando não estão a participar nas hostilidades. A estas utilizações, já controversas, acrescem os relatos de mortes de civis que nunca participaram das hostilidades e que são assumidas como danos colaterais.

Verifica-se, uma vez mais, a violação de princípios e regras vigentes num Estado de Direito. O quadro legal aplicável aos conflitos armados é mais permissivo do que aquele que vigora em tempos de paz, nomeadamente ao permitir a execução de quem esteja envolvido nas hostilidades. No entanto, ainda que seja duvidosa a aplicação do quadro legal destinado aos conflitos armados num contexto de luta contra o terrorismo, as Convenções de Genebra não só proibem o ataque contra civis que não participem nas hostilidades, como preveem que o inimigo fora de combate não deva ser objeto de um ataque – artigos 41.º e 42.º do Protocolo Adicional I às Convenções de Genebra. Nos casos em que os veículos aéreos não tripulados sejam utilizados nos termos acima descritos, verifica-se uma violação dos compromissos assumidos internacionalmente. Fora do quadro legal aplicável aos conflitos armados, a violação do Direito Internacional é ainda mais evidente, nomeadamente a violação dos compromissos assumidos na DUDH, a qual acresce à violação das normas jurídicas nacionais que consagram direitos, liberdades e garantias.

22 Sobre este tema, veja-se, por exemplo, o relatório elaborado em 2018 pelo grupo de trabalho parlamentar do Reino Unido sobre o uso de veículos aéreos não tripulados para fins militares, intitulado *The UK's Use of Armed Drones: Working with Partners* (APPG, 2018). Este relatório aborda algumas das fragilidades do uso destes veículos no contexto militar e, em particular, os riscos para a violação de compromissos internacionais, relacionados com direitos humanos.

23 Entre as várias vozes que se têm erguido contra a utilização dos veículos aéreos não tripulados para fins militares, destaca-se a do Relator Especial das Nações Unidas para execuções extrajudiciais, sumárias ou arbitrárias. Em 2009, este relator, Philip Alston, apresentou um relatório junto da Assembleia Geral das Nações Unidas que sustentava que a utilização daqueles veículos para fins de execução constituía uma clara violação do Direito Internacional, que apenas poderia ser evitada se fossem implementados mecanismos que, entre outros fins, visassem a responsabilização pelos atos cometidos através desses veículos (UN News, 2009).

O terceiro caso relaciona-se com o desenvolvimento e gestão de programas de vigilância das comunicações que abrangem indiscriminadamente militares e civis, em contextos quer de guerra, quer de paz. Estes programas são desenvolvidos sob o argumento de garantir a segurança dos Estados e de, em particular, combater o terrorismo. Como exemplos destes programas de vigilância, podem apontar-se o ECHELON²⁴, bem como, mais recentemente, o PRISM²⁵. Estes programas efetuam a interceção de comunicações e, por esta forma, o tratamento de dados pessoais de milhões de cidadãos, sem o seu consentimento ou sequer conhecimento, representando, assim, uma clara restrição do seu direito à privacidade ou, quando autonomizado, do seu direito à proteção de dados pessoais.

Poderia pensar-se que estes programas de vigilância das comunicações violam diretamente os diplomas legais da União Europeia que protegem os dados pessoais, uma vez que estes diplomas legais têm vindo a ter uma grande projeção mediática e são normalmente invocados neste tipo de cenários. Contudo, uma leitura atenta destes diplomas legais revela que os mesmos não são aplicáveis a situações como as que se visam cobrir com estes programas de vigilância. Em particular, a anterior Diretiva da União Europeia relativa à proteção da privacidade e dos dados pessoais, bem como o atual Regulamento Geral sobre a Proteção de Dados²⁶,

24 O ECHELON consiste num sistema de vigilância electrónica desenvolvido pelo Reino Unido, Estados Unidos da América, Canadá, Austrália e Nova Zelândia, que atuava mediante a interceção de comunicações privadas e que se distingue pela sua enorme capacidade de atuação. De acordo com o Relatório do Parlamento Europeu, de 11 de julho de 2001, sobre a existência de um sistema global de interceção de comunicações privadas e económicas, “O sistema designado por “ECHELON” distingue-se dos outros sistemas de informação pelo facto de apresentar duas características destinadas a conferir-lhe um nível de qualidade muito específico. / A primeira característica que lhe é atribuída é a capacidade praticamente global de vigilância. Recorrendo principalmente a estações receptoras via satélite e a satélites de espionagem, será possível interceptar qualquer comunicação via telefone, telefax, Internet ou e-mail, emitida seja por quem for, de molde a aceder ao respectivo conteúdo. / A segunda característica apontada ao ECHELON é o facto de o sistema funcionar a nível mundial graças a uma cooperação entre vários países (...) o que representa uma mais-valia relativamente a sistemas nacionais...” (Parlamento Europeu, 2001, pp. 24-25).

25 O PRISM consiste num programa desenvolvido pelos Estados Unidos da América de recolha e tratamento de dados de grande abrangência, cujo conhecimento resultou, entre outras fontes, das revelações de Edward Snowden, um antigo funcionário da National Security Agency (NSA), em 2014. A revelação da existência deste programa resultou numa forte reação por parte do Parlamento Europeu – veja-se o relatório European Parliament (2014). O Grupo de Trabalho do Artigo 29 também emitiu um documento sobre este tópico – veja-se o documento European Commission (2014). Sobre este tema, veja-se ainda Edgar (2017).

26 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

excluem a sua aplicação às atividades relacionadas com a defesa e segurança do Estado²⁷. Nos casos em que estas atividades pudessem estar cobertas pelo quadro legal, estes instrumentos jurídicos admitem igualmente o afastamento de algumas das suas previsões com vista a garantir a defesa e a segurança do Estado²⁸.

Os referidos programas de vigilância violam, porém, outras disposições legais, nacionais, regionais e internacionais, que consagram o respeito pela privacidade e a proteção de dados pessoais. Estes direitos encontram-se consagrados, por exemplo, nos artigos 26.º, 34.º e 35.º da Constituição da República Portuguesa, nos artigos 7.º, 8.º e 11.º da Carta dos Direitos Fundamentais da União Europeia ou ainda no artigo 12.º da DUDH. Estes direitos poderão ser restringidos, desde que a restrição seja necessária, adequada e proporcional para o respeito de interesses públicos relevantes ou para proteger os direitos e liberdades de outros. Contudo, a restrição operada pelos descritos programas de vigilância é indubitavelmente desproporcionada, uma vez que estes programas procedem à interceção de comunicações de forma indiscriminada, abrangendo todas as pessoas, independentemente de estas constituírem ou não uma ameaça para a defesa e a segurança dos Estados²⁹.

Nos três casos descritos, os Estados adotam posições que se destinam essencialmente a fazer face ao terrorismo, quer na detenção dos suspeitos da sua prática, quer na execução desses suspeitos, quer ainda na interceção de comunicações com vista a prevenir ou reprimir essa prática. A questão central que se deve colocar

27 Vejam-se os seus considerandos 16 e 19, bem como o artigo 2.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados. A revogada Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, continha esta exclusão ou limitação nos considerandos 13, 16 e 43, bem como no artigo 3.º, n.º 2.

28 Veja-se o artigo 23.º, n.º 1, do Regulamento Geral sobre a Proteção de Dados, bem como o artigo 13.º, n.º 1, da revogada Diretiva 95/46/CE.

29 Esta desproporcionalidade já foi declarada noutra sede, em situações similares, a propósito das legislações que permitem a retenção indiscriminada de dados de comunicações para fins de investigação de crimes graves. O Tribunal de Justiça da União Europeia invocou esta desproporcionalidade no processo que conduziu à declaração de invalidade da Diretiva de Retenção de Dados – Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações –, no âmbito do Acórdão proferido em 8 de abril 2014 nos processos apensos C-293/12 e C-594/12 (EU:C:2014:238, n.º 52). O Tribunal de Justiça da União Europeia invocou novamente esta desproporcionalidade no processo que concluiu no sentido da desconformidade das legislações nacionais de retenção de dados com a Carta dos Direitos Fundamentais da União Europeia nos casos de essas legislações prevejam a retenção de dados de comunicações de uma forma geral e indiscriminada, que abranja os dados de tráfego de todos os utilizadores de serviços de comunicações, no âmbito do Acórdão proferido em 21 dezembro 2016 nos processos apensos C-203/15 e C-698/15 (EU:C:2016:970).

perante estes casos é a de saber se, para combater o terrorismo, não estarão os Estados, com esta atuação, a destruir o próprio Estado de Direito e a abrir mão dos valores que muitas vezes esse terrorismo pretende desfazer.

O Estado de Direito deve atuar como garante dos cidadãos e impor limites à forma como os Estados atuam, ainda que estes estejam a atuar com o objetivo de neutralizar as ameaças a estes mesmos Estados ou ao Estado de Direito. Mesmo nestas circunstâncias, os limites que caracterizam o Estado de Direito devem ser observados. Sem a observância dos limites que caracterizam o Estado de Direito, este já não existirá.

Os critérios de definição de quais sejam os limites a impor decorrem de mecanismos previstos pelo Estado de Direito, como o princípio da proporcionalidade. De acordo com este princípio, é possível restringir direitos fundamentais se esta restrição for adequada e imprescindível para ir ao encontro de interesses públicos relevantes ou para proteger os direitos fundamentais de outros³⁰. A restrição, porém, deve ser limitada ao estritamente necessário para alcançar estes outros fins. Adicionalmente, a legislação em causa deve ser precisa e clara quanto às restrições permitidas e providenciar meios que impeçam eventuais abusos. Estes critérios devem estar presentes em todos os momentos do combate ao terrorismo.

4. Reflexões Finais

O combate ao terrorismo é um dos mais difíceis que alguma vez tiveram lugar na história. O terrorismo não se circunscreve a uma zona geográfica, a um grupo de pessoas-pré-determinadas ou a um modo de atuação previsível. Devido ao seu impacto devastador no sentimento de segurança das populações, os atos de extrema violência que o caracterizam têm conduzido a uma profunda alteração da vida quotidiana no mundo ocidental. Para ilustrar esta alteração, basta referir o aumento do tempo e de recursos despendidos em procedimentos de segurança.

O combate ao terrorismo só tem sido possível com uma profunda alteração do quadro legal aplicável, que fixa crescentes atribuições e competências nessa matéria, reforça obrigações por parte dos operadores e, em especial, daqueles que prestam serviços essenciais ou operam infraestruturas críticas, regula novos poderes de supervisão nessa área e determina sanções para a inobservância das normas aplicáveis. O combate ao terrorismo faz-se, sobretudo, pelo incremento da segurança. Por sua vez, o incremento da segurança só pode concretizar-se pela ocupação de um espaço que estava antes destinado à liberdade, na sua aceção ampla. A restrição da liberdade é, assim, neste contexto inevitável e aceitável, na medida em que se torna necessária para garantir a própria subsistência do Estado de Direito.

Foi longa e dura a viagem histórica até se abraçarem as conquistas do Estado de Direito. No entanto, estas conquistas, pelos valores que transportam, de suprema-

³⁰ Veja-se, por exemplo, o artigo 52.º, n.º 1 da Carta dos Direitos Fundamentais da União Europeia.

cia do Direito e de proteção dos direitos fundamentais, entre outros, merecem empenho na sua defesa.

Nesta trajetória de robustecimento da segurança e restrição da liberdade não se pode, assim, perder de vista o ponto de partida que justifica esses robustecimento e restrição: a defesa do Estado de Direito. Por esta razão, nunca serão demais os mecanismos de monitorização constante dessa trajetória, para assegurar que se consegue alcançar, em cada momento, o melhor equilíbrio possível entre segurança e liberdade, sem comprometer os limites do Estado de Direito.

Os critérios de definição daquele que será o equilíbrio certo entre segurança e liberdade são complexos. Variam, desde, logo, em razão do contexto histórico. Alguns critérios são, contudo, fixados pelo próprio Estado de Direito, como o da observância do princípio da proporcionalidade. A liberdade só pode ser restringida na medida exata em que essa restrição seja imprescindível, adequada e necessária para proteger interesses públicos ou outros direitos dos cidadãos. A restrição deve limitar-se ao estritamente necessário para alcançar estes outros fins. A legislação que preveja estas restrições deve ser precisa e clara quanto à exata configuração dessas restrições e deve providenciar meios que impeçam eventuais abusos.

O controlo constante e apertado do Estado com vista a evitar abusos de poder é um dos bastiões definidores do Estado de Direito, como último reduto de proteção do cidadão perante o poder político. Os sentimentos de insegurança e de terror despoletados pelo terrorismo podem fazer perder de vista este bastião. No calor do combate, é fácil baixar a guarda em relação ao próprio atacado, permitindo que este exceda na sua defesa. Se o próprio guardião do Estado de Direito, que é o Estado, não estiver a ser devidamente monitorizado, quem poderá garantir que os valores do Estado de Direito ainda estão a ser respeitados? Após o atrás exposto, cabe perguntar: no combate ao terrorismo, *quid custodiet ipsos custodes?*³¹

Referências Bibliográficas

All-Party Parliamentary Group (APPG), 2018. *The UK's Use of Armed Drones: Working with Partners* [pdf]. Report by the All-Party Parliamentary Group on Drones, July. London, House of Commons. Disponível em [website] https://www.bsg.ox.ac.uk/sites/default/files/2018-07/INH_PG_Drones_AllInOne_v25.pdf

Bodin, J., 2013. *Les Six Livres de la République/De Republica libri sex*, 1576, reimpressão. Paris: Classiques Garnier.

Chaliand, G. e Blin, A., dir., 2004. *Histoire du Terrorisme: de l'Antiquité a Al Qaida*. Paris: Bayard.

31 Veja-se a frase inicialmente transcrita, de Dwight David Eisenhower, que aqui de novo se recorda: "Because, therefore, we are defending a way of life, we must be respectful of that way of life as we proceed to the solution of our problem. We must not violate its principles and its precepts, and we must not destroy from within what we are trying to defend from without" – Dwight David Eisenhower, speech before NATO Council, 11/26/51 [DDE's Pre-Pres. Papers, Box 197].

- Dupuy, P.-M., 2004. State Sponsors of Terrorism: Issues of Responsibility. In Andrea Bianchi, ed., *Enforcing International Law Norms against Terrorism*. Studies in International Law. Londres: Hart Publishing.
- Edgar, T. H., 2017. *Beyond Snowden: Privacy, Mass Surveillance and the Struggle to Reform the NSA*. Washington: Brookings Institution Press.
- European Commission, 2014. *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, 819/14/EN WP 215. Article 29 Data Protection Working Party, adotado em 10 de abril, Bruxelas. Disponível em European Commission [website] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf
- European Parliament, 2014. *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, A7-0139/2014 EN. Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, 21 de fevereiro. Disponível em European Parliament [website] <https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//EN>
- Greene, A., 2017. Defining terrorism: one size fits all? *International and Comparative Law Quarterly*, 66(2), pp. 411-440.
- Jellinek, G., 2005. *Teoria General del Estado*. Buenos Aires: Editorial B de f.
- Juncker, J.-C., 2017. *President Jean-Claude Juncker's State of the Union Address 2017*, SPEECH/17/3165, 13 de setembro, Bruxelas. Disponível em http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm
- Kant, I., 1988. Que é o iluminismo? In Kant, I., *A Paz Perpétua e outros Opúsculos*, trad. de Artur Mourão. Lisboa: Edições 70.
- Lewis, N. A., 2004. Red Cross Finds Detainee Abuse in Guantánamo. *The New York Times* [em linha], 30 de novembro. Disponível em: <https://www.nytimes.com/2004/11/30/politics/red-cross-finds-detainee-abuse-in-guantanamo.html>
- Miranda, J., 2014. *Manual de Direito Constitucional*, Tomo I, vol. 1. Coimbra: Coimbra Editora.
- Novais, J. R., *Direitos de Liberdade e Direitos Sociais na Constituição Portuguesa*, disponível em https://www.fd.unl.pt/docentes_docs/ma/jrn_ma_8782.doc
- Parlamento Europeu, 2001. *Relatório sobre a existência de um sistema global de interceção de comunicações privadas e económicas (sistema de interceção "ECHELON") (2001/2098 (INI))*, FINAL A5-0264/2001 PAR 1 PT. Comissão Temporária sobre o Sistema de Intereção ECHELON, Relator: Gerhard Schmid. Bruxelas, 11 de julho. Disponível em European Parliament [website] <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//PT>
- Schmid, A., 2004. Terrorism – the Definitional Problem, *Case Western Reserve Journal of International Law*, 36(2), pp. 375-419.
- UN News, 2009. UN rights expert voices concern over use of unmanned drones by United States. *UN News* [em linha], 28 de outubro. Disponível em: <https://news.un.org/en/story/2009/10/319502-un-rights-expert-voices-concern-over-use-unmanned-drones-united-states>
- Wojciechowski, S., 2009. Why is it so difficult to define terrorism? *Polish Political Science Yearbook*, Vol. XXXVIII, pp. 58-72.

Vigilância Vídeo, Intercepção Preventiva de Comunicações e Contraterrorismo

Júlio Pereira

Exerce atualmente funções de Procurador-Geral Adjunto no Supremo Tribunal de Justiça, tendo desempenhado, entre outros, o cargo de Diretor-Geral Adjunto do Serviço de Informações de Segurança, Diretor-Geral do Serviço de Estrangeiros e Fronteiras e Secretário-Geral do Sistema de Informações da República Portuguesa.

Resumo

Este artigo aborda a estratégia nacional de combate ao terrorismo nas suas múltiplas dimensões. É dado especial enfoque às questões relacionadas com a vigilância vídeo, intercepção preventiva de comunicações e contraterrorismo. Para o autor, a estratégia nacional corresponde, grosso modo, à estratégia europeia neste domínio. Como é sublinhado, o problema da videovigilância é sempre o do equilíbrio entre o valor da segurança e o respeito pelos direitos constitucionais, particularmente no que respeita ao direito à privacidade e direito à imagem.

Abstract

Video Surveillance, Preventive Interception of Communications and Counterterrorism

This article addresses the national counter-terrorism strategy in its multiple dimensions. Particular focus is given to issues related to video surveillance, preventive interception of communications and counterterrorism. For the author, the national strategy corresponds to the European strategy in this area. As is emphasized, the problem of video surveillance is always that of the balance between the value of security and respect for constitutional rights, particularly with regard to the right to privacy and the right to image.

A Estratégia Nacional de Combate ao Terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 7-A/2015, de 20 de fevereiro, aponta como objetivos estratégicos detetar, prevenir, proteger, perseguir e responder, assim procurando combater o terrorismo em todas as suas manifestações:

- Detetar, identificando precocemente potenciais ameaças terroristas, mediante a aquisição do conhecimento essencial para um combate eficaz, tanto na perspetiva do seu desmantelamento isolado, quanto da deteção de outros focos de ação terrorista. A recolha, tratamento e análise de dados e informações e a sua disponibilização recíproca entre entidades responsáveis neste domínio, no território nacional e no estrangeiro, permite antecipar o conhecimento e a avaliação de ofensivas em preparação.
- Prevenir, conhecendo e identificando as causas que determinam o surgimento de processos de radicalização, de recrutamento e de atos terroristas. O domínio dos factos que potenciam a sua expansão permite a adoção de medidas que obstem ao seu surgimento e desenvolvimento.
- Proteger, fortalecendo a segurança dos alvos prioritários, reduzindo quer a sua vulnerabilidade, quer o impacto de potenciais ameaças terroristas. A proteção concretiza-se no aumento da segurança das pessoas, das fronteiras, da circulação de capitais, das mercadorias, dos transportes, da energia e das infraestruturas críticas, nacionais e ou europeias.
- Perseguir, desmantelando ou neutralizando as iniciativas terroristas, projetadas ou em execução, e as suas redes de apoio, impedindo as deslocações e as comunicações e o acesso ao financiamento e aos materiais utilizáveis em atentados e submetendo os fenómenos terroristas à ação da justiça.
- Responder, gerindo operacionalmente todos os meios a utilizar na reação a ocorrências terroristas. A capacidade de resposta permite limitar as suas consequências, quer ao nível humano, quer ao nível das infraestruturas. A resposta incide ainda na assistência, tendo em consideração as necessidades especiais das vítimas e das testemunhas.

O mesmo documento indica como linhas de ação para prossecução do primeiro objetivo estratégico (detetar), entre outras as seguintes:

- Robustecer as estruturas responsáveis pela produção e coordenação e partilha de informações relevantes na identificação da ameaça terrorista;
- Reforçar os meios de produção, tratamento e análise de informações.

Por esta breve alusão aos objetivos estratégicos e algumas das respetivas linhas de ação é desde logo possível verificar a importância quer da videovigilância quer da intervenção preventiva de comunicações no prosseguimento da estratégia nacional de combate ao terrorismo, nomeadamente no que diz respeito à proteção das pessoas e das infraestruturas críticas e na capacidade de resposta no caso de um incidente terrorista.

A estratégia nacional corresponde *grosso modo* à estratégia europeia neste mesmo domínio, se bem que entre nós, no que diz respeito à prevenção, se tenha operado um desdobramento para dois objetivos estratégicos: por um lado a deteção e por outro a prevenção. Não creio que tenha havido nisso qualquer vantagem e receio mesmo que isso se tenha ficado a dever a uma mais fácil e menos quezilenta repartição de competências entre forças e serviços de segurança, na concretização de cada um dos pilares da estratégia. Falo assim por ter na memória o conturbado processo que levou à aprovação do plano de coordenação, controlo e comando operacional das forças e serviços de segurança, que se arrastou durante anos, precisamente por causa das disputas corporativas em matéria de competências, particularmente no que diz respeito à gestão dos incidentes tático-policiais, que viriam a ser ultrapassadas pela perspetiva da criação do cargo de secretário-geral do sistema de segurança interna e por uma postura mais assertiva do então responsável da tutela. No conjunto das medidas que um pouco por todo o mundo foram sendo adotadas em matéria de contraterrorismo, destaca-se o reforço de capacidades e de meios dos serviços de informações e a partilha de informações entre forças e serviço de segurança, tanto a nível nacional como no plano internacional. É verdadeiramente impressionante o avanço que neste domínio se fez sentir, particularmente no âmbito internacional, já que a temática das informações foi sempre encarada como matéria de soberania sujeita a especiais medidas de sigilo e a cooperação só existia no âmbito de questões pontuais e específicas e entre países que partilhavam interesses convergentes ou de manifesta proximidade.

Quando Portugal, em fins dos anos 90, por iniciativa do então diretor do Serviço de Informações de Segurança (SIS), Dr. Rui Pereira, propunha a criação de uma Eurointel, um serviço de informações de segurança interna dos países da União Europeia, a proposta foi encarada com espanto e manifesta animosidade. Todavia, com os acontecimentos de 11 de Setembro, subsequentes atentados de Madrid e Londres e posterior disseminação do terrorismo jihadista o realismo apoderou-se das mentes dos líderes americanos e europeus e hoje, para além de um INTCEN – EU Intelligence and Situation Centre –, que produz informação de natureza estratégica no âmbito da Comissão Europeia, temos um grupo de contraterrorismo no seio do Clube de Berna – organização informal que reúne representantes dos serviços internos de Estados-membros da União Europeia – e ainda uma estrutura sedeadada em Haia, que partilha em tempo real informação sobre ameaças e atentados terroristas, na qual estão representados todos os serviços internos dos países da UE, que constitui uma verdadeira unidade europeia de prevenção e combate ao terrorismo.

No que diz respeito aos meios e capacidades dos serviços registou-se uma evolução semelhante. Os serviços, muito centrados durante o período da Guerra Fria nas questões associadas ao conflito leste/oeste, particularmente na espionagem e ameaças terroristas de cariz ideológico e independentista, que na generalidade dos

casos espelhavam também esse conflito, foram perdendo terreno e chegou mesmo a ser questionada a sua utilidade após a falência da União Soviética. Com a emergência do terrorismo de cariz islamista e quando a respetiva ação se fez sentir nos Estados Unidos e na Europa, ganharam necessariamente novo fôlego e rapidamente se reajustou o seu dispositivo para poderem enfrentar esta nova ameaça. Na generalidade dos países europeus foi alterada a sua estrutura, criaram-se instâncias de coordenação, alargaram-se os seus poderes e ampliaram-se os seus meios materiais e humanos.

Compreende-se a razão deste processo evolutivo. As ameaças deixaram de ser nacionais, luta-se contra um inimigo invisível e os caminhos que conduzem à realização de atentados são percorridos, em cerca de 90% do seu percurso, na penumbra ou na sombra. Neste contexto reconhece-se que o trabalho dos serviços de informações é essencial para se poder evitar, ou pelo menos para reduzir a ocorrência de atentados ou para limitar os respetivos efeitos.

Para chegar a esse inimigo invisível, é essencial a sua deteção nos meios onde desenvolve a sua ação preparatória, desde a fase de doutrinação, passando pela radicalização, recrutamento e treino e posterior preparação para a ação terrorista, o que implica um vasto conjunto de ações e de disponibilização de recursos, sendo indispensável uma grande cooperação no plano internacional, que passa essencialmente pela troca ampla e célere de informações e atividades operacionais conjuntas e, no plano nacional, por uma empenhada cooperação entre forças e serviços de segurança e também forças armadas, indispensável para acompanhar indivíduos, locais e comunidades de risco e detetar indícios técnicos que apontem para o envolvimento individual ou de grupos em atividades suspeitas.

As interceções de comunicações constituem, no elenco dos meios ao dispor das forças e serviços de segurança, imprescindíveis para tal finalidade. Até porque é no universo da internet, com a imensidão dos fornecedores desse serviço, com a possibilidade de ocultação e multiplicação de identidades e de recurso a redes de acesso condicionado ou interdito, que grande parte das coisas acontecem e em geral onde elas começam.

Cremos que em Portugal as polícias dispõem no plano legal de capacidades equivalentes ao que ocorre em grande parte dos países da União Europeia em matéria de videovigilância. Poderão não dispor dos mesmos meios em termos técnicos, dada a constante evolução da tecnologia e custos que lhe estão associados, mas no plano legal não sofrerão mais limitações do que em outros países do espaço europeu, até porque esta matéria tem o essencial das suas regras fixadas em instrumentos jurídicos da União Europeia.

O problema da videovigilância é sempre o do equilíbrio entre o valor da segurança e o respeito pelos direitos constitucionais, particularmente no que respeita ao direito à privacidade e direito à imagem. E este equilíbrio será cada vez mais difícil

à medida que se vão sofisticando os instrumentos de vigilância, designadamente com a maior capacidade de definição de imagem e o *software* que lhe está associado para reconhecimento de voz, reconhecimento facial e identificação pelos diversos elementos biométricos. Ou seja, quanto mais sofisticado o equipamento mais eficaz se torna para a respetiva finalidade mas simultaneamente maior é a sua capacidade de devassa e mais difícil é conciliar a videovigilância com os diversos direitos constitucionais que serve ou com que contende.

Deve dizer-se que não é unânime a opinião sobre a mais-valia da videovigilância, tanto em matéria de contraterrorismo como de prevenção da criminalidade comum. Se em geral se reconhece a sua eficácia, por exemplo na preservação dos centros urbanos contra ações de vandalismo, ou para a proteção de locais procurados para a prática de crimes por carecerem de vigilância ou mais afastados de instalações policiais, alude-se por outro lado ao facto de as câmaras de videovigilância empurrarem o crime para outros locais e até de estigmatizarem certas zonas. Há mesmo quem acuse o uso de câmaras de constituírem um fator de radicalização terrorista, nomeadamente quando direcionadas para a vigilância de certas comunidades étnicas ou religiosas. Há, no entanto, que reconhecer que a maioria destas críticas vem de sectores que privilegiam a proteção das liberdades individuais em detrimento do vetor segurança.

Vivemos hoje numa sociedade cada vez mais urbanizada, com uma enorme mobilidade de pessoas, provenientes das mais diversas origens, de todas etnias, professando diferentes confissões religiosas. Está definitivamente ultrapassado o tempo em que a rotina uniforme dos dias permitia assinalar qualquer situação anómala. Hoje encontramos-nos em permanência com pessoas diferentes, em diferentes contextos situacionais, tornando-se praticamente inviáveis os velhos mecanismos informais de controlo, muito assentes na cooperação dos próprios cidadãos. É agora impossível policiar uma grande cidade, todos os locais de concentração de pessoas, sem recurso a meios técnicos, nomeadamente videovigilância, que de forma ativa ou passiva auxiliem a polícia no desempenho das suas tarefas, nomeadamente de prevenção da criminalidade. Ora, se em matéria de segurança, a colaboração ativa dos cidadãos é indispensável, como de resto é reconhecido em diversos países com apelos à vigilância cidadã, como acontece em França ou, para dar um exemplo mais radical com a China, onde a lei da segurança nacional faz menção expressa a essa participação, isso já não basta. A configuração das cidades e o *modus vivendi* de hoje não permitem que o tradicional controlo informal opere de forma eficaz, podendo mesmo dar origem a lamentáveis equívocos que, em termos de ofensa aos direitos individuais, podem até ser mais lesivos do que os apontados excessos de qualquer programa de vigilância vídeo.

A eficácia da videovigilância no âmbito do contraterrorismo, começou a ser amplamente reconhecida por altura dos atentados de 2005 em Londres, já que permitiu

identificar os terroristas da primeira vaga de atentados e deter os que se preparavam para uma segunda. Foi também reconhecida nos atentados mais recentes, como nos atentados de Paris em 2015 e de Bruxelas em 2016, se bem que neste último caso as imagens divulgadas tenham sido um bônus oferecido aos terroristas, permitindo-lhes ver aquilo que deviam evitar em atentados subsequentes. Daí que as autoridades francesas tenham reforçado o seu dispositivo de videovigilância e o atentado de Berlim, de dezembro de 2016, tenha removido as reservas que existiam na Alemanha, de enveredar por caminho semelhante.

Na verdade, à medida que vão sendo recolhidos mais elementos sobre agentes da ameaça terrorista, se vai partilhando a informação a nível europeu e se vão desenvolvendo novos mecanismos para tratamento inteligente dos dados obtidos, registam-se novas capacidades de prevenção de atentados ou de contenção subsequente dos respetivos efeitos.

Pelo que sei, a videovigilância em Portugal tem obtido resultados positivos, constituindo fator não negligenciável de redução da criminalidade urbana. Felizmente não temos tido oportunidade de avaliar as suas potencialidades na prevenção do terrorismo mas, não estando nós imunes a uma possível ocorrência dessa natureza, podemos pelo menos considerar que a sua importância não será menor do que a que tem tido em países que até agora têm sido fustigados pelo fenómeno.

Um outro fator importante a ter em conta é o contributo da videovigilância para o sentimento de segurança das populações. Não obstante as cautelas e as preocupações quanto ao uso deste meio de prevenção, a verdade é que a população, em toda a Europa, é favorável ao seu uso e sente-se mais segura com a sua utilização. Ora o sentimento de segurança é um importantíssimo fator de paz social. O sentimento de insegurança gera intranquilidade e em alguns países tem até contribuído para um desvio rumo a políticas não democráticas porque a segurança, não sendo o direito mais importante, é o palco onde se exercem todos os outros direitos. E é até mais relevante, mais impactante o sentimento de segurança do que real situação de segurança. Uma sociedade é mais tranquila se nela prevalecer a ideia entre as pessoas de que estão seguras, ainda que a real situação não lhe corresponda exatamente, do que, apesar de objetivamente desfrutar de um bom clima de segurança nela prevalecer um sentimento de insegurança. Nestas circunstâncias, a sociedade sofre daquilo que eu costumo designar por hipocondria securitária, que Kafka ilustrou magistralmente no seu conto “A toca”.

Por outro lado e numa sociedade democrática, onde as forças e serviços de segurança atuam em conformidade com a constituição e a lei, os procedimentos de segurança acrescentam liberdade. Nos países fustigados pelo terrorismo e até pela criminalidade comum, em que as pessoas têm receio de frequentar determinadas zonas, de viajar para certos locais, elas sofrem uma efetiva restrição da liberdade. O habitante de uma grande cidade que a certas horas da noite não entra em deter-

minadas linhas do metropolitano, ou em certos bairros chama um táxi para se deslocar por escassas centenas de metros, vê reduzida a sua liberdade, só que não percebe esse facto como tal. Para ele é apenas insegurança. Mas não, é efetiva restrição da liberdade. Ou seja, a segurança acrescenta liberdade.

Se as polícias estão dotadas de meios legais condizentes com as necessidades da sua atuação no plano da prevenção da criminalidade, já o mesmo se não pode dizer relativamente aos serviços de informações que, agindo numa fase precoce, de prevenção antecipada, quando ainda não há elementos que permitam o início de uma investigação criminal, no âmbito da qual os órgãos de polícia criminal, com permissão da autoridade judiciária competente podem recorrer a meios intrusivos, têm que agir no maior sigilo. E aí, os instrumentos legais existentes, não estão manifestamente à altura das necessidades, nomeadamente para controlo de alvos determinados.

A Lei n.º 1/2005, de 10 de janeiro, regula a utilização de sistemas de vigilância por câmaras de vídeo pelas Forças e Serviços de Segurança em locais públicos de utilização comum, para captação e gravação de imagem e som. Um dos fins para que pode ser autorizada é a prevenção de atos terroristas – art.º 2.º, n.º 1 alínea e).

A instalação de câmaras fixas está sujeita a autorização do membro do governo que tutela a FSS – art.º 3.º, n.º 1 – precedida de parecer da Comissão Nacional de Proteção de Dados – art.º 3.º, n.º 2 – e, os locais objeto de vigilância é obrigatória a afixação, em local bem visível, de informação da existência e localização das câmaras, finalidade da captação da imagem e som, responsável pelo tratamento de dados e direitos de acesso e retificação que podem ser exercidos – art.º 4.º.

Um diploma com esta norma está talhado para a prevenção da criminalidade comum. Não tem sentido no âmbito da prevenção do terrorismo.

No que diz respeito à interceção de comunicações a situação portuguesa, no que concerne aos serviços de informações é deplorável, constituindo Portugal um fator de vulnerabilidade do Espaço Schengen. É o único país desse espaço que veda essa possibilidade aos serviços. Sem interceção de comunicações a prevenção do terrorismo chegará tarde de mais. Dificilmente se compreende que no âmbito da investigação criminal tal seja possível e que esse procedimento esteja banido para efeitos de prevenção, o que revela maior empenho na punição do delincente do que na proteção das vítimas.

Diz-se que o problema decorre de limitações de ordem constitucional porquanto, nos termos do art.º 34.º, n.º 4 da Constituição da República Portuguesa “É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal”. Porém, mais do que na norma, pode o problema situar-se na amplitude com que a mesma tem sido interpretada. Havendo boas razões para se entender que esta norma foi pensada tendo em vista o conteúdo das comunica-

ções, confiou-se na possibilidade de dela se fazer uma interpretação que a isso a reconduzisse, dados os riscos associados ao terrorismo, à espionagem e criminalidade altamente organizada.

Foi por isso ensaiada a possibilidade de dar aos serviços de informações o poder “de aceder aos dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar ou identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização” e nesse sentido foi aprovado na Assembleia da República, por larga maioria, o Decreto n.º 426/XII. Era uma inovação tímida, que dava essa possibilidade para fins determinados e desde que autorizada por uma comissão constituída por três juizes do Supremo Tribunal de Justiça, designados pelo seu Presidente.

O diploma foi sujeito pelo Presidente da República a fiscalização preventiva e a norma em causa foi considerada inconstitucional.

Portugal não tem lições a dar, em matéria de proteção dos direitos fundamentais, à generalidade dos países democráticos, onde a interceção preventiva de comunicações, em termos muito mais amplos do que os previstos na norma constitucionalmente vetada, era permitida. Ainda assim o Tribunal Constitucional, com um esclarecido voto de vencido, pronunciou-se pela inconstitucionalidade.

Pode apontar-se para isso uma boa razão: Portugal tem sido imune aos atentados terroristas que têm afligido outros países da Europa e o grau de ameaça não tem ultrapassado o nível moderado. De facto, têm sido os atentados e os graus de ameaça que têm impulsionado a produção de legislação mais intrusiva neste domínio, como aconteceu por exemplo nos Estados Unidos ou com a França. Ou seja, não é apenas em Portugal que neste domínio tem prevalecido uma atitude reativa. Também em outros países as coisas evoluíram não por força da razão mas por impulso das bombas e do sangue das vítimas. Só que nesses outros países o que tem estado em causa não é a atribuição de poderes, como em Portugal, mas a sua ampliação.

Ora, não obstante a situação de risco moderado que temos tido em Portugal, há alguns sinais que merecem a devida atenção, designadamente alguns sinais de radicalização, casos de recrutamento para a militância terrorista e a possibilidade de vinda para Portugal de soldados de Alá, portugueses ou com ligações a Portugal e ainda outros que com eles se relacionaram.

Deparamo-nos também com um trauma que ainda não foi ultrapassado e que gera um sentimento de recusa num determinado espetro político, em conferir estes meios aos serviços de informações, sugerindo-se mesmo que seria de alargar os poderes da Polícia Judiciária por forma a abarcar a possibilidade de recurso a esse meio com vista à produção de informações. Todavia esta posição afronta a matriz do sistema de informações que foi estruturado com vista a uma separação nítida entre a atividade de polícia e a atividade de informações. O nosso legislador preten-

deu evitar a criação de polícia de informações, que era o paradigma existente até 25 de abril de 1974.

Próxima desta razão há uma outra que se prende com um alargamento progressivo da judicialização da atividade de segurança interna, aliada a um também alargamento do conceito de prevenção criminal o qual, no entendimento de alguns, poderia abranger a produção de informações no domínio do contraterrorismo, a cargo da Polícia Judiciária como órgão competente na investigação e prevenção dos crimes de terrorismo, sob supervisão do Ministério Público. Resulta esta posição, como disse, de um conceito alargado de prevenção criminal, que sob o ponto de vista da proteção dos direitos das pessoas é positivo mas que desequilibra em excesso a relação com o vetor segurança e gera o risco de tomada de assalto de competências de segurança interna, que não cabem nem ao Ministério Público nem em exclusivo à Polícia Judiciária.

Finalmente há que registar uma tendência para reconduzir a atividade de informações ao paradigma do processo penal e centrar a proteção dos direitos fundamentais em entidades judiciais ou de natureza judicial.

Não obstante todas estas dificuldades a possibilidade de acesso aos dados de tráfego foi consagrada na Lei Orgânica n.º 4/17, de 25 de agosto, embora num contexto excessivamente burocrático que não se sabe se alguma vez irá funcionar. No que diz respeito ao acesso a dados de tráfego os mesmos terão que se destinar exclusivamente à prevenção de atos de espionagem e terrorismo e a violação das disposições previstas nesta lei geram sanções criminais agravadas.

É efetuado um controlo judicial dos pedidos, por uma entidade constituída pelos presidentes das secções criminais do Supremo Tribunal de Justiça e por um conselheiro designado pelo Conselho Superior da Magistratura, entidade que é também a que autoriza. O pedido é dirigido pelo Secretário-Geral do Sistema de Informações da República Portuguesa à comissão judicial, com conhecimento ao Procurador-Geral da República e, uma vez dada autorização, a mesma pode ser cancelada em qualquer momento por esta entidade, que tem competência para fiscalizar a sua execução, poderes de fiscalização que competem também à Comissão de Fiscalização de Dados e ao Conselho de Fiscalização do Sistema de Informações da República Portuguesa.

As possibilidades de este regime merecer o aval do Tribunal Constitucional são escassas dados os precedentes acima mencionados. Tudo aponta no sentido de que, em matéria de meios de prevenção do terrorismo continuaremos a estar orgulhosamente sós, exibindo a bandeira de elo mais vulnerável do Espaço Schengen.

Terrorismo e Propaganda nos *Media*

Hugo Franco

Licenciado em Ciências de Comunicação no ISCSP. Jornalista do Expresso da secção de Sociedade e coautor do livro Os Jiadistas Portugueses. Escreve habitualmente sobre segurança, crime e terrorismo.

Resumo

Realizar a cobertura jornalística de atentados terroristas requer um especial bom senso por parte dos profissionais dos *media*. Sobretudo para não causar alarme social e poupar as vítimas desses ataques a um duplo sofrimento: o do atentado e o de serem expostas na comunicação social. No entanto, em quase todos os ataques jornais e televisões cometem erros grosseiros e inadvertidos, mas também de uma forma consciente. Esses erros podem explicar-se em parte pela urgência em dar um exclusivo em primeira mão antes da concorrência, ou simplesmente porque existe a necessidade de fazer aumentar as audiências a todo o custo. Este artigo conta alguns casos-estudo passados no estrangeiro, sobretudo em França, país que tem sido alvo de vários ataques de cariz jihadista nos últimos anos. E, paralelamente, usa a experiência adquirida pelo autor no jornal *Expresso* nos últimos anos, nestes dossiers delicados e o *modus operandi* utilizado pelo semanário nas questões ligadas ao terrorismo.

Abstract

Terrorism and Propaganda in the Media

Carrying out the journalistic coverage of terrorist attacks requires a special common sense from the media's professionals. Especially not to cause social alarm and spare the victims of these attacks to double suffering: that of the attack and of being exposed in the media. However, in almost all attacks, newspapers and televisions make huge and inadvertent mistakes, but also in a conscious way. These errors can be explained in part by the urgency of giving a first-hand exclusive before the competition, or simply because there is a need to increase audiences at all costs. This article tells a few case-studies spent abroad, especially in France, a country that has been the target of several jihadist attacks in recent years. And, in parallel, this work uses the experience acquired by the author on the Expresso in the last years, in these delicate dossiers and the modus operandi used by the weekly newspaper on these terrorism-related issues.

Introdução

Os últimos quatro anos puseram à prova as redações de todo o mundo e Portugal não foi exceção. O aparecimento meteórico do autodenominado Estado Islâmico, ou Daesh, e as novas formas de propaganda do grupo jihadista que se implantou em poucos meses na Síria e no Iraque, em 2014, vieram desafiar os jornalistas que cobrem os assuntos de segurança e terrorismo. De repente surgiam nas redes sociais homens de cara tapada a realizar execuções no deserto a vítimas indefesas, vestidas com uniformes cor de laranja. Mais recentemente, seguimos os atentados que se multiplicaram por toda a Europa, sobretudo após o ataque à redação do jornal satírico francês *Charlie Hebdo*, no início de 2015. O Daesh definha neste momento, por isso creio ser esta a altura certa de recordar o que os *media* fizeram de bem, e menos bem, em relação à cobertura jornalística a uma das organizações terroristas mais tenebrosas que o mundo já conheceu.

Propaganda dos Jihadistas Portugueses

Escrevo sobretudo sobre a experiência pessoal que vivi com alguns colegas da redação do *Expresso*, o jornal onde trabalho há doze anos. Algures em março de 2014, o país recebeu a informação dos serviços de informações portuguesas, através de mais um *Relatório Anual de Segurança Interna*, publicado pelo Gabinete do Secretário-Geral do Sistema de Segurança Interna (GSG SSI), de que havia cidadãos nascidos em Portugal ou com ascendência portuguesa que se tinham juntado a grupos islamitas que lutavam na Síria. O documento não trazia muitos pormenores sobre o fenómeno, mas estava lá tudo o que era necessário para iniciarmos uma investigação jornalística que quatro anos depois ainda está longe de ser totalmente desvendada.

Quando uma fonte nos revelou que deveríamos procurar o apelido “Al Andaluz” nas redes sociais, apercebemo-nos que aquela era a melhor dica que poderíamos ter recebido. No Twitter, mas sobretudo no Facebook, abundavam as páginas de indivíduos com aquele apelido ou *nickname*. Sorridentes, e quase sempre de cara parcialmente tapada, mostravam-nos dezenas de fotografias com armas de guerra em punho, no meio de cenários inóspitos, acompanhadas por comentários em inglês, árabe, mas também em português. Faziam aquilo a que designamos de apologia ao terrorismo, convidando outros rapazes e raparigas a juntarem-se a eles no Califado, espécie de paraíso na Terra. Sabíamos pouco sobre eles, mas era nos comentários de amigos e familiares que surgiam as principais pistas que íamos seguindo como cães de fila.

Descobrimos que moravam na Linha de Sintra e depressa soubemos que tinham estado em Leyton e Walthamstow, zona oriental e norte de Londres. Seguimos sobretudo este grupo de seis rapazes e fomos por duas vezes à capital britânica conhecer as influências e razões que os terão levado de uma vida não muito dife-

rente de tantos nós para uma guerra longínqua na Síria. Um irmão de dois deles, que continua a viver em Londres, levando uma vida do lado certo da lei, explicou-nos que os familiares tinham ido ter “com o verdadeiro Islão”. Não conseguimos acreditar naquelas palavras e prosseguimos a nossa investigação, paralelamente àquela que era, e é, realizada pelo Serviço de Informações e Segurança (SIS), pela Unidade Nacional de Contra Terrorismo (UNCT) da Polícia Judiciária, pelo Serviço de Estrangeiros e Fronteiras (SEF) e também pela PSP e GNR.

Olhando agora para os primeiros artigos que publicámos sobre este tema no *Expresso*, é fácil verificar que fomos cautelosos, embora não isentos de erros. Era um terreno ainda virgem por explorar, e feito com avanços e recuos. Recordo-me de uma reunião com editores e diretores, em que foi decidido não revelar ao público os nomes completos dos jihadistas, nem os rostos descobertos. Um exemplo? O já internacionalmente conhecido Nero Saraiva era referido apenas como “Patrício”, um dos nomes do meio. Proteger a identidade daqueles rapazes e raparigas saídos da escola para a *Jihad* era naquela altura uma prioridade para nós. As famílias não tinham culpa das suas más escolhas de vida. Também as moradas, principalmente em Portugal, eram arredondadas. Assim, um prédio em Massamá passava a ser um prédio na Linha de Sintra.

O objetivo era nobre. Não é por acaso que ainda hoje, mesmo com todas as falhas que lhe possam ser apontadas, o *Expresso* é apelidado de “jornal de referência”. Mas previsivelmente não iria resultar durante muito tempo.

A primeira machadada veio do Reino Unido. Um dos irmãos, Rodrigues da Costa, divulgou um vídeo de propaganda em abril de 2014 em que apelava à *Jihad* global. Apesar de estar de cara tapada, os serviços de informações aperceberam-se de um sotaque característico da comunidade lusófona que reside naquele país. Uma fonte revelou-nos a identidade do jihadista, informação que acabámos por partilhar com um repórter inglês que nos havia ajudado na mesma matéria. Mas apesar dos nossos alertas de que não iríamos publicitar o nome do português, pedindo-lhe para fazer o mesmo, ele mandou o acordo informal às urtigas e publicou o nome completo num dos principais diários britânicos. O jornalismo tem destas histórias.

No mês seguinte foi a vez de um diário de cariz mais popular abrir uma fenda na nossa muralha: desconfiamos que uma fonte informal contactada por nós na altura tenha passado a informação. Não tenho certezas sobre o que afirmo, mas garanto não estar muito longe da verdade. Tal como referi há pouco, o jornalismo tem destas histórias.

Em poucos dias, Portugal inteiro ficava a saber os nomes, moradas, mãe, pais, tios e enteados do pequeno grupo de jihadistas portugueses. Não podíamos escamotear esse facto, e um pouco contra a nossa vontade acabámos também por publicar os nomes, sem, no entanto, ir a correr para as portas dos prédios em Massamá, Queluz

de Baixo ou de Mem Martins, como aconteceu com alguma da nossa concorrência. Esta foi a primeira fase da nossa ligação ao submundo jihadista. Onde seguimos todas as normas deontológicas, à risca. Volto a repetir, não isenta de erros.

Os Vídeos das Matanças no Deserto

No verão de 2014, a máquina de propaganda do autodenominado Estado Islâmico começou a ganhar pujança com a divulgação dos primeiros vídeos de produção *made in Hollywood*. As imagens das decapitações marcaram-nos a todos. Primeiro foram os jornalistas norte-americanos James Foley e Steven Sotloff, depois o inglês David Haines, funcionário de uma organização humanitária. Seguiram-se outros igualmente repugnantes onde um carrasco vestido de negro e de cara tapada decapitava a vítima, ajoelhada num deserto com um uniforme laranja igual aos prisioneiros de Guantánamo. As imagens impactantes obrigaram todos os órgãos de comunicação social a tomarem medidas. Não me recordo de ter assistido à divulgação da decapitação, mas foram poucos os canais ou jornais que não emitiram ou publicaram *frames* dos vídeos.

O Estado Islâmico ganhava no terreno e na guerra da propaganda. Acredito que se fosse hoje, vendo um Daesh agonizante no Médio Oriente e uma Europa ferida depois de dezenas de ataques terroristas, muitas televisões e jornais não teriam publicado um só vídeo daquele ato tão vil e covarde. Basta comparar com um exemplo recente da divulgação de um vídeo que mostra uma suposta morte de Ronaldo e de Messi, olímpicamente ignorada pela esmagadora maioria dos *media* mundiais e nacionais. Mas na altura, tudo aquilo era novo, metia medo e colocava em causa o estilo de vida que defendíamos no Ocidente. Jihadi John e as suas torturas “Mensagens para a América” eram como um filme de *suspense*, mas com vítimas reais. Para qualquer jornalista era mais importante descobrir quem era o homem por detrás da máscara do que pensar uma, duas, três, quatro vezes antes de publicar e publicitar mais um vídeo de *marketing* terrorista.

Em relação ao *Expresso*, acredito que as falhas se deram mais nas edições digitais. Lembro-me de um ou dois exemplos de artigos que poderiam não ter sido publicados: um sobre uma ameaça feita nos habituais canais de propaganda de um atentado em Portugal e na Hungria, que felizmente nunca se veio a concretizar; outro sobre a identidade de um luso-luxemburguês que de cara semitapada terá sido o carrasco de mais uma execução do Estado Islâmico.

Aí, sejamos francos, falhámos todos nós, jornalistas, editores, diretores. Tenho a percepção clara de que se os *media* se tivessem organizado, como mais tarde fez a imprensa francesa depois do atentado de Nice, o Estado Islâmico não teria ganhado a mesma pujança na altura.

Estes são só alguns exemplos. Mas há vários estudos que o comprovam, com dados do passado recente.

É o caso do trabalho acadêmico *Terrorism and the Media: The Effect of US Television Coverage on Al-Qaeda Attacks*, de Michael Jetter (2017).

Analisando o período entre o ataque às torres gêmeas, em Nova Iorque, a 11 de Setembro de 2001 até ao final de 2015, o autor norte-americano conclui que a Al-Qaeda intensificava o número de atentados sempre que a cobertura televisiva à organização terrorista aumentava.

Havia uma relação causa-efeito – pior, um efeito de contágio – entre a quantidade de reportagens realizadas pelos quatro principais canais, CNN, NBC, CBS ou Fox News, e as bombas colocadas pelos terroristas. “Em média, cada minuto de cobertura sobre a Al-Qaeda num noticiário de 30 minutos encorajava um ataque adicional nos sete dias seguintes”, lê-se no relatório. Pelo contrário, os atentados quase desapareciam quando não era dada atenção às atividades terroristas.

Michael Jetter é um estudioso que conhece a dinâmica das redações norte-americanas. Tem a noção de que será difícil aplicar de cima para baixo, ou seja, dos governos para as redações, sanções para os *media* que continuem a fazer a cobertura noticiosa a organizações terroristas. É que uma restrição ou proibição vinda diretamente do governo poderia colocar facilmente em causa a liberdade de expressão. É por isso que o autor sugere aos jornalistas e diretores de informação dos principais canais dos EUA para repensarem a forma como é feita a cobertura jornalística dos atentados terroristas. E dá o exemplo dos suicídios, em que a comunicação social se autoimpôs em não divulgar para não encorajar os chamados *copycats*, os imitadores. Jetter (2017) conclui que, desde o 11 de Setembro, a Al-Qaeda recebeu mais atenção dos *media* norte-americanos do que a China e a Rússia juntas.

Cito outros estudos importantes sobre esta matéria, como o “Mainstream Media Propaganda Fuels and Fans the Flames of War”, de Joachim Hagopian (2015), republicado em 2017, já com dados sobre o ISIS.

E também o “Can a Copycat Effect be Observed in Terrorist Suicide Attacks?”, de Nicholas Farnham e Marieke Liem (2017).

União dos *Media* Contra o Terror

Voltemos à noite de festa na comemoração da Bastilha na Promenade des Anglais, em Nice. Às 22h40 de 14 de julho de 2016 e ao camião conduzido por Mohamed Bouhlel, um indivíduo de dupla nacionalidade francesa e tunisina, autor de crimes comuns não associados a redes terroristas. Todos sabem quase de cor o que aconteceu nos minutos seguintes. Os franceses voltavam a ser alvo de um grande atentado – depois de *Charlie Hebdo* e do Bataclã –, desta feita com um *modus operandi* que iria inspirar mais atentados nos meses seguintes, um pouco por toda a Europa. Era o chamado *do it yourself*, em que qualquer pessoa com um veículo pesado e com más ideias na cabeça poderia causar uma tragédia onde quer que fosse, tornando o trabalho das polícias ainda mais difícil. E que meses depois, após os atropelamen-

tos em massa no mercado de Natal de Berlim e também na Catalunha, obrigaram as principais cidades europeias a colocar barreiras de segurança nas zonas turísticas de grande afluência, Lisboa e Porto incluídos.

Em Nice, as vítimas do franco-argelino de 31 anos ficaram espalhadas pela rua durante longos minutos. Era impossível recolher os corpos dos 84 mortos e dos 18 feridos para hospitais e morgues num curto espaço de tempo. O que permitiu a jornalistas, familiares, amigos e curiosos tirarem fotografias àquele cenário macabro. Nas horas seguintes, algumas televisões passaram essas imagens, algumas delas não editadas. O corredor de mortos e feridos foi também parar a muitas primeiras páginas de jornais. Houve diários portugueses que seguiram esse mau exemplo. Os horrores do terrorismo iam ganhando sistematicamente honras de aberturas de telejornais e os autores dos massacres eram sacralizados pela propaganda do Estado Islâmico. Uma lógica tortuosa que obrigava a medidas drásticas. Foi assim, que após o ataque em Nice, um grupo de publicações francesas fez um acordo inédito. Para o canal de televisão BFM TV ou os jornais *Le Monde* e *La Croix* tinha terminado uma era. A partir de então, decidiram parar de publicar fotografias dos autores de atentados para evitar que sejam colocados no mesmo nível das vítimas.

O diretor do *Le Monde*, Jérôme Fenoglio (2016), escreveu num editorial que, após o atentado de Nice, não publicará mais fotografias dos autores de massacres para “evitar eventuais efeitos de glorificação póstuma”. Explicou que “não se deve esconder os factos ou a vida dos assassinos, e por isso não somos favoráveis a manter o seu anonimato, mas as suas fotos não servem para descrever o seu passado”. No mesmo artigo são explicitados os pontos de vista dos principais órgãos de comunicação social franceses, à mesma data de julho de 2016. O chefe de redação da BFM TV, Hervé Bérout afirmou: “A foto tem um carácter simbólico e emblemático” e “pode colocar ao mesmo nível vítimas e terroristas”.

Por sua vez, o redator-chefe do jornal católico *La Croix*, François Ernenwein, disse que a partir daquele momento “só publicariam o primeiro nome e a inicial do apelido do autor de um atentado. E não a foto”. A rádio Europe 1 também anunciou que deixaria de “citar os nomes de terroristas”.

Já o *Libération* não partilha este ponto de vista. Segundo o diretor-adjunto do jornal, Johan Hufangel, manter no anonimato os autores não é uma posição sustentável. “Sempre o fizemos, não vai ser diferente agora. Além disso, publicar fotos de terroristas e glorificá-los não é a mesma coisa. A ‘Dabiq’ (a revista do Estado Islâmico) glorifica. Nós não”, acrescentou.

Ao contrário do que aconteceu em França, em Portugal, o debate nem sequer chegou a nascer. O facto de o nosso país nunca ter sido alvo de um atentado pode explicar a falta de polémica. Cada caso é um caso. No *Expresso*, nunca se publicariam fotografias de cadáveres como aconteceu um pouco por todo o mundo, e

também em Portugal. Mas já publicámos por diversas vezes os nomes dos autores de ataques terroristas. E até fotografias dos suspeitos.

Em Portugal o código deontológico dos jornalistas é omissivo em relação a esta questão. O código de ética do *Expresso* também nada refere sobre como atuar em casos destes com o fim de evitar a propagação de organizações como o Daesh ou a Al-Qaeda.

Pelos doze anos que tenho de casa, e pelo que conheço dos colegas com quem trabalho todos os dias, tenho a certeza que existe uma dose muito elevada de bom senso, que prevalece sobre a quantidade de cliques ou de tiragens semanais. Todos nós temos na cabeça que a publicação de uma foto de uma pessoa mutilada num ataque terrorista contribui em muito para a descredibilização do jornalismo. Informar não é mostrar sangue a todo o custo.

O mais recente ataque terrorista realizado em março na Nova Zelândia veio ressuscitar a discussão sobre o que os *media* devem ou não publicar ou transmitir nestes casos. O autor dos atentados na mesquita de Christchurch transmitiu em direto pelo Facebook durante 17 minutos as atrocidades cometidas naquele dia, como se de um jogo de computador se tratasse. Houve órgãos de comunicação social que divulgaram uma parte destas imagens, sem filtros, o que voltou a colocar o tema em debate. Mas a maioria das televisões, sites e jornais optaram por não mostrar as imagens do horror.

As próprias redes sociais foram obrigadas a reagir rapidamente para evitar a disseminação do terror. O vídeo foi retirado pelo Facebook uma hora depois do ataque que matou 50 pessoas e feriu outras 50. Esta rede social anunciou na altura que removeu 1,5 milhões de cópias do vídeo nas 24 horas seguintes à sexta-feira de terror. Também o YouTube alterou e suspendeu os filtros de pesquisa nas horas posteriores ao massacre. Ainda assim, as autoridades não conseguiram estancar a hemorragia uma vez que é missão quase impossível limpar na totalidade este tipo de vídeos do espectro da internet e redes sociais.

Na Nova Zelândia, foi julgado um jovem de 18 anos, acusado de divulgar as imagens do ataque em *livestream*. O rapaz arrisca-se a uma pena de 14 anos de prisão por este crime de incitamento à violência e disseminação do terrorismo.

Uma coisa parece certa: os *media* terão urgentemente de unir esforços para não cair na tentação da propagação do terror. Caso contrário, irão repetir-se os mesmos erros e ilegalidades num próximo ataque terrorista. Tenha estas imagens em direto ou não.

Guia para a Cobertura Noticiosa de um Atentado

Ao realizar pesquisas para este trabalho, encontrei um estudo muito interessante realizado recentemente pela UNESCO (2017). Ao lê-lo, concluí tratar-se de um documento de consulta obrigatória para qualquer jornalista que escreva sobre

assuntos de segurança e terrorismo. Chama-se *Terrorism and the Media: a Handbook for Journalists* e está dividido por capítulos que dão conselhos muito práticos. Destaco três: “Como realizar a cobertura noticiosa de um atentado”, “Como se deve interagir com grupos terroristas” e “Como analisar um ataque terrorista quando regressa a paz”.

Em “Como realizar a cobertura noticiosa de um atentado”, o capítulo IV, os autores lançam algumas perguntas: Qual dos lados devemos escolher: o do jornalista ou da pessoa que pode ajudar a resgatar vítimas? Devemos ajudar as vítimas ou tirar fotos ou captar imagens do seu sofrimento?

Qualquer repórter que tenha estado num palco de um ataque terrorista já levantou estas interrogações.

Nem sempre são de resposta fácil e dependem de caso para caso. Um jornalista pode e deve fazer o seu trabalho, mas não pode esquecer-se de que é um ser humano e que durante a reportagem está rodeado de seres humanos em sofrimento. Devemos ter o bom senso de nos apresentarmos às vítimas que estão em choque e perguntar-lhes se elas necessitam de ajuda médica. Ao noticiarmos um ataque em direto, não nos devemos também esquecer de publicitar os números de emergência que ajudem as vítimas e seus familiares. E tentar não especular sobre os rumores acerca do número de mortos ou feridos. Ter bons contactos nas forças de segurança é essencial. E saber que por vezes é obrigatório não darmos um exclusivo se isso colocar em perigo a vida de pessoas sequestradas pelos terroristas. Os diretos televisivos não podem nem devem filmar tudo. E volto aqui às imagens de pessoas feridas ou mortas, ou outras que ponham em causa a sua dignidade.

Um dos maiores erros apontados pela UNESCO (2017) foi à televisão francesa que fez a cobertura dos ataques de 9 de janeiro de 2015, em Paris; alguns canais revelaram em direto as movimentações das forças de segurança que perseguiram os atacantes, dando pistas aos terroristas sobre como e para onde se deslocarem. Nos ataques de Bruxelas, a 18 de março de 2016, houve um canal que se colocou à porta do apartamento de um dos atacantes do atentado de Paris, de 13 de novembro do ano anterior, antes ainda de as forças de segurança chegarem ao local. Aquele direto punha em causa a investigação.

Os bons exemplos também são aqui citados. Ainda na Bélgica, os *media* acordaram em fazer um *blackout* durante uma operação antiterrorista nos bairros de Bruxelas e Charleroi, que tinha o objetivo de apanhar alguns dos autores do atentado de novembro em Paris. Jornalistas e polícias agiram em equipa para o bem comum.

O capítulo seguinte do mesmo relatório da UNESCO (2017), o da interação de jornalistas com grupos terroristas, diz menos aos repórteres portugueses, pouco habituados a confrontarem-se com este dilema. Principalmente nos últimos anos, depois das guerras civis na África lusófona. Ainda assim, vale a pena citar esta questão levantada pelos autores: O que faria um jornalista se um grupo de terroristas sugere-

risse filmar um ataque em direto? A resposta no meu caso seria fácil. Diria não e avisaria as autoridades, se tivesse meios para o fazer. Mas, infelizmente, nem todos os jornalistas teriam a mesma resposta. O afã noticioso e a avidez em noticiar algo bombástico em primeiro lugar, já fizeram mossas às questões éticas e deontológicas. Um fotógrafo alemão acompanhou uma facção de extrema-esquerda durante um ataque a uma residência em Hamburgo, nos anos 70. E este não é caso único.

As entrevistas com terroristas também devem ser evitadas. Por cá tivemos algumas. No *Expresso* depois de as realizarmos, sempre via *chat* do Facebook, optámos por publicar apenas algumas frases, com muita edição, e não na lógica de pergunta e resposta. A prioridade era não deixar que o terrorista fizesse publicidade gratuita à causa.

Um jornalista deve ter em mente que não pode alinhar no jogo dos extremistas. Entrevistas em direto pela televisão são mais difíceis de gerir, já que desta maneira mais facilmente um grupo passa a sua mensagem para o mundo. Os autores do estudo da UNESCO (2017) chegam ao ponto de interrogar: um jornalista que se encontra com um líder de um grupo terrorista não deve avisar as autoridades da sua localização? Mas coloca-nos outra dúvida: um jornalista é um informador da polícia? A resposta é seguramente negativa, mas a questão não deixa de ser pertinente. E polémica.

O estudo critica a reportagem autorizada, feita por um repórter alemão ao coração do Estado Islâmico em 2014, que acabou por dar um lado limpo, humanizado dos jihadistas, passando ao lado das atrocidades por eles cometidas contra os inimigos. Por fim, analisamos o capítulo do relatório da UNESCO (2017) intitulado “Como analisar um ataque terrorista quando regressa a paz”?

Depois de um atentado surge a análise. Os jornalistas tentam perceber se os serviços de informações falharam, se as medidas preventivas foram insuficientes para travar o ataque, ou se os serviços de emergência atuaram com rapidez e eficácia. É aqui que o papel da imprensa ganha importância e pode ajudar a melhorar as medidas de segurança no futuro, caso se prove que houve falhas graves por parte das autoridades.

Os *media* podem ajudar os familiares das vítimas de ataques, caso o Estado falhe em apoiá-las depois de tudo o que se passou. Nos últimos anos temos publicado no *Expresso* várias reportagens sobre as vítimas portuguesas dos atentados terroristas cometidos nas duas últimas décadas. Ao recolhermos os testemunhos percebemos que, na esmagadora maioria dos casos, as pessoas queixavam-se de terem tido pouco apoio psicológico e monetário por parte das autoridades. Acredito, talvez com alguma ingenuidade, que a publicação deste tipo de trabalhos pode ajudar a inverter o rumo dos acontecimentos.

Em França, na Bélgica, no Reino Unido ou na Alemanha, os períodos pós-atentados servem também para os *media* investigarem se as políticas de desradicalização estão

a ser bem realizadas. Ou se pelo contrário, há ainda muito a fazer para evitar que os jovens caiam nas mãos de pregadores radicais.

Termino com uma frase escrita por Charlie Beckett (2016), no relatório *Fanning the flames: Reporting on terror in a networked world*:

“Melhorar a cobertura noticiosa sobre atos terroristas é importante porque o extremismo violento é o sintoma da existência de problemas mais vastos por todo o globo. Uma reportagem mais inteligente, informada e socialmente responsável do terror não é apenas um argumento moral. É a oportunidade de mostrar que o jornalismo continua a ser uma parte vital da sociedade moderna”.

Bibliografia

- Beckett, C., 2016. *Fanning the flames: Reporting on terror in a networked world* [pdf], setembro. Columbia Journalism School/Democracy Fund Voice. Disponível em [website] <https://www.cjrarchive.org/img/posts/Reporting%20on%20Terror%20in%20a%20Networked%20World%20%28Beckett%29.pdf>
- Farnham, N. e Liem, M, 2017. *Can a Copycat Effect be Observed in Terrorist Suicide Attacks?* [pdf], ICCT Research Paper, março. Haia: International Center of Counter-Terrorism – The Hague (ICCT). Disponível em ICCT [website] <https://icct.nl/wp-content/uploads/2017/03/ICCT-Farnham-Liem-Copycat-Effects-in-Terrorist-Suicide-Attacks-March-2017-1.pdf>
- Fenoglio, J., 2016. Médias : faut-il divulguer l’identité et la photo des terroristes ? *Le Monde*, 27 de julho. Disponível em: https://www.lemonde.fr/actualite-medias/article/2016/07/27/des-medias-decident-de-ne-plus-publier-les-portraits-des-auteurs-d-attentats_4975341_3236.html
- Gabinete do Secretário-Geral do Sistema de Segurança Interna, 2014. *Relatório Anual de Segurança Interna 2014* [pdf]. Disponível em [website] http://mediaserver2.rr.pt/NEWRR/RASI_20142082031f.pdf
- Hagopian, J., 2017. “The Terrorists-R-US”: Mainstream Media Propaganda Fuels and Fans the Flames of War. *Global Research* [em linha], 10 de dezembro. Disponível em: <https://www.globalresearch.ca/the-terrorists-r-us-mainstream-media-propaganda-fuels-and-fans-the-flames-of-war/5491053>
- Hagopian, J., 2015. Terrorism Fallout: Mainstream Media Propaganda Fuels and Fans the Flames of War. *American Empire Exposed* [em linha], 23 de novembro. Disponível em: <http://empireexposed.blogspot.com/2015/11/terrorism-fallout-mainstream-media.html>
- Jetter, M., 2017. *Terrorism and the Media: The Effect of US Television Coverage on Al-Qaeda Attacks* [pdf]. IZA DP No. 10708, abril, pp. 50. Bona: IZA Institute of Labor Economics/Deutsche Post Foundation. Disponível em [website] <http://ftp.iza.org/dp10708.pdf>
- UNESCO, 2017. *Terrorism and the Media: a Handbook for Journalists* [pdf]. United Nations Educational, Scientific and Cultural Organization (UNESCO), Paris. Disponível em [website] <https://unesdoc.unesco.org/ark:/48223/pf0000247074>

Terrorismo e Violência Política: Como Combater o Ciberterrorismo e a Radicalização

Paulo Moniz

Diretor de Segurança de Informação e Risco de TI do Grupo EDP

Resumo

O ciberespaço, sendo uma realidade recente na história da humanidade, apresenta-se já como um espaço disruptivo onde se registam grandes alterações nas dinâmicas de poder e nos paradigmas de funcionamento da sociedade. Este artigo tem como objetivo compreender os fenómenos de radicalização, terrorismo e violência política no contexto do ciberespaço, propondo estratégias de atuação para o seu combate. Para atingir esse desiderato parte-se de uma definição do conceito do Ciberespaço e Ciberpoder, analisando-se as características que os distinguem e como as mesmas podem potenciar a atuação eficaz de grupos terroristas e radicais nesta nova conjuntura. São ainda identificadas as atuais formas de uso da internet por parte destes indivíduos ou organizações criminosas, dando-se uma perspetiva da evolução das suas atividades e as ameaças que encerram. Com base na formalização apresentada, são finalmente identificadas estratégias de combate aos fenómenos de ciberterrorismo e radicalização.

Abstract

Terrorism and Political Violence: How to Combat Cyberterrorism and Radicalization

Cyberspace, a recent reality in the history of mankind, presents itself as a disruptive space where great changes are taking place with impact on the power dynamics and in the paradigms that govern the functioning of society. This article aims to understand the phenomena of radicalization, terrorism and political violence in the context of cyberspace, offering strategic actions to combat them. To achieve this goal, we start with a definition for the Cyberspace and Cyberpower concepts, analyzing the characteristics that distinguish them and how they can, in this new context, enhance the effective performance of terrorist and radical groups. The manner Internet is used by these individuals or criminal organizations is also identified, providing information on the evolution of their activities and the threats they contain. Finally, we identify strategies to combat the phenomena of cyberterrorism and radicalization, based on the presented setting.

Introdução

Fenômenos como o terrorismo e a radicalização estão presentes na nossa sociedade e vivem nos nossos subconscientes, nas decisões que tomamos, muito mais do que queiramos admitir. O modo como os destinos das viagens de férias flutuam, consoante a localização dos episódios de violência ou a ocorrência de atentados terroristas recentes, são exemplos dos sintomas destes fenômenos assim como os impactos que têm na sociedade.

A ideia que temos do terrorismo está fortemente ligada às imagens que nos causam horror, que induzem emoções fortes no ser humano, todas elas baseadas no mecanismo básico do medo. O 11 de Setembro de 2001, com os cenários do embate das aeronaves nos edifícios emblemáticos dos EUA, o fogo imenso das torres que desmoronam, assim como os sucessivos saltos suicidas, foram, talvez, as imagens mais perfeitas que o terrorismo alguma vez conseguiu almejar. Na realidade, todas estas imagens aconteceram no plano real, no mundo convencional, por oposição ao que poderemos designar pela dimensão virtual do ciberespaço, materializada principalmente no conceito de internet, que, não deixando de ser uma estrutura física, constitui uma dimensão nova de interação, criada pelo homem, da qual a nossa sociedade depende, cada vez mais.

Parece, portanto, sensato afirmar que, para a biologia atual do ser humano, as imagens do 11 de Setembro de 2001 são muito mais poderosas e eficazes para os intentos dos terroristas, no que concerne ao ativar dos nossos medos, do que, por exemplo, a privação do acesso a certas localizações na internet ou a indisponibilidade do serviço de mensagens de texto, num determinado país, durante várias horas – ainda que estes acontecimentos possam ter um forte impacto económico e mesmo social. Assim sendo, não obstante o campo convencional continuar a reinar na capacidade de gerar imagens de horror, a verdade é que, atualmente, falamos cada vez mais da utilização do ciberespaço, quer como palco das ações terroristas, quer como veículo privilegiado para potenciar as mesmas no mundo convencional – por exemplo pela ciberpropaganda. Dentro deste domínio de utilização do ciberespaço, ainda que a balança penda, atualmente, para o seu uso enquanto meio para potenciar ações de terrorismo e radicalização, mais do que o cenário físico eleito para atentados, não invalida que esta nova dimensão tenha cada vez mais um papel preponderante e crucial na atuação destes indivíduos ou grupos, pelo que urge entendê-la, de modo a conseguir identificar e implementar estratégias para a neutralização deste tipo de ações.

No contexto deste trabalho, com o objetivo de melhor compreender a dinâmica do ciberespaço, no espectro da radicalização e do terrorismo, será conveniente começar por estabelecer e caracterizar alguns conceitos como “ciberespaço”, “cibepoder” e “ciberterrorismo”, para depois se descrever a utilização atual dos mesmos no contexto dos grupos radicais e, no final, identificar estratégias de combate à radicalização, ao ciberterrorismo e à ciberpropaganda.

Ciberespaço, Informação e Difusão do Poder

O “Ciberespaço”, à semelhança dos oceanos ou espaço aéreo exterior, povoado pelos satélites de comunicações civis e militares à escala global, é muitas vezes entendido como um *Global Common*, assumindo-se como um domínio ou espaço partilhado pelos diversos Estados, mas que não pode ser reclamado como propriedade de nenhum Estado em particular (Buck,1998). Nesta linha de raciocínio é legítimo englobar o “Ciberespaço” como o primeiro *Global Common* totalmente criado pelo homem, sendo que nele assenta a internet, uma rede global de troca de informação e conhecimento partilhada e utilizada, quase sem barreiras, por todos.

Através da internet, em particular pela disponibilização de aplicações e conteúdos, estabelecem-se trocas de informação entre indivíduos e organizações de forma praticamente imediata, criando-nos a sensação de que as fronteiras físicas perdem o sentido e as distâncias deixam de ter significado. Não obstante o nível de abstração do plano físico proporcionado pelo uso da internet, a questão assume uma complexidade adicional, se nos lembrarmos que esta rede global de trocas de informações assenta numa estrutura física, composta por servidores, equipamentos de rede e *links* de comunicações, instaladas em territórios geográficos de diferentes Estados soberanos, regidos por leis secularmente estabelecidas e gerida, quase na totalidade, por empresas privadas. Este facto, relevante para o entendimento do conceito do “Ciberespaço” e das dinâmicas de poder que nele se estabelecem, leva a que alguns autores rejeitem a sua classificação como *Global Common* (Tsagourias e Buchan, 2015), alegando que o princípio da não exclusão de acesso não é assegurado.

É neste novo contexto do “Ciberespaço” que assistimos a um novo nível de “democratização da sociedade”, permitindo que indivíduos com poucos recursos, situados em locais remotos no globo, tenham uma voz ativa e a possibilidade de influenciar os acontecimentos do mundo como nunca antes. Alguns observadores apontam para um “achatamento” da estrutura social, com a eliminação de centros de controlo burocráticos e hierárquicos, passando, inclusivamente, algumas funções dos Estados a ser executadas por privados e assentes em tecnologias inovadoras. Neste contexto, veja-se o exemplo da tecnologia *blockchain*¹ e os impactos que a mesma poderá ter em todo o processo da celebração de contratos entre diferentes partes (EU Blockchain Observatory and Forum, 2018). É também no ciberespaço que cir-

1 *Blockchain*, é uma tecnologia que consiste numa base de dados distribuída por vários nós numa rede, que guarda, de forma segura e confiável, registos de transações, que podem ser validados por todos os nós participantes de uma rede de *blockchain*, sem a necessidade de validação por uma entidade central.

cula uma quantidade de informação que era inimaginável apenas há 20 anos atrás², emergindo praticamente por todo o lado e circulando a uma velocidade estonteante, levantando a questão de qual será o impacto deste fenómeno para os governos e as dinâmicas de poder no século XXI.

As assimetrias ou os diferentes equilíbrios de “Poder” entre Estados são fenómenos a que estamos habituados e que têm estado sempre presentes ao longo da história das sociedades modernas. O fenómeno relativamente novo a que estamos a assistir diz respeito à difusão do “Poder” potenciada pela internet, em concreto pela geração de fluxos informação e acessos a conteúdos de forma pouco controlada e instantânea por qualquer individuo. Os Estados sempre foram ciosos de controlo da informação, pelo que um dos grandes desafios que se lhes apresenta na atualidade prende-se com a aparente incapacidade do exercício de pleno controlo sobre um novo domínio, em especial no que concerne à disseminação e delimitação da circulação de fluxos de informação à escala global.

Ainda que se possa defender que as implicações da disseminação da informação nas dinâmicas de poder não sejam um fenómeno novo, pois, por exemplo, a invenção de Gutenberg no Sec XV permitiu a distribuição e o acesso à Bíblia em larga escala, o que foi considerado um fator decisivo para a Reforma da Igreja Católica, é factual que o fenómeno a que estamos a assistir tem diferenças fundamentais em relação a qualquer outro ocorrido na história da humanidade, em concreto no que diz respeito à sua velocidade exponencial, à abrangência e escala global, assim como às dificuldades no estabelecimento de mecanismos de controlo.

Ciberpoder

O conceito de “Poder” é, como não poderia deixar de ser, um conceito controverso. Existem inúmeras definições de “Poder”, criadas em diferentes contextos e adaptadas às diferentes situações, que foram evoluindo ao longo do tempo, contudo é razoável afirmar que o “Poder” implica a capacidade de exercer “força” ou “influência” de modo a provocar um efeito desejado em determinado domínio. O “Ciberpoder” é o entendimento dessa capacidade no ciberespaço.

O “Ciberpoder” pode, portanto, ser definido como a capacidade de usar o ciberespaço para criar vantagem ou eventos de influência em outros ambientes operacionais através de instrumentos de poder (Nye Jr., 2010). Consta-se, com base nesta definição, que para produzir efeitos do exercício de poder dentro ou fora do próprio ciberespaço, é possível utilizar, com diferentes gradações, instrumentos de poder disponibilizados, quer no ciberespaço, quer no mundo físico convencional.

2 Um estudo muito citado da empresa DOMO apontava que, em 2017, 90% de toda a informação existente na internet tinha sido criada nos dois anos anteriores e que, diariamente, se produzem 2,5 Triliões de Bytes. Ver DOMO (2017).

Com o objetivo de clarificar estas combinações entre meios e efeitos, apresenta-se, na figura 1, exemplos das dimensões do “Ciberpoder” de forma esquematizada.

Figura 1 – Dimensões do Ciberpoder com Exemplos

Dimensão Física e Virtual do Ciberpoder	Efeitos dentro do Ciberespaço	Efeitos fora do Ciberespaço
Instrumentos do Ciberespaço para o exercício de poder	Intrusivos: Ataques de negação de serviços na internet. Ligeiros: Estabelecimento de normas e standards para requisitos de segurança.	Intrusivos: Ataques aos sistemas que controlam infraestruturas físicas. Ligeiros: Difusão de mensagens na internet para a mudança de opinião pública.
Instrumentos “Físicos” para o exercício de poder	Intrusivos: Controlo dos Governos sobre as empresas e os serviços de internet que disponibilizam. Ligeiros: Disponibilização de plataformas e comunicações para suportar causas ligadas à defesa dos direitos humanos.	Intrusivos: Destruição física de recursos tecnológicos. Ligeiros: Discriminação seletiva de serviços ou mesmo a difamação de certas localizações na internet.

Fonte: adaptação de Nye Jr. (2010).

Na dimensão de utilização de instrumentos de poder disponibilizados no ciberespaço, é possível conseguir alcançar efeitos:

- **Dentro do próprio ciberespaço**, utilizando instrumentos intrusivos que podem passar pelo lançamento de ataques tecnológicos de negação de serviço através do uso de *botnets*³, direcionados a certas localizações da internet, ou, então, pela utilização de instrumentos mais ligeiros, como o estabelecimento de normas e requisitos que contribuam para um elevado nível de segurança dos recursos tecnológicos das organizações.
- **Fora do ciberespaço**, com a utilização de instrumentos intrusivos, que podem passar por um ataque informático aos sistemas que controlam infraestruturas críticas⁴, resultando desse ataque consequências no mundo físico, tais como

3 A utilização de *botnets*, para perpetrar ataques de negação de serviço a localizações na internet, é uma prática comum das organizações criminosas. As *botnets* são redes de computadores infetados, sem o conhecimento dos seus utilizadores, que são controlados remotamente através de um *software* de comando e controlo, estando essa rede de máquinas ao dispor de atores mal-intencionados para participar em ataques a outros recursos tecnológicos da rede.

4 Um dos tipos de sistemas mais conhecidos, que permitem o controlo de infraestruturas físicas, algumas delas críticas, são os sistemas SCADA (Supervisory Control And Data Aquisition), utilizados geralmente pelas *utilities* e empresas industriais para monitorizar as variáveis de controlo dos processos com impactos no mundo físico – exemplo, a distribuição em redes de energia ou água. Um ataque bem sucedido a estes sistemas pode ter consequências catastróficas na segurança da sociedade.

uma falha generalizada do abastecimento de energia. Por via do uso de instrumentos mais ligeiros, constitui-se como um bom exemplo desta atuação, a disseminação de informação pelas redes sociais de modo a influenciar a opinião pública.

Na dimensão de utilização de instrumentos “físicos” de poder, os efeitos são os seguintes:

- **Dentro do ciberespaço**, tendo como exemplo de um instrumento intrusivo o controlo direto dos governos sobre os serviços de internet das empresas privadas ou de outras organizações, ou, na categoria dos instrumentos ligeiros, a disponibilização de plataformas tecnológicas de *hardware* para suportar causas ligadas à defesa de direitos humanos.
- **Fora do ciberespaço**, dentro da esfera dos instrumentos intrusivos, pode-se falar na utilização de ataques convencionais com objetivo de destruição física, de modo a colocar inoperacionais infraestruturas de servidores e comunicações ou, na gradação dos instrumentos ligeiros, pode-se exemplificar com uma ação de discriminação seletiva de serviços ou mesmo na difamação de certas localizações na internet⁵.

Ciberespaço e Ciberpoder

A caracterização do ciberespaço passa essencialmente pela identificação e análise dos seus elementos diferenciadores no contexto da sua utilização pelo ciberpoder. Neste âmbito, identificam-se os seguintes quatro fatores essenciais a destacar:

1. **Baixas barreiras de entrada.** Vivemos atualmente numa sociedade interligada através de uma rede global com uma acessibilidade nunca antes experienciada. É fácil, a qualquer indivíduo, praticamente em qualquer parte do planeta, ligar um recurso computacional a esta rede global e aceder instantaneamente a sistemas num outro lado do mundo. Para além da facilidade de acesso tem-se assistido ultimamente à proliferação de ferramentas fáceis de utilizar pelos ciberatacantes, acessíveis através de plataformas concebidas para a sua comercialização, exigindo-se destes cada vez menos capacidades tecnológicas para perpetuar ações criminosas.
2. **Possibilidade de ocultação.** Este é outro aspeto fundamental para o estudo do exercício do poder no ciberespaço e prende-se com a facilidade que indivíduos mal-intencionados têm para esconder as suas ações sem correrem

5 Para ilustrar melhor esta dimensão que envolve o ciberespaço, mas ao mesmo tempo o exclui, quer como alvo de efeitos diretos, quer na sua utilização como meio para o exercício de poder, temos o exemplo dos protestos de 2006 nas ruas de Washington, contra a divulgação pela Yahoo da lista de ativistas chineses, que conduziu à prisão destes indivíduos pelo governo desse país (Nye Jr., 2010).

grandes riscos de ser identificados ou detetados. Esta facilidade deve-se à simplicidade de entrar na rede através da criação de identidades fictícias ou à possibilidade de realizar ações em geografias remotas. Como ilustrado por Peter Steiner, 24 anos atrás, num famoso *cartoon* do *The New York Times*: “on the Internet, nobody knows you’re a dog” (Fleishman, 2000).

3. **Mutabilidade do ciberespaço.** Trata-se de uma outra característica que importa perceber para compreender o exercício de poder no ciberespaço. A internet tem uma forma muito mutável, com a capacidade de criar e desmantelar dinamicamente sítios de internet ou locais de armazenamento de dados. Uma operação num campo convencional tem como base o reconhecimento territorial e a assunção de que o mesmo, embora possa sofrer mutações, manter-se-á, no essencial, na sua forma física conhecida. Já no ciberespaço, essa premissa não pode ser assumida.
4. **Ausência de fronteiras.** Outro aspeto que dificulta muito o controlo do ciberespaço está relacionado com a ausência de fronteiras geográficas, no sentido convencional como as conhecemos. Na prática, a navegação na internet e o acesso aos diversos recursos acontece de forma transversal, sem respeito pelas fronteiras dos Estados, o que dificulta muito a atuação jurídica, dado que um crime, perpetrado sobre um recurso em determinada localização geográfica, pode ter origem numa outra, remota, com enquadramentos legais totalmente diferentes.

Pode-se assim entender o ciberespaço como um ambiente assimétrico no que diz respeito ao exercício de poder, na medida em que potencia ações maliciosas de agentes com poucos recursos. Deve-se, no entanto, deixar claro que a difusão do poder não é o mesmo que a sua equalização, ou seja, não obstante qualquer ator poder ter um papel relevante no exercício do poder no ciberespaço, não implica que o faça da mesma forma e com o mesmo grau de eficácia que um outro agente que disponha de grandes recursos.

Agentes que Exercem Poder no Ciberespaço

Tendo por base o objetivo de compreender o exercício de poder no ciberespaço é agora conveniente proceder a uma breve identificação dos principais agentes que nele atuam, assim como as suas motivações. Para uma identificação mais clara dos agentes do ciberespaço existem alguns modelos muito completos, como aquele que apresenta a ENISA (2016, p. 59), contudo, para o objetivo que aqui se pretende atingir, a aproximação defendida por Nye Jr. (2010) é suficiente para enquadrar as estratégias apresentadas no final deste estudo. Este autor distingue as seguintes categorias de agentes do ciberespaço: Estados; as organizações com redes estruturadas; e indivíduos com redes fracamente estruturadas. Neste contexto, os diversos atores podem ser caracterizados da seguinte forma:

1. **Estados.** Os governos têm um papel determinante no governo do ciberespaço pois, tal como referido anteriormente, o ciberespaço, apesar de se apresentar com um domínio sem fronteiras, depende de infraestruturas físicas instaladas em territórios com quadros legais próprios, que servem do desígnio da soberania das Nações a que pertencem. Neste contexto o espaço geográfico é relevante e os governos podem atuar em diversos planos, desde a educação para a cibersegurança, capacitação de infraestruturas, aplicação de legislação específica ou mesmo exercendo poder de forma coerciva. Para ilustrar este último cenário recorde-se, como exemplo, a ação levada a cabo pelo governo chinês, nas greves de Xinjiang em 2009, deixando indisponíveis serviços de comunicação, resultando em 19 milhões de pessoas sem acesso a mensagens de texto e chamadas internacionais (LaFraniere e Ansfield, 2010). Ainda dentro deste tipo de ações na esfera de atuação dos Estados, existem registos de atos de guerra como, por exemplo, os atos de sabotagem de equipamento eletrónico no Iraque em 2003 ou na Geórgia em 2008 (Harris, 2009).
2. **Organizações com redes estruturadas.** Nesta secção, enquadram-se como exemplo, grandes empresas multinacionais, como a Microsoft e a Google, ou até organizações criminosas, que possuem recursos financeiros, humanos e tecnológicos muito avançados com presença transnacional. No que diz respeito às empresas de grande dimensão, algumas delas apresentam um poder maior que alguns Estados, tendo mesmo levado a Dinamarca a criar, na sua estrutura diplomática, um embaixador para estes gigantes tecnológicos (Gramer, 2017). Com o aumento da utilização da computação em nuvem⁶, quer para o alojamento de dados e aplicações, quer para uso de ferramentas corporativas como o e-mail, acentua-se cada vez mais o domínio que estas organizações possuem no ciberespaço, assim como a dependência da própria sociedade nos seus serviços e na segurança dos produtos que desenvolvem. Pelo lado mais negro, temos as organizações criminosas que fazem uso do ciberespaço para alimentarem o seu crescimento orgânico e as suas operações. A Al-Qaeda, por exemplo, deixou de ser uma organização fortemente hierárquica e confinada geograficamente para ser uma rede global e horizontal com uma forte dinâmica no recrutamento e na capacitação dos seus operacionais (Nye Jr., 2010, p.12).
3. **Indivíduos sem redes estruturadas.** Esta categoria assume especial importância, devido a um dos fatores distintivos do ciberespaço, que é a baixa barreira de entrada. É com facilidade que indivíduos podem interagir na rede

6 O conceito de computação em nuvem – em inglês, *cloud computing* – refere-se à utilização de memória, capacidade de armazenamento e cálculo, de computadores e servidores, interligados em rede, e acedidos através da internet. Consultar https://pt.wikipedia.org/wiki/Computa%C3%A7%C3%A3o_em_nuvem [Acedido 27 outubro 2018].

global, juntando-se a organizações ou atuando sozinhos. Neste contexto, as ferramentas desenvolvidas e disponibilizadas para a sua atuação tornam menos clara a distinção entre estes agentes e as organizações com redes estruturadas. Pelo lado negativo, o fenómeno a que assistimos mais frequentemente neste plano, está associado ao cibercrime, em que as vítimas são indivíduos e organizações e a principal motivação dos atacantes é o lucro económico. Cenários típicos de cibercrime são os ataques de *ransomware*, em que os atacantes cifram as máquinas das vítimas exigindo um resgate para as desbloquearem ou, então, os ataques de *phishing*, onde se tentam obter credenciais ou outra informação relevante, capaz de aportar valor económico a ser extraído das vítimas. Enquadra-se também nesta categoria os denominados ataques internos, normalmente perpetrados por indivíduos contra as organizações de que fazem parte.

A figura 2 ilustra os diferentes agentes e a sua capacidade de uso das ferramentas de poder descritas anteriormente.

Figura 2 – Utilização das Ferramentas de Poder pelos Diferentes Agentes do Ciberespaço

	Estados	Organizações com redes estruturadas	Indivíduos sem redes estruturadas
Instrumentos do Ciberespaço para o exercício de poder	<p>Intrusivos: Podem exercer poder no ciberespaço através de valências como, por exemplo, os centros de ciberdefesa das forças armadas.</p> <p>Ligeiros: Podem estabelecer normas e <i>standards</i> para requisitos de segurança para operadores de comunicações.</p>	<p>Intrusivos: Podem ter ações coordenadas com os Estados e enquadradas nas sociedades de direito (por exemplo os operadores de internet bloquearem a propagação de mensagens ou acesso a domínios de internet).</p> <p>Ligeiros: Podem divulgar e promover ideais e convicções organizacionais, como a luta contra o racismo, através dos seus canais no ciberespaço (sites, contactos com clientes, entre outras).</p>	<p>Intrusivos: Não está previsto, sendo que, inclusive, algumas atuações na internet, como a procura de vulnerabilidades em serviços, podem ser classificadas de cibercrime pelo quadro legal em vigor.</p> <p>Ligeiros: Podem, em blogs ou redes sociais, divulgar e promover os seus ideais e convicções.</p>
Instrumentos “Físicos” para o exercício de poder	<p>Intrusivos: Podem exercer controlo sobre serviços de empresas mediante enquadramento legal (ex: para investigação criminal).</p> <p>Ligeiros: Podem disponibilizar meio tecnológicos como plataformas e comunicações para generalizar o acesso à internet.</p>	<p>Intrusivos: Não está previsto no quadro das organizações legítimas.</p> <p>Ligeiros: Podem participar e promover ideais e convicções organizacionais, como a luta contra o racismo, fora do ciberespaço.</p>	<p>Intrusivos: Não está previsto.</p> <p>Ligeiros: Na sua atuação como cidadão pode difamar certas utilizações da internet (por exemplo, condenando alguns locais da internet, na defesa da propriedade intelectual de músicas e livros).</p>

Fonte: elaboração do autor.

Terrorismo e Ciberpoder: Ciberterrorismo

Antes de adotarmos uma definição para “Ciberterrorismo”, será sensato partirmos de uma definição para “Terrorismo”. No entendimento do Departamento de Defesa dos EUA, “Terrorismo” corresponde ao uso premeditado, não legitimado na lei, de violência ou ameaça, para criar medo, coagir ou intimidar governos e sociedades,

na persecução de objetivos políticos, religiosos ou ideológicos (DoD, 2018, p.232). No que diz respeito ao “Ciberterrorismo”, apesar de existirem várias definições, optar-se-á por uma que tenha em consideração a definição de “Terrorismo” aqui apresentada, assim como toda a caracterização relativa ao ciberpoder aqui feita. Deste facto resulta, como exemplo, que se exclui à partida definições de “Ciberterrorismo” que não integrem na sua definição os ataques físicos a recursos de informação, pois não seria coerente com a abordagem mais ampla aqui apresentada sobre os instrumentos do ciberpoder. Uma definição particularmente interessante do “Ciberterrorismo”, pela sua simplicidade e abrangência, diz-nos que se tratam de ações premeditadas, com motivações políticas, contra informação, sistemas, programas de computadores e dados, que resultem em violência contra entidades não-beligerantes, perpetradas por grupos ou agentes clandestinos (Pollitt, 1997). Na prática, no quadro aqui apresentado, o “Ciberterrorismo” materializa a convergência dos objetivos e ideais terroristas com a realidade do ciberespaço, explorando, nesse domínio, os instrumentos do ciberpoder, com o desiderato de aumentar a eficácia no atingimento dos seus objetivos.

Atualmente, porventura pelo facto referido anteriormente, a saber, que os ataques a recursos no ciberespaço não têm o mesmo atrativo espetacular dos ataques convencionais, pois não proporcionam imagens de terror facilmente captáveis pelos meios de comunicação social, não existem registos evidentes da sua utilização pelo ciberterrorismo. O ciberespaço tem sido sim, usado pelas organizações terroristas, para potenciar e aumentar a eficácia dos ataques convencionais, em concreto nas seguintes dimensões (UNODC, 2012):

1. **Propaganda.** Trata-se basicamente de utilizar o ciberespaço para a disseminação dos ideais dos grupos terroristas, em concreto como um método importante para concretizar o ciclo de recrutamento, radicalização e instigação à ação violenta. A ciberpropaganda pode assumir várias formas, desde apresentações; documentos; revistas; filmes; vídeos ou mesmo jogos. Um dos exemplos é a revista *Dabiq*⁷, utilizada para promoção dos objetivos do auto-proclamado “Estado Islâmico”. A ciberpropaganda acaba por beneficiar da rapidez oferecida pelo ciberespaço, mas também das baixas barreiras de entrada, o que permite aos grupos disseminar informação sem qualquer filtro e em qualquer lugar de forma imediata, ao mesmo tempo que lhes faculta a possibilidade de o fazer de maneira camuflada. Beneficia também da estru-

⁷ A revista *Dabiq* foi publicada, em várias línguas, pela primeira vez em julho de 2014 pelo auto-proclamado “Estado Islâmico”. Inicialmente era publicada através da *deep web* – internet não acessível nos motores de busca normais, utilizada, genericamente, para fins menos lícitos – mas facilmente estava disponível em outros sítios na internet acessíveis por qualquer cidadão. Disponível em [https://en.wikipedia.org/wiki/Dabiq_\(magazine\)](https://en.wikipedia.org/wiki/Dabiq_(magazine)) [acedido 25 outubro 2018].

tura de enquadramento das sociedades democraticamente mais avançadas, onde o direito à liberdade de expressão é uma prerrogativa basilar a preservar, ainda que seja aceite que tal não se aplica quando estão em causa mensagens capazes de ameaçar a segurança nacional. Pode-se, com propriedade, dizer que os locais chave para a radicalização deixaram de ser áreas geográficas, como o Iémen ou Afeganistão, e passaram a ser as comunidades virtuais estabelecidas com base na internet (Roy, 2010).

2. **Financiamento.** Segundo o relatório da United Nations Office on Drugs and Crime (UNODC, 2012) sobre o uso da internet para o cibercrime, existem quatro formas de angariação de fundos que beneficiam das características únicas do ciberespaço: solicitação direta; comércio eletrónico; pagamentos e transferências *online*; e utilização de organizações sem fins lucrativos. O financiamento direto diz respeito às solicitações realizadas através de e-mails diretos, *chats* ou sítios da internet, enquanto o comércio eletrónico está orientado para a venda de material referente às organizações, tais como livros ou vídeos. As transferências *online* são operações realizadas através de aplicações tipo PayPal ou mesmo usando moedas virtuais, sendo que, dentro desta categoria, ainda se enquadram os métodos ilegítimos, tais como roubo de credenciais e cartões de crédito ou fraudes eletrónicas. Existem também formas de financiar grupos terroristas através de organizações sem fins lucrativos, como se verificou com o financiamento de grupos terroristas no Médio Oriente, realizado através de organizações com nomes como Benevolence International Foundation ou Global Relief Foundation, que justificavam a sua atividade com base em fins de caridade (UNODC, 2012, p.7).
3. **Treinos.** Ultimamente as organizações terroristas têm utilizado a internet como plataforma de treino dos seus membros. Diversos sítios na internet providenciam informação e instruções pormenorizadas, sob o formato de manuais, ficheiros de áudio ou vídeo, em várias línguas, sobre as formas de alistamento, como construir explosivos ou planejar atentados⁸. Muitas vezes estas plataformas também incluem medidas e métodos de apoio ao desenvolvimento de atividades de contra informação e *hacking*, explicando como aumentar a segurança nas comunicações através da sua encriptação e anonimização. Em síntese, as características particulares do ciberespaço, permitem às organizações terroristas uma capacidade de treino muito mais eficiente e com menor risco, por oposição às deslocações físicas através das fronteiras de diversos estados, para frequentar ações de formação, que se apresentam como demasiado arriscadas.

8 Exemplo deste tipo de atuação é possível encontrar na revista *Inspire*, publicada pela Al-Qaeda, que tem como objetivo facilitar o treino em casa dos muçulmanos para a *jihad*.

4. **Planeamento.** O planeamento das operações é outro exemplo do uso do ciberespaço pelos grupos terroristas de modo a concretizarem com sucesso os seus objetivos. Uma vez mais a facilidade de estabelecimento de comunicações seguras e praticamente anónimas entre diversas partes, assim como a disponibilização de informação em tempo real, transformam a internet numa ferramenta essencial para o planeamento de ataques. No planeamento de ações terroristas, pode-se ainda fazer uso de um manancial de informação pública, muitas vezes desprotegida, como imagens de edifícios de interesse, número de pessoas concentradas num determinado local numa certa hora do dia ou, ainda, informações pessoais de possíveis vítimas, disponibilizadas em redes sociais.
5. **Execução.** Neste plano considera-se a internet como o espaço privilegiado para coordenar e perpetrar ataques físicos, mas também para concretizar outras ações com o objetivo de gerar o medo generalizado. No primeiro caso, podemos recordar o uso intensivo da internet nos atentados do 11 de Setembro de 2001, enquanto no segundo se enquadram os vídeos, recentemente difundidos, de decapitações, apedrejamentos e genocídios perpetrados pelo autointitulado “Estado Islâmico”.
6. **Ciberataques.** Apesar de se ter referido antes que os cenários de ataques terroristas no ciberespaço são menos frequentes e apetecíveis para os efeitos de medo que os terroristas pretendem atingir, existem alguns registos desses atos, com consequências, quer no plano virtual quer no plano físico, consubstanciando exercícios de poder no ciberespaço e fora dele. Com consequências no ciberespaço, recorde-se o exemplo do ataque ocorrido à TV5 francesa, inicialmente assumido pelo autoproclamado “Estado Islâmico”, mas, mais tarde, atribuído a *hackers* russos⁹. Contudo, não obstante os exercícios de força no ciberespaço comecem a ganhar o seu protagonismo, as maiores consequências, ainda não muito exploradas, serão aquelas que os terroristas consigam almejar através de ações no ciberespaço com impactos no mundo físico. Fala-se, neste plano, das infraestruturas críticas de informação, que são aquelas que controlam em tempo real equipamentos como sistemas de sinalizações de redes de transporte; controlo do espaço aéreo; produção e distribuição de energia – por exemplo em centrais nucleares – ou redes de distribuição de águas, entre outras. A maioria destas infraestruturas estão sobre

9 Este caso foi um exemplo típico de uma APT (*Advanced Persistent Threat*), iniciado e preparado muito antes do dia da concretização do ataque propriamente dito, e que conseguiu colocar os onze canais da TV5 indisponíveis, difundir mensagens de reivindicações islâmicas nos meios de comunicação da empresa na internet, assim como tornar indisponíveis os recursos tecnológicos deste canal.

controle de empresas privadas, o que implica que estas entidades têm responsabilidades na sua defesa e proteção, no plano do ciberespaço, semelhantes às forças armadas e de segurança no campo convencional. Se as infraestruturas destas empresas não tiverem implementados mecanismos de defesa e reação, a segurança da nossa sociedade, e em última instância a soberania dos países, pode ficar ameaçada¹⁰.

Estratégias de Combate ao Ciberterrorismo e Radicalização

Estamos agora em condições de estabelecer e compreender melhor as estratégias de combate ao ciberterrorismo e radicalização, que deverão ter em consideração todas as características que aqui já foram identificadas sobre o ciberespaço, assim como a dinâmica de poder que se desenrola nesse ambiente. Segundo Lachow (2009) podem-se definir três tipos de estratégias de combate, nomeadamente no plano físico, informacional e cognitivo.

Estratégia de Combate no Plano da Infraestrutura Física

O objetivo desta estratégia é atingir as infraestruturas físicas que suportam a internet de modo a causar indisponibilidade ou interrupção dos seus serviços. Convém aqui lembrar o que até aqui dissemos sobre o ciberespaço, a saber, que, não obstante este se apresentar, numa determinada camada de abstração, como um espaço sem fronteiras, virtual, na verdade ele assenta em recursos físicos e materiais perfeitamente identificáveis, instalados em territórios de Estados soberanos. Podemos estar a falar de ações que destruam nós de comunicações nevrálgicos (infraestruturas de comunicações) ou mesmo centros de dados que albergam servidores utilizados por organizações terroristas.

As ações neste domínio de atuação serão mais eficazes quando mais focalizadas e dirigidas elas poderem ser. Destruir uma infraestrutura poderá ter um efeito imediato e com alguma durabilidade, contudo, também poderá afetar outros serviços legítimos, muitas vezes de Estados aliados, que partilhem as mesmas infraestruturas. Neste contexto, recorde-se que as plataformas internet mais utilizadas para comunicação e disponibilização de informação estão instaladas em Estados europeus ou norte-americanos. Depreende-se com facilidade que a destruição convencional de uma infraestrutura física que afete apenas o alvo desejado só poderá acontecer, com grande sucesso, em situações muito excecionais, como por exemplo equipamentos que suportem grupos terroristas em locais de treino remotos, onde os efeitos colaterais serão residuais.

10 Esta é uma das razões que levou a União Europeia a criar a legislação NIS (Network and Information Security) para toda a comunidade, com o objetivo de nivelar e reforçar as capacidades de defesa destas infraestruturas por todas as geografias do espaço europeu.

Mais eficaz neste domínio será solicitar aos operadores de serviços de internet dos Estados aliados que desliguem ou inativem serviços que estão a ser usados pelos terroristas. Contudo estas ações também têm alguma dificuldade em ser materializadas, se recordarmos o que atrás se referiu, constatando-se que o ciberespaço permite, com alguma facilidade, o desenvolvimento de uma ação camuflada e que o mesmo tem uma geografia muito mutável. Desta forma, não é difícil para os grupos terroristas moverem-se para outros serviços de internet e fazer uso dos mesmos para continuarem a perpetuarem as suas ações.

Finalmente, pode-se considerar que, dentro deste tipo de estratégia de atuação, a vigilância física das infraestruturas, sem interrupção física dos serviços, poderá ser, em muitos casos, a medida mais eficaz, monitorizando as comunicações entre organizações criminosas e utilizando essa informação para atuar no contraterrorismo. A principal e relevante dificuldade desta abordagem prende-se com eventual violação de direitos estabelecidos nas sociedades democráticas, uma vez que uma atitude de vigilância aumenta o grau de desconfiança dos cidadãos nos serviços e governos, podendo, inclusive, vir a ter impactos económicos.

Em resumo, os principais benefícios desta estratégia são obviamente a sua eficácia em termos da destruição e bloqueio do acesso à internet como instrumento de poder, dado que o seu suporte físico fica seriamente afetado no local atingido. Não obstante se conseguir um efeito destrutivo imediato, não poderemos considerar esta estratégia como a mais eficaz a longo prazo, pelas razões de que, não só a maioria dos recursos se encontram instalados em territórios europeus e norte-americano, mas também porque, ao afetar de forma pouco seletiva alguns desses recursos, estar-se-ia a afetar outros serviços, legítimos, de Estados aliados, que também fazem uso dessas infraestruturas. Corre-se assim o risco destas ações serem interpretadas como atos de guerra. É um nível de estratégia de atuação que entra nas competências dos Estados e que apenas fará sentido em ações táticas ou operacionais em determinado cenário de conflito.

Estratégia de Combate no Plano Informacional

As ações neste nível estratégico têm como objetivo intervir nas propriedades de segurança da informação, em concreto na sua confidencialidade, integridade e disponibilidade.

No que diz respeito à confidencialidade, a capacidade de interceção de mensagens difere da descrita na estratégia anterior, no plano da infraestrutura, na medida em que aqui, ao contrário do referido anteriormente, não se prevê a interferência junto dos operadores de serviços de internet, mas sim na utilização de agentes capazes de entrar nos grupos eletrónicos dos terroristas ou na capacidade de decifrar as mensagens trocadas entre indivíduos criminosos. Neste plano, as agências governamentais são os principais agentes, mas também existem outros participantes, como

por exemplo o SITE Institute¹¹, que foi, durante anos, uma organização sem fins lucrativos que monitorizava os sítios internet utilizados pelos grupos terroristas. Já no que se prende com a integridade, entendem-se aqui as ações que visem conduzir a decisões erradas por parte dos atacantes, tais como, realizar intrusões nas bases de dados ou em sítios internet, utilizados pelas organizações criminosas, com o objetivo de criar desconfiança entre os atacantes. Existe neste ponto um aspeto muito relevante e que dá conta das especificidades do ciberespaço atrás descritas. Dentro dos registos deste tipo de atuação, à partida atribuído aos Estados, existem casos de cidadãos que se infiltraram em redes terroristas e que trabalham voluntariamente para as agências governamentais.

No que se refere à disponibilidade, já mencionada no plano físico através da condução de ações destrutivas mais convencionais, constata-se agora uma clara ligação a aspetos mais tecnológicos, como a capacidade de realizar ataques DoS (*Denial of Service*)¹² aos serviços internet utilizados pelos terroristas ou então às ações desenvolvidas para provocar a indisponibilidade de recursos através da exploração das suas vulnerabilidades.

Em suma, constata-se que as estratégias desenvolvidas ao nível informacional são mais fáceis de levar a cabo do ponto de vista logístico e têm menos consequências colaterais do que as estratégias desenvolvidas no plano físico. Contudo, também é verdade que estas ações necessitam de muitos recursos técnicos e não é difícil, para os atacantes, contornarem estas ações movendo-se entre localizações na internet ou alterando o esquema de cifrar mensagens que trocam entre si, mantendo-se dessa forma anónimos no ciberespaço. Fundamentalmente, é necessário perceber que estas estratégias, apesar de mais perenes e eficazes que as desenvolvidas no plano físico são também mais demoradas a produzir efeitos, exigindo mais recursos intelectuais e tecnológicos. O aspeto mais curioso e que é fundamental aqui realçar, é que estas podem ser levadas a cabo não só pelos Estados, mas também por outros agentes, como organizações com redes estruturadas ou indivíduos com recursos limitados.

11 O SITE Institute (Search for International Terrorist Entities Institute) foi fundado em 2002 e tinha como objetivo monitorar a atividade *online* de organizações terroristas. O projeto terminou em 2008 e alguns dos elementos que o integravam continuaram as suas atividades numa outra organização denominada SITE Intelligence Group.

12 DoS (*Denial of Service*), é uma interrupção de um serviço de internet causado por acessos legítimos ou ilegítimos, normalmente com intuítos maliciosos. Acessos legítimos podem ser oriundos de uma rede *botnet*, que lançam um número extraordinariamente elevado de pedidos, concentrados temporalmente, a páginas de internet, com o objetivo de esgotar a capacidade de resposta dos servidores e provocar indisponibilidade. Acessos ilegítimos podem ser atacantes que explorem vulnerabilidades de sítios da internet.

Estratégia de Combate no Plano Cognitivo

Finalmente, a um nível mais elevado de sofisticação, temos estratégias ao nível cognitivo, que têm como objetivo a mudança de percepção por parte do público em geral, influenciando desta forma as suas decisões. Neste cenário, inserem-se, por exemplo, as ações de contrapropaganda. A atuação neste plano pode ter como objetivo, entre outros, diminuir a atratividade das organizações terroristas sobre certas franjas da população, sendo fundamental para tal ter em consideração aspetos cruciais como o contexto sociopolítico, a cultura, a língua ou mesmo os valores. Para levar a cabo ações nesta dimensão será também necessário coordenar esforços, quer na vertente diplomática, quer junto dos órgãos de comunicação, balançando o respeito pela liberdade de imprensa e a necessidade de transmitir as mensagens corretas.

As ações levadas a cabo neste plano podem ser comparadas a uma guerra de ideias, onde é mais eficiente ser pró-ativo que reativo. É sabido que é necessário muito mais esforço para conseguir mudar a opinião de uma audiência quando esta já tem uma ideia preconcebida do que estabelecer novos factos e percepções. Neste âmbito, devem ser empreendidos esforços para edificar ideias nas populações mais frágeis e suscetíveis de abraçar as motivações dos terroristas, tendo em atenção o seu contexto cultural e cuidando de todos os aspetos da comunicação, desde a utilização das terminologias corretas – por exemplo, evitar a expressão “Estado Islâmico” sem referenciar a sua auto intitulação, caso contrário fica a ideia de uma legitimação que não é real – até à disponibilização abundante de contrainformação sobre as mensagens dos grupos radicais.

É sabido que a eficácia máxima só será conseguida através da educação, essencialmente na promoção dos valores que devem reger as sociedades de bem e na capacitação dos cidadãos para discernir e questionar a qualidade da informação que lhes é disponibilizada. Os Estados devem investir numa correta educação e preparação dos seus cidadãos para as novas realidades emergentes do ciberespaço. Contudo, a dificuldade destas estratégias surge porque muitos dos problemas são atuais e emergentes, sendo que, as medidas estruturais profundas que esta abordagem exige, demoram muito tempo a surtir efeito. Estas medidas tornam-se mesmo pouco atrativas para as alternâncias políticas que passam pelo poder, omitindo-se estas de empreender quaisquer esforços na criação de políticas concretas e de longo prazo em áreas fundamentais à sociedade.

Estratégia Global da Informação e Estrutura Orgânica

Foram apresentadas estratégias de combate que, como constatámos, podem ser levadas a cabo por diversos agentes e fazer uso de diferentes tipos de instrumentos de poder. Será agora conveniente realizar agora uma breve análise sobre alguns aspetos relevantes para a criação de governo que permita a implementação, com sucesso, dessas estratégias.

As estratégias de combate aqui referidas evidenciam um novo tipo de conflitualidade que se desenvolve no ciberespaço, e que é baseada na informação e nos sistemas que a suportam. Atendendo ao princípio de que cada forma de coação corresponde uma estratégia global, então a utilização conflitual da informação como forma de coação, deve fazer emergir uma Estratégia Global da Informação (Nunes, 2015). A Estratégia Global da Informação influencia outras estratégias globais, até porque a informação revela-se como um recurso necessário para atuação em outros domínios, como o económico ou militar. Neste sentido, os domínios de defesa militar e segurança do ciberespaço, respetivamente ciberdefesa e cibersegurança, deveriam, idealmente, edificar as suas estratégias em consonância com uma Estratégia Global da Informação. Considerando o que foi aqui exposto, mormente as alterações nas dinâmicas de poder proporcionadas pelo ciberespaço, conclui-se também, que as estratégias de combate ao ciberterrorismo e radicalização aqui descritas, não podem ser operacionalizadas de forma desgarrada, e só terão sentido e maior eficácia se estiverem enquadradas numa Estratégia Global da Informação que, consoante o quadro a considerar, poderá ser de âmbito nacional ou europeu.

O ciberespaço é um domínio onde existe uma responsabilidade coletiva, tornando-se necessário clarificar os papéis a desempenhar pelos diversos atores. Determinar as origens, intenções, ou mesmo o impacto dos ciberataques, não se assume como tarefa fácil, levando a que o plano de atuação integre os eixos civil-militar e nacional-internacional. Neste contexto, apesar de ser fundamental deixar clara a distinção entre ciberdefesa e cibersegurança, por terem missões diferentes, é também igualmente fundamental assegurar uma articulação entre estes dois domínios. Por oposição aos cenários convencionais, um ataque a uma infraestrutura crítica, perpetrado por via do ciberespaço, poderá exigir uma atuação coordenada, quer das forças de segurança e defesa, como, em especial, das organizações privadas detentoras dessas infraestruturas, sendo que, com elevada probabilidade, nenhum dos atores mencionados terá capacidades suficientes, em isolado, para combater uma ameaça desse tipo.

A cooperação, quer entre Estados, quer entre entidades do Estado e atores civis, surge como orientação fundamental nas estratégias de combate ao ciberterrorismo e radicalização. Da mesma forma deverá existir uma entidade responsável e regulamentação dirigida à coordenação entre os dois domínios da Cibersegurança e Ciberdefesa, de modo a aproveitar sinergias e concertar políticas de proteção e reação, em especial, na edificação de uma capacidade de resposta conjunta em cenários de crise. Estabelecer protocolos de atuação com os operadores de serviços de internet ou com as empresas que controlam infraestruturas críticas, são exemplos, que não esgotam, de forma alguma, o rol das iniciativas possíveis, de contributos para uma maior eficiência das estratégias de combate, assim como de ações capazes de estabelecer um nível de confiança dos cidadãos.

Conclusão

O ciberespaço, sendo uma realidade muito recente na história da humanidade, apresenta o potencial para provocar a maior das disrupções da nossa civilização. Neste espaço virtual, criado pelo homem, já se começaram a produzir alterações estruturais ao funcionamento das sociedades, sendo que algumas delas ameaçam baralhar as dinâmicas de poder nelas estabelecidas, conduzindo, ainda, a uma fragilização do controlo exercido pelos governos dos países. É um domínio que apresenta uma grande facilidade de acesso e ocultação, com circulação de enormes volumes informação de forma praticamente instantânea e sem controlo, oferecendo, desta forma, uma assimetria de exercício do poder (ainda que os atores com mais recursos continuem a ter muito mais probabilidades de êxito nas suas ações). No contexto do ciberterrorismo e radicalização, constata-se que, atualmente, indivíduos ou organizações terroristas, continuam a privilegiar o mundo físico convencional para os seus golpes, em prejuízo dos ataques em que os alvos são recursos no ciberespaço. Cientes do poder das imagens mediáticas e dos cenários trágicos de terror, que provocam medo na mente das populações, estes agentes mal-intencionados preferem utilizar a internet como meio para aumentar a eficácia dos seus ataques convencionais, sendo poucos, ou inexistentes de forma claramente assumida, os registos de ataques terroristas com efeitos no próprio ciberespaço.

Não obstante esta tendência preferencial, para as ações de terrorismo e radicalização, seria perigoso descurar, não só o atual nível de utilização do ciberespaço pelas organizações terroristas, como as possibilidades ainda não exploradas, por estes indivíduos ou organizações, que constituem verdadeiras ameaças à nossa sociedade, como é o caso de eventuais ataques direcionados às infraestruturas críticas. A evolução tecnológica e do bem-estar social fez com que infraestruturas, como redes de energia ou águas, estejam, atualmente, quase na totalidade, dependentes de sistemas e comunicações instalados no ciberespaço. Um ataque aos sistemas que controlam infraestruturas críticas pode ter consequências dramáticas, no limite catastróficas para as nossas sociedades.

Com o objetivo de combater o ciberterrorismo e a radicalização, há que compreender os agentes com capacidade de intervenção no ciberespaço, as possibilidades das suas ações no âmbito dos instrumentos de poder oferecidos por este ambiente, e as estratégias de combate eficazes a diversos níveis. É importante ainda perceber que a atuação deverá estar assente sobre pilares estratégicos e estruturais muito fortes, nomeadamente numa definição de uma estratégia global da informação e uma coordenação muito clara e eficaz entre os domínios militar e civil.

Estamos na presença de desafios com contornos diferentes daqueles que estávamos habituados no passado, problemas sistémicos e holísticos, que exigem abordagens de colaboração e coordenação, a escalas globais, quer dos Estados e das forças de defesa e segurança, quer das empresas e cidadãos. Resolver os problemas das socie-

dades contemporâneas com metodologias do passado, baseadas em silos e centradas em competências específicas, ignorando a partilha e o diálogo, não produzirá certamente os efeitos que se desejam. Acresce que o tempo de reação aos acontecimentos não permitirá que cheguemos a essa conclusão de forma vagarosa, pelo que urge atuar, reforçando e melhorando todas as iniciativas nacionais e europeias já implementadas, assegurando ainda, ao nível da governação, acordos para estratégias eficazes de longo prazo, de modo a assegurar um melhor bem-estar às próximas gerações.

Finalmente, existe um aspeto fundamental que deverá estar presente em qualquer estratégia de combate ao ciberterrorismo e radicalização, trata-se do respeito que Estados e organizações deverão ter em relação aos direitos humanos e às legislações em vigor, em que a Lei de Proteção de Dados Europeia é um exemplo relevante. É crucial, para confiança nas sociedades democráticas, deixar claro que as medidas de contraterrorismo e o respeito pelos direitos humanos não são objetivos conflituosos. Não é necessário sacrificar os direitos adquiridos das nossas sociedades democráticas em prol de estratégias de combate ao terrorismo. São efetivamente finalidades complementares, em espaços colaborantes, e não conflituosas.

Bibliografia

- Buck, S. J., 1998. *The Global Commons: An Introduction*. Washington: Island Press.
- Department of Defense (DoD), 2007. *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication 1-02, 12 April 2001 as amended through 17 October 2007. Washington: The Joint Staff. [online] Disponível em: <https://marineparents.com/downloads/dod-terms.pdf>
- DOMO, 2017. Data Never Sleeps 5.0. *DOMO* [online]. Disponível em: <https://www.domo.com/learn/data-never-sleeps-5> [acedido 16 outubro 2018].
- European Union Agency for Network and Information Security (ENISA), 2016. *ENISA Threat Landscape 2015*, janeiro, ENISA. [online] Disponível em: https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport [acedido em 18 de outubro de 2018]
- EU Blockchain Observatory and Forum, 2018. *Blockchain Innovation in Europe*. Workshop report, EU Blockchain Observatory and Forum, European Commission, Rathaus Vienna, 22 de maio. [online] Disponível em: https://www.eublockchainforum.eu/sites/default/files/reports/20180613_workshop_report_blockchain_innovation_europe.pdf
- Fleishman, G., 2000. Cartoon Captures Spirit of the Internet. *The New York Times* [online], 14 de dezembro. Disponível em: <https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html> [acedido em 18 de outubro de 2018].
- Gramer, R., 2017. Denmark Creates the World's First Ever Digital Ambassador. *Foreign Policy* [online], 27 de janeiro, 2:37 PM. Disponível em: <https://foreignpolicy.com/2017/01/27/>

denmark-creates-the-worlds-first-ever-digital-ambassador-technology-europe-diplomacy [accedido em 18 de outubro de 2018].

Harris, S., 2009. The Cyberwar Plan. *National Journal*, 13 November, Washington.

Lachow, I., 2009. Cyber Terrorism: Menace or Myth? Em Franklin Kramer, Stuart Starr e Larry Wentz, eds., *Cyberpower and National Security*. Washington: Center for Technology and National Security Policy, National Defense University Press, pp. 437-464.

LaFraniere, S. e Ansfeld, J., 2010. Cyberspying Fears Help Fuel China's Drive to Curb Internet. *The New York Times*. [accedido em 18 de outubro de 2018].

Nunes, P. V., 2015. *Sociedade em Rede, Ciberespaço e Guerra de Informação: Contributos para o Enquadramento e Construção de uma Estratégia Nacional da Informação*. Lisboa: Instituto da Defesa Nacional.

Nye Jr., J., 2010. *Cyber Power*, maio. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School. [online] Disponível em: <https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf> [accedido em 18 de outubro de 2018].

Pollitt, M., 1997. Cyberterrorism: Fact or Fancy? Conference Paper, *20th National Information Systems Security Conference*, October 7-10, Baltimore, Maryland. Disponível em National Institute of Standards and Technology (NIST): <https://csrc.nist.gov/publications/detail/conference-paper/1997/10/10/proceedings-of-the-20th-nissc-1997>

Roy, O., 2010. Recruiting Terrorists. *International Herald Tribune*, 11 de janeiro.

Tsagourias, N. e Buchan, R., eds., 2015. *Research Handbook on International Law and Cyberspace*. Cheltenham: Edward Elgar Publishing.

United Nations Office on Drugs and Crime (UNODC), 2012. *The use of the Internet for terrorist purposes*. Nova Iorque: United Nations Publication. Disponível em: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

O Terrorismo Transnacional Contemporâneo: Segurança, Justiça e Cooperação

Luís Elias

Superintendente da PSP e atual Diretor do Departamento de Operações na Direção Nacional da PSP. Doutorado em Ciência Política na Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa. Licenciado em Ciências Policiais no Instituto Superior de Ciências Policiais e Segurança Interna. É Coordenador do Mestrado em Ciências Policiais e Docente no Instituto Superior de Ciências Policiais e Segurança Interna.

Resumo

O terrorismo é uma das ameaças mais relevantes à estabilidade e segurança dos Estados de direito democráticos e não só, aumentando os sentimentos de insegurança e potenciando políticas que apostam sobretudo na reação musculada, em detrimento da prevenção e inteligência.

A relação entre a criminalidade e o terrorismo, a propaganda online, o recrutamento e a radicalização, são realidades que exigem respostas multidisciplinares e dinâmicas. O terrorismo de inspiração religiosa apresenta-se hoje como uma das ameaças mais mediatizadas, mas outras formas de ação violenta mantêm-se presentes e necessitam de respostas igualmente eficazes.

Analisaremos o papel da Segurança e Justiça, bem como das Forças e Serviços de Segurança, Serviços de Informações e Forças Armadas; a investigação e debate promovidos pelas universidades e *think tanks*, num contexto marcado pela complexidade, pelo mediatismo e pelo papel das redes sociais.

Abstract

Contemporary Transnational Terrorism: Security, Justice and Cooperation

Terrorism is one of the most relevant threats to the stability and security of democratic states and not only, increasing feelings of insecurity and policies that focus mainly on the muscular reaction, to the detriment of prevention and intelligence.

The relationship between crime and terrorism, online advertising, recruitment and radicalization are realities that require multidisciplinary and dynamic responses. Terrorism of religious inspiration is today one of the most mediated threats, but other forms of violent action remain present and require equally effective responses.

We will analyze the role of Internal Security and Justice. The importance of Security Forces and Services, Intelligence Services and Armed Forces, as well as the research and debate promoted by universities and think tanks in a context marked by complexity, media and social networks.

Introdução

Os índices positivos de segurança em Portugal, conjugados com a ameaça terrorista no Norte de África, no Médio Oriente e em diversos Estados europeus, têm ajudado ao investimento e desenvolvimento do nosso país, em particular, da atividade turística, contribuindo para consolidar os padrões nacionais de qualidade de vida e de competitividade económica face a outros Estados.

Abordaremos o terrorismo transnacional como uma das principais ameaças à estabilidade das sociedades contemporâneas e também aquela que tem sido mais tratada nas últimas décadas nos meios científicos, nos órgãos de comunicação social e na análise estratégica, operacional e tática das polícias, dos serviços de informações e das forças armadas.

Embora tenhamos consciência que tem consequências muito menos tangíveis e imediatas na segurança das comunidades e no quotidiano dos cidadãos do que a criminalidade de massa, a criminalidade violenta e grave, a criminalidade organizada, incluindo os tráficos de drogas, de armas e de seres humanos, o terrorismo inspira um grande sentimento de insegurança nas opiniões públicas.

Apesar de se configurar como uma ameaça moderada em diversos países, o terrorismo alimenta-se da mediatização, tem um enorme impacto político e influencia de forma determinante as estratégias e políticas de segurança, defesa e justiça, tendo uma enorme capacidade de alterar o estilo de vida nos países com maiores índices de desenvolvimento.

1. Indicadores Oficiais Sobre Segurança

Optamos por apresentar alguns relatórios estatísticos, demonstrando a posição privilegiada de Portugal na atualidade no quadro dos indicadores de segurança que reputamos mais significativos, em termos internacionais. A manutenção destes indicadores é imprescindível como garante da estabilidade política e social e como vantagem competitiva em termos económicos.

As novas ameaças são mais diversificadas, menos visíveis e menos previsíveis. A maioria das estratégias e relatórios internacionais debruçam-se sobre as ameaças transnacionais que têm maior impacto nas nossas sociedades, sendo identificadas invariavelmente ameaças de origem humana como o terrorismo, a criminalidade organizada, a criminalidade violenta e grave, as ciberameaças, ou ainda acidentes de origem dolosa ou negligente, por exemplo em centrais nucleares, na indústria química, na indústria petrolífera, nas celuloses. Quanto às ameaças naturais são referidos diferentes tipos de catástrofes: sismos, incêndios florestais, cheias, poluição, entre outras. Podemos ainda acrescentar as crises económico-financeiras e crises bolsistas, as epidemias e os problemas na segurança alimentar e as crises energéticas. Percorremos alguns relatórios internacionais que identificam e analisam as principais ameaças e riscos transnacionais potencialmente geradoras de crises pontuais ou sistémicas.

A Estratégia Europeia em Matéria de Segurança: uma Europa Segura num Mundo Melhor de 12 de dezembro de 2003 encontra-se direcionada para a segurança externa da UE. Neste relatório são mencionados: o terrorismo global ligado ao extremismo religioso de caráter violento, a proliferação das armas de destruição massiva (ADM), os conflitos regionais e a criminalidade organizada.

A Estratégia de Segurança Interna da União Europeia: Rumo a um Modelo Europeu de Segurança, de março de 2010, aponta como principais ameaças à União Europeia: terrorismo, criminalidade violenta e grave, a cibercriminalidade, a criminalidade transfronteiriça e a violência.

A Agenda Europeia para a Segurança apresentada em 28 de abril de 2015 preconiza uma resposta forte da UE ao terrorismo e ao fenómeno dos combatentes terroristas estrangeiros. É referido também que a criminalidade transnacional grave e organizada identifica novos domínios de operação e novas formas para escapar à deteção por parte dos órgãos de policia criminal. A cibercriminalidade é considerada uma ameaça crescente para os direitos fundamentais dos cidadãos e a economia, assim como para o correto desenvolvimento de um mercado único digital.

No quadro das conclusões do Conselho sobre a *Estratégia Renovada de Segurança Interna da União Europeia para 2015-2020*¹ são identificadas as seguintes prioridades para os próximos anos, no domínio da segurança interna da União: combater e prevenir o terrorismo, a radicalização para o terrorismo e o recrutamento; prevenir e lutar contra a criminalidade grave e organizada e prevenir e lutar contra a cibercriminalidade e reforçar a cibersegurança. É igualmente sublinhado que a UE e os Estados-membros, de acordo com as respetivas competências, deverão: 1) melhorar a troca e a acessibilidade das informações, em especial garantindo a interoperabilidade dos diferentes sistemas de informação e incentivando a escolha mais adequada do canal de intercâmbio das informações pertinentes, dentro do quadro jurídico existente; 2) reforçar a cooperação operacional; 3) melhorar a prevenção e a investigação de atos criminosos, com especial incidência na criminalidade financeira organizada e no confisco dos produtos do crime e de ataques terroristas, incluindo a prevenção da radicalização e a salvaguarda dos valores através da promoção da tolerância, da não discriminação, das liberdades fundamentais e da solidariedade em toda a União Europeia; 4) melhorar as possibilidades de formação, financiamento, investigação e inovação, desenvolvendo em particular uma política de segurança industrial autónoma, em domínios como o controlo das fronteiras, a interoperabilidade de equipamentos de segurança e a ação policial; 5) desenvolver e promover a disponibilidade e a utilização de tecnologias fiáveis e seguras de informação e comunicação, a fim de melhorar a cibersegurança na UE.

1 Doc. 9798/15, de 10 de junho de 2015, JAI 442 COSI 67.

No *Conceito Estratégico de Defesa Nacional* (CEDN), aprovado pela Resolução do Conselho de Ministros n.º 19/2013 de 5 de abril, é mencionado que Portugal se depara com ameaças de natureza global que podem pôr em causa a sua segurança: o terrorismo, uma vez que a liberdade de acesso e a identidade de Portugal como uma democracia ocidental podem tornar o país um alvo do terrorismo internacional; a proliferação de ADM; a criminalidade transnacional organizada, uma vez que a posição geográfica de Portugal como fronteira exterior da UE e o vasto espaço aéreo e marítimo sob sua jurisdição impõem-lhe particulares responsabilidades; a cibercriminalidade; a pirataria, não só pela dependência energética e alimentar e pela importância do transporte marítimo para a economia nacional, mas também pelas crescentes responsabilidades nacionais na segurança cooperativa dos recursos globais. No CEDN é sublinhado igualmente que Portugal está sujeito a vários riscos ambientais e tem que melhorar a sua capacidade de prevenção, adaptação e resposta rápida aos seguintes desafios: alterações climáticas, riscos ambientais e sísmicos; ocorrência de ondas de calor e de frio; atentados ao ecossistema, terrestre e marítimo, como sejam a poluição, a utilização abusiva de recursos marinhos e os incêndios florestais; pandemias e outros riscos sanitários.

Nos termos do *Global Risks Report* de 2019 do Fórum Económico Mundial, os dez riscos mais relevantes em termos de probabilidade de ocorrência são: 1.º fenómenos meteorológicos extremos; 2.º fracasso na mitigação e adaptação às mudanças climáticas; 3.º os desastres naturais; 4.º fraude e furto de dados; 5.º ciberataques; 6.º desastres ambientais provocados pelo Homem; 7.º migrações involuntárias em larga escala; 8.º perda de biodiversidade e colapso do ecossistema; 9.º crise de água; 10.º bolha de ativos em termos macroeconómicos.

Os dez riscos mais relevantes em termos de impacto são: 1.º as armas de destruição massiva; 2.º fracasso na mitigação e adaptação às mudanças climáticas; 3.º fenómenos meteorológicos extremos; 4.º crise de água; 5.º os desastres naturais; 6.º perda de biodiversidade e colapso do ecossistema; 7.º ciberataques; 8.º quebra do sigilo de informações sobre infraestruturas críticas; 9.º desastres ambientais provocados pelo Homem; 10.º propagação de doenças infecciosas. Os riscos atrás elencados poderão, de forma individual ou combinada, ser causadores de crises pontuais ou de crises sistémicas ou em crises em cadeia.

Segundo o *Relatório da Competitividade Global (2017-2018)* do Fórum Económico Mundial, Portugal encontra-se em 42.º lugar no índice de países com uma economia mais competitiva em 137 Estados. Neste âmbito, salientamos alguns indicadores parciais relativos a Portugal: encontra-se em 16.º lugar no pouco impacto causado pelo terrorismo na economia (15.º em 2016/2017), em 11.º no reduzido impacto provocado pela criminalidade e violência (10.º em 2016/2017), em 15.º lugar na reduzida influência que a criminalidade organizada tem na competitividade da nossa economia (12.º em 2016/2017), em 28.º no grau de confiança em relação às

polícias (31.º em 2016/2017), em 35.º lugar na independência do sistema judicial (40.º em 2016/2017) e em 60.º lugar no grau de confiança que os cidadãos têm no poder político (69.º lugar em 2016/2017).

Paradoxalmente, na Resolução do Conselho de Ministros n.º 134/2017 de 27 de setembro que aprova a *Estratégia para o Turismo 2027*, o termo “segurança” só é mencionado duas vezes. Como aspetos positivos são referidos: a autenticidade com modernidade e preservação do destino; as pessoas e a hospitalidade; a História e a Cultura; Portugal surpreende, supera expectativas; a diversidade de oferta e a liberdade para viajar; o aumento das acessibilidades aéreas; a relação preço/qualidade de serviço e, ainda, a segurança. Também entre os ativos emergentes, que começam a ser reconhecidos internacionalmente e que apresentam elevado potencial de crescimento, para a opção de viver em Portugal é sublinhada a segurança. Conforme apresentado, parece-nos que é muito escassa a importância atribuída à segurança, parecendo indiciar uma noção de “dado adquirido”, o que não nos parece ser uma postura adequada. Os elevados índices de segurança são resultado de muitos fatores, mas certamente são produto do bom trabalho das Forças e Serviços de Segurança e este valor não aparece repercutido em vários documentos oficiais com o devido destaque, como é o caso do acima apresentado.

O relatório do Eurobarómetro 432, resultados para Portugal, da responsabilidade da Comissão Europeia, designado por *Atitudes dos Europeus em Relação à Segurança*, de abril de 2015, é também uma referência importante para perspetivar o sentimento de segurança no velho continente. No relatório de 2015 é efetuada uma análise comparativa com outro inquérito equivalente realizado em 2011.

Numa questão relativa à perceção de segurança dos cidadãos, 53% dos inquiridos em 2015 (53% em 2011) concordam totalmente que o local onde residem é seguro; 47% concordam completamente que a sua cidade é segura em 2015 (49% em 2011); 35% concordam em 2015 totalmente que o país onde residem é seguro (36% em 2011); 27% concordam completamente que a União Europeia como um todo é uma região segura (28% em 2011). Como se constata, o sentimento de segurança é tanto mais diluído, quanto mais o inquirido se afasta do objeto em análise: da vizinhança ou bairro, passando pela cidade, pelo país e finalmente pela UE.

Cerca de 35% dos entrevistados consideraram que a situação económica e do emprego no seu país têm um impacto negativo sobre o sentimento de segurança.

A proporção de europeus que consideraram o terrorismo, o crime organizado e o extremismo religioso como os principais desafios para a segurança da UE, aumentou consideravelmente desde 2011. É de notar que 49% dos entrevistados em 2015 entenderam o terrorismo como a principal ameaça, em comparação com 33% em 2011. No respeitante ao crime organizado, em 2015, 23% consideram-no a principal ameaça, enquanto em 2011 eram 21%. Em relação ao extremismo religioso, em 2015,

20% veem o extremismo religioso como a ameaça mais preocupante, enquanto em 2011 apenas 9% o consideram desta forma.

Em outro capítulo do inquérito, verificou-se um aumento significativo na proporção dos cidadãos europeus que pensam que o terrorismo é um desafio muito importante para a segurança interna da UE – 65% em 2015 e 58% em 2011. As ideologias extremistas, a guerra e a instabilidade política nos países vizinhos da UE, são vistos como as fontes de ameaça mais prováveis à segurança dos Estados-membros da UE. Cerca de dois terços dos entrevistados pensam que a ameaça do terrorismo é suscetível de aumentar ao longo dos próximos três anos.

Salienta-se ainda que 68% dos entrevistados consideram a Polícia, 61% o Sistema Judicial e 46% as Forças Armadas como sendo os principais responsáveis por garantir a segurança dos cidadãos nos Estados-membros da UE. A maioria dos entrevistados afirmou que a Polícia e outras agências de aplicação da lei estão a fazer o suficiente para combater o terrorismo (61%) e o tráfico de droga (53%).

Finalmente, segundo o *Relatório Anual de Segurança Interna (RASI) de 2018* “a criminalidade em Portugal apresenta níveis inferiores à média registada na União Europeia (UE) (...). Entre a aprovação da atual Lei de Segurança Interna, através da Lei no 53/2008 de 29 de agosto e o ano de 2018, a criminalidade geral passou de 421.037 participações para 333.223 (redução de 20,9%) e, dentro desta, a criminalidade violenta e grave diminuiu de 24.317 participações para as 13.981 (redução de 42,5%). Atualmente a criminalidade violenta e grave representa apenas 4,2% de toda a criminalidade participada” (SSI, 2018).

No que concerne à ameaça terrorista, o *RASI de 2018* sublinha que “a existência de uma elevada ameaça terrorista no entorno geográfico de Portugal, i.e., a própria UE e as regiões vizinhas – que se caracteriza por uma paisagem estratégica marcada pelos conflitos regionais e instabilidade endémica – implica, simultaneamente, riscos de projeção em perigos para os interesses e cidadãos nacionais radicados nessas regiões. Os agentes da potencial ameaça terrorista à Europa e a Portugal pertencem, sobretudo, a duas entidades transnacionais que se encontram envolvidas numa disputa ideológico-operacional pela liderança da *Jihad* global. Estas duas organizações são complementares, na sua capacidade de agregar diferentes correntes *jihadistas*, pondo em prática planos divergentes e concorrentes: (i) a *Al Qaida* (AQ) e a sua rede de filiais; e, (ii) o Grupo Estado Islâmico (GEI), as suas divisões territoriais designadas *wilayat* e os extremistas que juraram fidelidade a Abu Bakr al-Baghdadi” (SSI, 2018, p. 76).

2. Definições de Terrorismo

O terrorismo pode ser entendido como “o uso de força física para atingir um adversário político” (Della Porta, 1995, p. 2), como “violência – ou a ameaça de violência – utilizada e dirigida em busca de, ou em serviço de um objetivo político”

(Hoffman, 2006, p. 3) ou, ainda, como “uma ação violenta premeditada e ilegal contra uma população não-combatente ou tendo um alvo com significado simbólico, com o objetivo de provocar uma mudança política, através da intimidação e desestabilização ou vitimando a população identificada como inimiga” (Forst, 2009, p. 5). Trata-se, no entanto, de um termo, cuja definição apresenta dificuldades, designadamente para distinguir o terrorismo de outras formas de atividade política que utilizem alguma forma de coação ou ação direta violenta para alcançar um objetivo político. O terrorismo, em geral, tem subjacente uma ideologia política, podendo lutar por causas ou reparar injustiças sofridas pelas comunidades, das quais os terroristas derivam (Toolis, 1995, p. 39). A definição operacional de terrorismo utilizada pelo FBI na década de 90 foi a seguinte: “o uso de violência contra pessoas ou propriedade, ou ameaça de uso dessa violência, com vista a intimidar ou coagir um governo, o público ou qualquer setor do público, a fim de promover objetivos políticos, sociais, ideológicos ou religiosos” (Lloyd, 1996, § 5.22).

Embora estas definições de terrorismo enfatizem o “fator medo” – incluindo a ameaça do uso de violência –, a guerra convencional geralmente utiliza táticas com o objetivo de criar também temor no inimigo – por exemplo, através do recurso a ataques sucessivos com vista à saturação do inimigo ou recorrendo ao bombardeamento de alvos inimigos em aglomerados populacionais.

O terrorismo é um fenómeno intrinsecamente político, o que significa que as pessoas ou organizações que optam pelo terrorismo atuam por descontentamento em relação à sociedade e aos poderes que a organizam e a estruturam. É um conceito subjetivo influenciado pelas conceções políticas de cada um – para algumas pessoas uma ação violenta pode ser terrorista, para outras pode ser considerada como um ato legítimo com o objetivo de defender uma determinada causa. A guerra civil que eclodiu na Síria desde 2011 simboliza em grande medida este dilema: o governo do Presidente Bashar al-Assad e os seus aliados catalogam os rebeldes como terroristas, enquanto para muitos países algumas das fações existentes no teatro de operações são vistas como opositores legítimos de um regime tirânico. O terrorismo é, deste modo, um termo que é quase sempre utilizado de forma pejorativa, “o rótulo utilizado pelo ameaçado” (Morris e Hoe, 1987, p. 22) em relação a uma organização, grupo ou indivíduo.

Quando o Estado é o destinatário final da violência, em regra, os terroristas não procuram a confrontação direta com as Forças e Serviços de Segurança ou com as Forças Armadas, procuram, sim, atacar a população civil de forma indiscriminada como estratégia para obtenção de visibilidade política para a organização ou para a causa suportada e como forma de pressão. Podem, porém, executar ataques seletivos e cirúrgicos a equipas ou unidades das Forças Armadas ou das Forças de Segurança, polícias e militares isolados, juizes, entre outros por serem símbolos da autoridade do Estado.

O terrorismo é retratado como uma forma de violência “para os desprotegidos” (Combs, 2009), que não têm recursos para se envolverem em confrontos mais convencionais, o que, na nossa opinião, é controverso e nem sempre é verdade na prática, já que em muitos casos os promotores da ação direta não são propriamente desfavorecidos ou excluídos socialmente, casos do terrorismo de Estado promovido por diversos regimes autoritários e de organizações em que a violência é assumida como uma estratégia e/ou tática para impor pela força ideias de supremacia, racistas, extremistas ou que visem alterar o nosso modelo de sociedade – casos do Ku Klux Klan, da seita religiosa japonesa Aum e de diversos grupos anarquistas ou de extrema-direita.

Os terroristas procuram atingir os seus objetivos através de uma “guerra” de atrito, que pode envolver táticas que procuram sobretudo intimidar os cidadãos, não sendo a sua conduta limitada pela Convenção de Genebra e por outras convenções internacionais, mas apenas pela Lei Penal. O propósito do terrorismo “não é uma vitória militar, é atemorizar, mudar o comportamento das potenciais vítimas, criando o medo hoje, o medo amanhã e o medo das diversas sociedades entre si”². Esta última frase sugere, assim, que a tentativa de criar tensões na nossa sociedade entre grupos religiosos, raciais ou étnicos, constitui em geral um objetivo específico das campanhas terroristas conduzidas nas sociedades multiculturais hodiernas.

O terrorismo é, muitas vezes, confundido ou equiparado a guerrilha ou insurgência, dada a semelhança de táticas e de objetivos. Hoffman distingue estes três fenómenos: a guerrilha diz respeito a um grupo de indivíduos armados que operam como uma unidade militar, atacam as forças militares do adversário e procuram ganhar ou controlam um determinado território e população; a insurgência incorpora as mesmas características, embora a sua estratégia vá para além de táticas de ataque e fuga, incluindo ainda atos de guerra psicológica com vista à mobilização do apoio popular numa luta contra um governo, poder imperial ou força de ocupação estrangeira; pelo contrário, os terroristas não desejam ocupar qualquer território, não operam em unidades militares, evitam chamar as forças militares do inimigo para o combate, enfrentam constrangimentos numéricos e logísticos e não exercem qualquer controlo sobre uma população (Hoffman, 2006, pp. 35-36).

Nos últimos anos, vários autores têm vindo a delinear uma distinção entre o que é designado por “velho terrorismo” e “novo terrorismo”. Embora a expressão de “novo terrorismo” tenha sido utilizada desde a década de 1990, os ataques de 11 de Setembro de 2001 intensificaram o debate sobre se o terrorismo contemporâneo é diferente daquele que tinha existido até então. A discussão nos meios académicos e no seio das Forças de Segurança, Serviços de Informações e Forças Armadas

2 Palestra do ex-Presidente norte-americano, Bill Clinton, na London School of Economics sobre Terrorismo em 13 de dezembro de 2001.

identificou, no início do século XXI, a Al-Qaeda como o protótipo do novo terrorismo sustentado no desígnio de expandir a violência em termos globais, no fanatismo religioso e na demanda de destruição dos valores e do modelo de sociedade ocidentais.

As principais características deste alegado “novo terrorismo” tem vindo a ser identificadas como sendo “estruturado em torno de redes em vez de ser uma organização hierarquizada, transnacional ou com base local; procura alvos civis de forma deliberada; é motivado pelo fanatismo religioso, ao invés de se inspirar numa ideologia política; e destinado a causar a máxima destruição” (Gofas, 2012, p. 18).

Morgan (2004, p. 29) defende que o novo terrorismo é “apocalíptico e catastrófico”, pelo que a violência extrema é vista como “um fim em si mesmo, em vez de um meio para se atingir um fim” (Morgan, 2004, p. 30). São apontados “os riscos associados ao terrorismo transnacional, que professa uma cultura de suicídio, martírio e destruição, com uma inaceitável magnitude potencial de destruição e desafiando as tradicionais abordagens sobre dissuasão e racionalidade” (Tomé, 2007).

Todavia, mantém-se a discussão nos *think tanks* e universidades para avaliar até que ponto o terrorismo atual é de facto “novo”. O terrorismo inspirado pela religião existe desde a década de 1970, já para não abordar outros exemplos históricos mais remotos. A visão de que o novo terrorismo se baseia numa organização diferente e é caracterizado por uma rede internacional de células e de apoio ligeiramente conectadas, em vez de se organizar de forma hierarquizada, piramidal e de possuir uma estrutura de comando e controlo localizada num Estado ou região específica foi contestada pela noção de que os grupos terroristas “tradicionais” como o “IRA provisório” concederam um grau de autonomia muito elevado às suas diferentes células (Gofas, 2012, p. 23). Além disso, embora “a religião seja uma característica da atividade terrorista contemporânea” (Gofas, 2012, p. 26), tais motivações ou inspirações não são inéditas, podendo ser constatadas, por exemplo, nos Zelotas do século I d.C.

É de referir que os ataques indiscriminados que visam provocar vítimas em massa foram igualmente característicos do terrorismo pré-11 de setembro de 2001 (Gofas, 2012, p. 28), não sendo um sinónimo apenas da ação violenta da atualidade. Arguir que a natureza religiosa e jihadista do terrorismo atual, o caracteriza como uma nova forma de violência constitui um método eficaz de enquadrar a ameaça e de mobilizar tanto o público como as elites, com vista à mudança de políticas (Gofas, 2012, p. 19), favorecendo ainda a afetação de mais recursos no quadro da prevenção e combate ao terrorismo. De igual modo, a dicotomia “velho” *versus* “novo”, trata-se de uma forma de simplificação da realidade, de certa forma menosprezando a complexidade do contexto social, histórico e cultural, subjacente a diversas formas de terrorismo e ajudando a chamar a atenção dos *media*.

O terrorismo tem diversas causas e orientações, assumindo-se ao longo da história, como um recurso tático, fora do contexto de guerra, de diversos tipos de organizações sociais ou políticas, de motivação distinta, decorrente de conflitos/crises religiosas, sociais ou políticas.

A RAND Corporation³ define o terrorismo baseando-se na natureza do ato e não na identidade do autor ou na natureza da causa. Inclui elementos fundamentais na sua definição, entre os quais se contam a violência ou ameaça de violência, a intenção calculada de criar medo, a intenção de coagir, o motivo político, o alvo civil e, finalmente, se se trata de um grupo ou de um indivíduo.

No Reino Unido, de acordo com o *Terrorism Act 2000*, revisto sucessivamente em 2003, 2005, 2006, 2008, 2009, 2010, 2013 e 2015⁴ o terrorismo consubstancia-se “no uso ou ameaça de ação violenta com o objetivo de influenciar o governo ou uma organização internacional governamental, intimidar o público ou um setor do público, com o propósito de fazer progredir uma causa religiosa, racial ou ideológica. Envolve ou provoca: violência grave contra uma pessoa; graves danos materiais; uma ameaça à vida de uma pessoa; um risco grave para a saúde e segurança do público; ou interferência grave com ou perturbações num sistema eletrónico”. Os alvos vulneráveis, a componente psicológica, a ação violenta e o fator político, religioso, racial, ou ideológico, englobam também a mais recente vertente técnica e eletrónica da ameaça, ou seja, o ciberterrorismo.

A ONU adotou em 2004, a seguinte definição de terrorismo: “atos criminosos, incluindo contra civis, cometidos com a intenção de causar a morte ou danos físicos graves, ou tomada de reféns, com o objetivo de provocar um estado de terror no público em geral, num grupo de pessoas, ou numa pessoa em particular, intimidar a população ou forçar um governo ou uma organização internacional a adotar ou deixar de tomar qualquer ação, conforme definido nas convenções e protocolos internacionais relacionados com o terrorismo, não podendo, em caso algum, ser justificados por razões de natureza política, filosófica, ideológica, racial, étnica, religiosa ou outra semelhante” (United Nations Security Council, 2004)⁵.

3 Disponível em RAND Corporation [website] <http://www.rand.org/nsrd/projects/terrorism-incidents/about/definitions.html>, consultada em 20 de outubro de 2016. A RAND Corporation é uma organização de investigação que desenvolve soluções para fazer face aos desafios das políticas públicas, com vista a ajudar as comunidades ao nível mundial a ficarem mais seguras.

4 No Reino Unido, a estratégia de combate ao terrorismo tem tido revisões sucessivas: *The Terrorism Act 2000*, *The Anti-terrorism, Crime and Security Act 2001*, *The Criminal Justice Act 2003*, *The Prevention of Terrorism Act 2005*, *The Terrorism Act 2006*, *The Counter-Terrorism Act 2008*, *The Coroners and Justice Act 2009*, *The Terrorism (United Nations Measures) Order 2009*, *The Terrorist Asset-Freezing (Temporary Provisions) Act 2010*, *The Justice and Security Act 2013*, *The Counter-Terrorism and Security Act 2015*.

5 Definição adotada na *United Nations Security Council Resolution 1566*, em 2004.

Por sua vez, a União Europeia (2002) considera que o terrorismo é “um ato que, dada a sua natureza ou o seu contexto, possa causar sérios danos a um país ou a uma organização internacional quando cometido com o intuito de: intimidar gravemente uma população, ou obrigar indevidamente autoridades públicas ou uma organização internacional a praticar ou abster-se de praticar qualquer ato, ou desestabilizar gravemente ou destruir as estruturas políticas, constitucionais, económicas ou sociais fundamentais de um país ou de uma organização internacional”.

A Europol (2018) no seu relatório anual da ameaça terrorista *European Union Terrorism Situation and Trend Report 2018* subdivide o terrorismo em cinco categorias, baseando-se na motivação ideológica das organizações ou indivíduos: terrorismo de inspiração religiosa, terrorismo etnonacionalista e separatista, terrorismo de extrema-esquerda e anarquista, terrorismo de extrema-direita e terrorismo de causa única ou *single issue*.

O terrorismo de inspiração religiosa tem como suporte ideológico uma interpretação radical ou fundamentalista da religião – ex.: Al-Qaeda e suas afiliadas, Daesh, entre outros.

O terrorismo etnonacionalista ou separatista visa a autodeterminação política e o reconhecimento internacional – ex.: ETA, IRA, Resistência Galega, Frente de Libertação da Córsega, PKK ou outros.

O terrorismo de extrema-esquerda ou anarquista procura a alteração do sistema político, social e económico segundo um modelo de extrema-esquerda ou libertário – ex.: Conspiração das Células de Fogo.

O terrorismo de extrema-direita procura a alteração do sistema político, social e económico segundo um modelo de extrema-direita – ex.: National Socialist Underground, English Defence League, Aurora Dourada.

O terrorismo *single issue* promove a violência com a intenção de alterar uma política ou prática numa sociedade-alvo, estando muito relacionado com causas ambientalistas – ex.: Animal Liberation Front e Earth Liberation Front.

Independentemente da motivação ideológica, o terrorismo partilha uma intenção comum que se traduz na provocação de um sentimento generalizado de medo, através da evocação da atenção de uma audiência, visando limitar ou impedir que a vida em sociedade se desenvolva em normalidade. Como referem Jenkins e Johnson (1975, p. 3), o terrorismo destina-se mais a quem observa e não às suas vítimas.

Para a NATO (2016), o terrorismo é definido como “o uso ilegítimo ou a ameaça de uso da força ou violência contra indivíduos ou bens na tentativa de coagir ou intimidar governos ou sociedades a atingir objetivos políticos, religiosos ou ideológicos”. A *Lei de Combate ao Terrorismo*, Lei n.º 52/2003, de 22 de agosto, define em Portugal o conceito de organização terrorista, de terrorismo, de terrorismo internacional, de financiamento do terrorismo e a responsabilidade penal de pessoas coletivas e equiparadas. De acordo com a legislação penal portuguesa, o terrorismo é sobretudo um crime ou um conjunto de crimes interligados previstos e punidos na lei.

De acordo com o artigo 2.º da *Lei de Combate ao Terrorismo* considera-se grupo, organização ou associação terrorista todo o agrupamento de duas ou mais pessoas que, atuando concertadamente, visem prejudicar a integridade e a independência nacionais, impedir, alterar ou subverter o funcionamento das instituições do Estado previstas na Constituição da República Portuguesa, visem forçar a autoridade pública a praticar um ato, a abster-se de o praticar ou a tolerar que se pratique ou ainda intimidar certas pessoas, grupos de pessoas ou a população em geral, mediante:

- a) crime(s) contra a vida, a integridade física ou a liberdade das pessoas;
- b) crime(s) contra a segurança dos transportes e das comunicações, incluindo as informáticas, telegráficas, telefónicas, de rádio ou de televisão;
- c) crime(s) de produção dolosa de perigo comum, através de incêndio, explosão, libertação de substâncias radioativas ou de gases tóxicos ou asfixiantes, de inundação ou avalanche, desmoronamento de construção, contaminação de alimentos e águas destinadas a consumo humano ou difusão de doença, praga, planta ou animal nocivos;
- d) ato(s) que destruam ou que impossibilitem o funcionamento ou desviem dos seus fins normais, definitiva ou temporariamente, total ou parcialmente, meios ou vias de comunicação, instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população;
- e) investigação e desenvolvimento de armas biológicas ou químicas;
- f) crimes que impliquem o emprego de energia nuclear, armas de fogo, biológicas ou químicas, substâncias ou engenhos explosivos, meios incendiários de qualquer natureza, encomendas ou cartas armadilhadas;
- g) sempre que, pela sua natureza ou pelo contexto em que são cometidos, estes crimes sejam suscetíveis de afetar gravemente o Estado ou a população que se visa intimidar. Incorre também em ilícito criminal quem promover ou fundar grupo, organização ou associação terrorista, a eles aderir ou os apoiar, nomeadamente através do fornecimento de informações ou meios materiais, quem chefiar ou dirigir grupo, organização ou associação terrorista e quem praticar atos preparatórios da constituição de grupo, organização ou associação terrorista.

É de referir, também, a aprovação da Lei n.º 25/2008 de 5 de junho, *Lei do Combate ao Branqueamento de Capitais e do Financiamento ao Terrorismo*, que estabelece, no nosso país, medidas de natureza preventiva e repressiva de combate ao branqueamento de vantagens de proveniência ilícita e ao financiamento do terrorismo, transpondo para a ordem jurídica interna as Diretivas n.º 2005/60/CE, do Parlamento Europeu e do Conselho, de 26 de outubro, e 2006/70/CE, da Comissão, de 1 de agosto, relativas à prevenção da utilização do sistema financeiro e das atividades e profissões especialmente designadas para efeitos de branqueamento de capitais e de financiamento do terrorismo.

O terrorismo de inspiração fundamentalista islâmica apresenta, porém, novas características que o distinguem das abordagens mais tradicionalistas. Tem uma capacidade de organização de ações violentas de grande impacto político e mediático e de baixo custo que implicam, porém, um planeamento detalhado e profissionalismo dos atores envolvidos, mas nos últimos tempos, assume um sentido messiânico, utilizando crescentemente indivíduos que buscam um sentido para as suas vidas e que se auto radicalizam, encontrando-se permeáveis à narrativa jihadista que lhes fomenta a vontade do sacrifício pessoal em busca da fé perfeita e de matar infiéis. Estes atores solitários ou pequenos grupos ou células, em muitos casos, têm passado criminal, planeiam operações de baixo custo, inspirando-se na propaganda que divulga táticas, armas e *modus operandi* para infligir o maior número possível de vítimas.

3. A Prevenção e o Combate ao Terrorismo

Em termos nacionais, o dispositivo de prevenção e combate ao terrorismo divide-se entre as Forças e Serviços de Segurança, o sistema de Justiça e o trabalho de apoio dos Serviços de Informações. Segundo o artigo 7.º n.º 2 alínea l) da Lei n.º 49/2008 de 27 de agosto, *Lei de Organização da Investigação Criminal*, constitui competência reservada da Polícia Judiciária, através da Unidade Nacional de Combate ao Terrorismo (UNCT), a investigação dos crimes de organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo, não podendo ser deferida a outros órgãos de polícia criminal.

Os restantes atores do Sistema de Segurança Interna, nomeadamente a GNR e a PSP, representam um papel importantíssimo na prevenção – incluindo a prevenção da radicalização e a proteção de espaços públicos –, na deteção de indícios técnicos que configurem a difusão de ideologia extremista, situações de radicalização, recrutamento, a preparação de atos terroristas ou ações de apoio de logístico, de treino e na reação a incidentes críticos.

O Serviço de Estrangeiros e Fronteiras (SEF) desempenha também uma função primordial no controlo de pessoas que circulam na fronteira externa da UE, no controlo documental (passaportes e vistos), nomeadamente através do Sistema de Informação do Passaporte Eletrónico Português (SIREP), do Sistema de Informação de Vistos (VIS) e do Sistema de Informação Antecipada de Passageiros (APIS), na deteção de situações de fraude de identidade, de tráfico de seres humanos e de auxílio à imigração ilegal bem como instaurar, instruir e decidir os processos de expulsão administrativa de estrangeiros do território nacional e dar execução às decisões de expulsão administrativas e judiciais.

Saliente-se que foi recentemente incorporada no quadro do Sistema de Segurança Interna, a Unidade de Coordenação Antiterrorismo (UCAT), conforme artigo 23.º

da *Lei de Segurança Interna*⁶. Integram a UCAT: o Secretário-Geral do Sistema de Segurança Interna, o Secretário-Geral do Sistema de Informações da República Portuguesa, representantes da Guarda Nacional Republicana (GNR), Polícia de Segurança Pública (PSP), da Polícia Judiciária, do Serviço de Estrangeiros e Fronteiras (SEF), da Polícia Marítima, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS). Este é o órgão de articulação e partilha de informações, no âmbito do combate ao terrorismo, entre os serviços que a integram. Compete à UCAT a coordenação dos planos de execução das ações previstas na *Estratégia Nacional de Combate ao Terrorismo* e, no plano da cooperação internacional, a ligação entre os pontos de contato para as diversas áreas de intervenção em matéria de terrorismo.

A *Estratégia Nacional de Combate ao Terrorismo de Portugal* deriva da *Estratégia Contra-terrorista da União Europeia*, complementada pela *Estratégia da União Europeia de Combate à Radicalização e ao Recrutamento para o Terrorismo* e pelos planos de ação, relativos à sua implementação e da estratégia revista sobre o financiamento do terrorismo. Estas estratégias representam marcos importantes no combate integrado ao terrorismo, promovendo uma abordagem coesa e concertada do fenómeno, bem como o seu acompanhamento e avaliação permanentes ao nível da União Europeia. A *Estratégia Nacional de Combate ao Terrorismo* assenta nos seguintes objetivos estratégicos: detetar, prevenir, proteger, perseguir e responder:

- a) detetar: identificar precocemente potenciais ameaças terroristas, mediante a aquisição do conhecimento essencial para um combate eficaz, tanto na perspetiva do seu desmantelamento isolado, quanto da deteção de outros focos de ação terrorista. A recolha, tratamento e análise de dados e informações e a sua disponibilização recíproca entre entidades responsáveis neste domínio, no território nacional e no estrangeiro, permite antecipar o conhecimento e a avaliação de ofensivas em preparação;
- b) prevenir: conhecer e identificar as causas que determinam o surgimento de processos de radicalização, de recrutamento e de atos terroristas. O domínio dos factos que potenciam a sua expansão permite a adoção de medidas que obstem ao seu surgimento e desenvolvimento;
- c) proteger: fortalecer a segurança dos alvos prioritários, reduzindo quer a sua vulnerabilidade quer o impacto de potenciais ameaças terroristas. A proteção concretiza-se no aumento da segurança das pessoas, das fronteiras, da circulação de capitais, das mercadorias, dos transportes, da energia e das infraestruturas críticas, nacionais e ou europeias;

6 Conferir a Lei n.º 59/2015, de 24 de junho, primeira alteração à Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna, modificando a composição do Conselho Superior de Segurança Interna e a organização e o funcionamento da Unidade de Coordenação Antiterrorismo.

- d) perseguir: dismantelar ou neutralizar as iniciativas terroristas, projetadas ou em execução e as suas redes de apoio, impedir as deslocções e as comunicações e o acesso ao financiamento e aos materiais utilizáveis em atentados e submeter os fenómenos terroristas à ação da justiça;
- e) responder: gerir operacionalmente todos os meios a utilizar na reação a ocorrências terroristas. A capacidade de resposta permite limitar as suas consequências, quer ao nível humano quer ao nível das infraestruturas. A resposta incide ainda na assistência, tendo em consideração as necessidades especiais das vítimas e das testemunhas.

À partida, este documento encerra objetivos e medidas estratégicas muito ambiciosas ao nível interministerial preconizando abordagens tão diversas como a defesa, segurança interna, justiça, saúde, educação, finanças, obras públicas e ações concretas no plano operativo e mesmo tático, o que nos leva a questionar a coerência do documento e a necessidade de estabelecer um ou vários planos de ação, a candidatura a fundos da União, a calendarização de ações e respetivo acompanhamento da sua implementação e avaliação.

O intercâmbio de informações entre os Estados-membros é um instrumento decisivo para as autoridades de aplicação da lei, não só no combate à criminalidade grave e organizada, mas também às infrações de menor gravidade cometidas em grande escala, por grupos criminosos itinerantes ou por criminosos individuais que operam em vários desses países. Entre os instrumentos de apoio recomendados para adoção pelos Estados-membros na comunicação da Comissão Europeia ao Parlamento Europeu e ao Conselho salienta-se o de “Reforçar a cooperação em matéria de aplicação da lei na UE: o modelo europeu de intercâmbio de informações (EIXM)” encontra-se no *Single Point of Contact (SPOC)* ou Ponto Único de Contacto (PUC). Este projeta-se como um “balcão único”, em conformidade com as “Orientações para a criação de um ponto único de contacto para o intercâmbio internacional de informação entre serviços de polícia (Doc. 10492/14, de 13 de junho de 2014, DAPIX 75 ENFOPOL 157)”.

Neste contexto, foi publicado o Decreto-Lei n.º 49/2017 de 24 de maio, que cria, no âmbito do Sistema de Segurança Interna, na dependência e sob coordenação do Secretário-Geral do Sistema de Segurança Interna, o Ponto Único de Contacto para a Cooperação Policial Internacional (PUC-CPI), procedendo à segunda alteração à Lei n.º 53/2008, de 29 de agosto, alterada pela Lei n.º 59/2015, de 24 de junho.

Segundo o artigo 23.º A, n.º 1, da Lei n.º 53/2008, de 29 de agosto, o Ponto Único de Contacto para a Cooperação Policial Internacional (PUC-CPI) é o centro operacional responsável pela coordenação da cooperação policial internacional, que assegura o encaminhamento dos pedidos de informação nacionais, a receção, o encaminhamento e a difusão nacional de informação proveniente das autoridades policiais estrangeiras, a transmissão de informação e a satisfação dos pedidos por estas for-

mulados. O artigo 23.º A, n.º 2, estipula que compete ao PUC-CPI, designadamente: assegurar o intercâmbio internacional de informações entre os serviços de polícia, nos termos da Lei n.º 74/2009, de 12 de agosto⁷; definir critérios e dar orientações em matéria de interlocução externa no âmbito da cooperação policial internacional; garantir a operacionalidade dos mecanismos e instrumentos de cooperação policial internacional; definir e implementar boas práticas internas em matéria de cooperação policial internacional e dar execução às orientações veiculadas pelas competentes instâncias internacionais; definir os critérios para a escolha dos canais adequados para a transmissão de informações, nos termos da lei; identificar e promover a utilização de soluções de gestão de processos eficazes e definir fluxos de trabalho especificamente destinados à cooperação policial internacional em matéria de assistência jurídica mútua; assegurar a necessária articulação com as estruturas nacionais responsáveis pela cooperação judiciária internacional; assegurar a coordenação da representação externa, nas instâncias europeias e internacionais, no âmbito da cooperação policial internacional, por si, ou através dos órgãos de polícia criminal que a integram; programar e implementar ações destinadas à formação contínua dos trabalhadores em funções públicas em exercício na área da cooperação policial internacional, bem como das demais autoridades de aplicação da lei.

O artigo 23.º A, n.º 4, da Lei n.º 53/2008, de 29 de agosto, estipula que o PUC-CPI tem um Gabinete de Gestão constituído por elementos da Guarda Nacional Republicana, da Polícia de Segurança Pública, da Polícia Judiciária e do Serviço de Estrangeiros e Fronteiras, designadas(os) Coordenadores de Gabinete⁸. O n.º 9 do mesmo artigo e diploma legal prevê que a Polícia Marítima e a Autoridade Tributária e Aduaneira possam colocar elementos de ligação no PUC-CPI.

O PUC-CPI reúne, sob a mesma gestão, o Gabinete Nacional SIRENE (Supplementary Information Request at the National Entry), o Gabinete Nacional da Interpol, a Unidade Nacional da Europol, a coordenação dos oficiais de ligação nacionais e estrangeiros, a coordenação dos Centros de Cooperação Policial e Aduaneira, os pontos de contacto decorrentes das Decisões Prüm e o Gabinete de Informações de Passageiros – artigo 23.º A, n.º 6º.

7 Aprova o regime aplicável ao intercâmbio de dados e informações de natureza criminal entre as autoridades dos Estados-membros da UE, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2006/960/JAI, do Conselho, de 18 de dezembro de 2006.

8 De acordo com o artigo 2.º n.º 4 do Decreto Regulamentar n.º 7/2017, de 7 de agosto, no PUC-CPI operam as seguintes unidades orgânicas: Gabinete Nacional SIRENE; Gabinete Europol e Interpol (Unidade Nacional Europol e Gabinete Nacional Interpol); Gabinete para os Centros de Cooperação Policial e Aduaneira (CCPA); Gabinete para os Oficiais de Ligação e os Pontos de Contacto das Decisões Prüm. Mais recentemente, segundo a Lei n.º 21/2019, de 25/02, foi incluído no PUC-CPI, o Gabinete de Informações de Passageiros.

9 Segundo o artigo 3.º (Gabinete de Gestão) do Decreto Regulamentar n.º 7/2017, de 7 de agosto, o Gabinete de Gestão é constituído por elementos da Guarda Nacional Republicana, da Polícia

O PUC-CPI funciona todos os dias, 24 horas por dia, em regime de turnos e é coordenado, rotativamente, por cada um dos coordenadores de gabinete, do gabinete de gestão, o qual é denominado coordenador-geral e responsável pelo encaminhamento dos pedidos nacionais, pela decisão de distribuição dos pedidos ou informações recebidas do exterior e pela validação das respostas nacionais emitidas – artigo 23.º A, n.º 7.

O Procurador-Geral da República indica um ponto de contacto que assegura a articulação permanente entre o Ministério Público e o PUC-CPI, para o exercício das competências que lhe são próprias, no processo penal.

Outro mecanismo fundamental para a troca de informações entre as agências de aplicação da lei nos Estados-membros da UE é o Sistema de Informações Schengen (SIS). O SIS tem por objetivo ajudar a preservar a ordem e a segurança públicas, incluindo a segurança dos Estados, num contexto de livre circulação de pessoas. Visa ainda apoiar ações de controlo nas fronteiras externas e de cooperação policial, permitindo às autoridades nacionais responsáveis pela segurança pública e pelos controlos de fronteira, assim como às autoridades judiciais, obter informações sobre pessoas ou objetos.

Os Estados-membros alimentam o SIS graças a redes nacionais (N.SIS II) ligadas a um sistema central (CS-SIS II). Este sistema informático é completado por uma rede de Gabinetes Nacionais designados SIRENE, em cada um dos Estados que constitui a interface humana do SIS.

Em 9 de abril 2013 entrou em funcionamento o SIS II. Veio substituir o SIS I que se encontrava operacional desde 26 de março de 1995. O SIS II é um sistema mais evoluído tecnicamente, com novas funcionalidades e mais tipos de dados. Trata-se de um sistema informático de grandes dimensões, contendo atualmente 47 milhões de dados, de 28 Estados Schengen. O SIS II oferece novas funcionalidades: introduz melhorias relativamente às indicações sobre pessoas e objetos; introduz novas categorias de indicações de objetos – aeronaves, barcos, motores de barcos, equipa-

de Segurança Pública, da Polícia Judiciária e do Serviço de Estrangeiros e Fronteiras, designados coordenadores de gabinete. Cada coordenador de gabinete chefia uma das unidades orgânicas. Os coordenadores de gabinete são nomeados por despacho dos membros do Governo responsáveis pelas áreas da Administração Interna e da Justiça, sob proposta do Secretário-Geral do Sistema de Segurança Interna, e exercem funções em comissão de serviço pelo período de três anos. A coordenação do Gabinete de Gestão é assegurada, rotativamente e em acumulação de funções, por cada um dos coordenadores do Gabinete, nessas funções denominado coordenador-geral. O coordenador-geral é responsável pelo encaminhamento dos pedidos nacionais, pela decisão de distribuição dos pedidos ou informações recebidas do exterior e pela validação das respostas nacionais emitidas nos termos do presente decreto regulamentar, sem prejuízo das competências que lhe sejam atribuídas por delegação do Secretário-Geral do Sistema de Segurança Interna.

mento industrial, meios de pagamento; permite a interligação entre diferentes tipos de indicação; inclui dados biométricos e fotografias.

É uma base de dados policiais comum a todos os Estados Schengen, que através dela se encontram interligados. É a medida compensatória mais importante e efetiva para garantir a segurança interna dos Estados-membros e um instrumento que permite a troca de informações, através dos Gabinetes SIRENE, de determinados dados que exigem um elevado nível de segurança. Constitui a condição prévia à aplicação efetiva do acervo Schengen no território do Estado candidato e à supressão dos controlos de fronteira interna. A consulta ao SIS é obrigatória e sistemática para as entidades com direito de acesso.

As regras de funcionamento e funções dos Gabinetes SIRENE são as seguintes: regras de funcionamento comuns; disponíveis 24 horas por dia, 7 dias por semana; dispor de informação suplementar de imediato; meios de comunicação rápidos, eficazes e seguros; pessoal habilitado para comunicar em inglês e francês.

Até à integração do Gabinete Nacional SIRENE no PUC-CPI as competências por cada Força de Segurança representada no Gabinete SIRENE foram sempre separadas. Na sala operativa, existiam quatro grupos operativos: GNR, PSP, PJ e SEF.

As competências do Gabinete Nacional SIRENE consistem na criação, modificação e eliminação de indicações; na troca de informações relativas às indicações SIS; na cooperação policial Schengen com vista à prevenção e investigação de factos puníveis – artigo 39.º da Convenção de Aplicação do Acordo Schengen (CAAS) –, para a perseguição transfronteiriça terrestre – artigo 41.º da CAAS – e para efetuar a troca de informações, a prevenção de crimes e a ameaças à ordem e segurança públicas – artigo 46.º da CAAS.

As categorias de dados disponíveis no SIS úteis à troca de informações entre Polícias e Justiça dividem-se em dados sobre pessoas e sobre objetos. No que concerne às pessoas, existem dados sobre pessoas procuradas para detenção para efeitos de entrega ou extradição – artigo 26.º da Decisão 2007/533/JAI, de 12 de junho; estrangeiros não admissíveis ou interditados de permanecer no espaço Schengen – artigo 24.º do Reg. SIS II; pessoas desaparecidas – artigo 32.º da Dec. SIS II; pessoas procuradas no âmbito de um processo judicial (pedidos de paradeiro) – artigo 34.º da Dec. SIS II; pessoas sujeitas a controlo discreto ou controlo específico – artigo 36.º da Dec. SIS II. No que diz respeito aos objetos, existem dados sobre: veículos; reboques; caravanas; equipamentos industriais; armas de fogo; documentos em branco; documentos de identidade emitidos; notas de banco; valores imobiliários; meios de pagamento (cheques, cartões de crédito, ações, obrigações) – artigo 38.º da Decisão 2007/533 JAI, de 12 de junho.

4. Da Criminalidade ao Terrorismo

Para Matos (2016, p. 255), as organizações terroristas incorporam um processo “infiltração, dissimulação e engano no planeamento e execução de atentados terroristas”.

O terrorismo tem diversas causas e orientações, assumindo-se ao longo da história, como um recurso tático, fora do contexto de guerra, de diversos tipos de organizações sociais ou políticas, de motivação distinta, decorrente de conflitos/crises religiosas, sociais ou políticas. Por norma são cometidos vários ilícitos penais, antes da ação direta violenta, como a radicalização, o recrutamento e o financiamento, a aquisição de armas de fogo, explosivos ou substâncias precursoras, a falsificação de documentos, a clonagem de cartões, o furto e/ou viciação de viaturas, entre outros. De igual modo, a consumação de um ato terrorista envolve previamente várias etapas (atos preparatórios), desde: a seleção dos alvos, passando pela recolha de informação, a vigilância ao local selecionado, a dotação de financiamento e de meios logísticos, ações de treino e ensaio, até à materialização/execução do ato hostil.

Neste contexto, a deteção preventiva de potenciais indícios/indicadores que possam integrar a suspeita de execução de qualquer uma destas fases será determinante para a prevenção de um ato terrorista.

Com o recrutamento de novos membros e a transformação da Al-Qaeda num movimento mais lato, nodular, com lideranças mais difusas, assistiu-se a um aumento significativo da perpetração de ações terroristas por parte de pequenas estruturas terroristas locais no espaço europeu, que não possuíam a disponibilidade nem a capacidade técnica para a execução de ataques complexos, facto que acabou por determinar a simplificação dos processos de seleção de alvos e uma opção pelos mais vulneráveis (Curry, 2015).

O *modus operandi* utilizado em muitos atentados cometidos na Europa, EUA, Ásia, África e outros, caracterizou-se por uma atuação coordenada de vários agentes terroristas, em diferentes locais, quase em simultâneo, dirigidos, essencialmente, a *soft targets*, os quais por meio da utilização de uma viatura, de armas de fogo automáticas, de engenhos explosivos improvisados, de armas brancas ou de diversos destes meios conjugados, atingiram direta e indiretamente de forma estratégica alvos com enorme concentração de pessoas, a fim de provocarem um elevado número de vítimas. A escolha de alvos diversificados gera incerteza, privilegia o seu valor pragmático e a oportunidade, nomeadamente, os que apresentam grande concentração de pessoas e a ausência de medidas de segurança específicas.

Conforme refere Jenkins (2009), os terroristas têm um pensamento estratégico, na medida em que a seleção de alvos é efetuada em função da facilidade de acesso, do sucesso tático (imediatos) e da oportunidade associada ao resultado, traduzida na produção de um número elevado de vítimas. O sucesso da tática consubstancia-se

na obtenção de resultados de longo prazo. Para este autor, os espaços públicos são difíceis de proteger e o investimento no robustecimento das medidas de segurança, apenas é considerado face a uma vantagem evidente e à probabilidade de transferência do risco para uma outra infraestrutura igualmente acessível. Apesar da conhecida apetência natural pela seleção de alvos icônicos por parte das organizações terroristas, os atores isolados e as pequenas células optam (muitas vezes) por desencadear ataques contra alvos de oportunidade, mais vulneráveis e acessíveis, em função da sua menor capacidade operacional e do consequente efeito mediático (Hesterman, 2015).

A expressão *soft target* designa qualquer espaço, instalação ou infraestrutura que careça de dispositivos de segurança robustos e que, por esse motivo é fácil de atingir. Entre os *“soft targets”* encontram-se interfaces de transportes públicos, salas de espetáculos, escolas, locais de culto, hospitais, feiras e festas, zonas comerciais, concertos, eventos populares, zonas de interesse turístico ou outros espaços e eventos que concentrem público, por oposição aos *“hard targets”* que possuem numerosas medidas de segurança que previnem e desmotivam ataques (Hesterman, 2015, p. xiii), como sejam, instalações militares, policiais ou do Governo, bem como, infraestruturas críticas classificadas. A expressão ganhou popularidade quando o terrorismo de matriz islamista passou a selecionar alvos mais desprotegidos, essencialmente civis, procurando, através da vitimação de um grande número de pessoas, de preferência de diversas nacionalidades, o impacto mediático necessário a fazer passar a sua mensagem apologética. Pela sua natureza, os ataques a *soft targets* imprimem um efeito psicológico fortíssimo no público (Hesterman, 2015, p. 2) uma vez que atingem os ambientes tradicionalmente mais tranquilos e pacíficos, onde o *modus vivendi* ocidental se costuma desenrolar normalmente e sem violência. Os terroristas modernos optaram por trazer a violência, destruição e terror às zonas onde os cidadãos se sentiam seguros (Hesterman, 2015, p. 2), abalando todas as convicções sobre a sua segurança e fazendo instalar um sentimento de insegurança e de intranquilidade exacerbado.

Verifica-se ainda uma tendência de ligação cada vez mais estreita entre a criminalidade de massa, a criminalidade violenta e o terrorismo. Os desenvolvimentos recentes na estratégia e os *modus operandi* do terrorismo de inspiração religiosa islâmica têm vindo a desafiar alguns estereótipos no que diz respeito ao perfil do terrorista radicalizado, motivado e predisposto para a ação direta violenta. Alguns dos indicadores mais comuns, como a indumentária, o aspeto físico, a conduta individual e social e a devoção e prática religiosa rígidas, deixaram de servir como referencial para a identificação de indivíduos potencialmente radicalizados e perigosos.

Um dos traços que começa a assumir cada vez mais relevância para o perfil de potenciais terroristas, refere-se à existência de antecedentes criminais entre os perpetradores de atentados. No passado recente, os ex-presidiários ou indivíduos com

antecedentes criminais não eram bem acolhidos no seio da maioria das organizações terroristas de matriz fundamentalista islâmica, na medida em que o seu passado e a sua referência pelas autoridades judiciais e policiais constituíam uma vulnerabilidade para as organizações terroristas.

Porém, na atualidade, quer a Al-Qaeda quer sobretudo o Estado Islâmico, têm explorado de forma crescente a experiência criminal de alguns indivíduos, embora se mantenha a tendência maioritária de radicalização e recrutamento no seio dos templos religiosos, das comunidades imigrantes desfavorecidas social e economicamente e nas segundas e terceiras gerações das famílias imigrantes dessas mesmas comunidades.

No meio urbano cada vez mais massificado e anónimo a desintegração não é, no entanto, uniforme ou um dado adquirido em todas as famílias emigrantes. A tendência de considerar os terroristas como vítimas de discriminação social e económica constitui, em grande medida, um estereótipo. Os estudos disponíveis apontam para uma desintegração e para sentimentos de aversão à cultura e valores ocidentais sobretudo nas segundas gerações. Esta desintegração não é, muitas vezes, económica ou sociocultural, mas sobretudo psicológica, na medida em que os jovens não se sentem identificados com a cultura dos pais, mas também não se reveem nos valores e no modo de vida da sociedade de acolhimento, optando por uma conduta marginal.

O conhecimento dos métodos, de outros indivíduos no submundo do crime especializados em determinados ilícitos, a experiência no manuseamento de armas de fogo, de explosivos, os peritos informáticos são algumas das áreas procuradas e que se constituem como uma vantagem e oportunidade para os terroristas. Constituem-se como vertentes relevantes no planeamento de atentados:

- segurança das operações: habituados a agir na ilegalidade, os indivíduos com antecedentes criminais são especialmente cuidadosos e experientes na adoção de medidas de segurança, de métodos para iludir as ações das autoridades;
- acesso a mercados criminais: o contacto com outros criminosos serve como meio de acesso a mercados criminais relevantes para a ação terrorista, nomeadamente o comércio ilegal de armas e explosivos, de contrafação de documentos, de perícia em *modus operandi* específicos;
- apoio logístico: a logística das operações terroristas é muito facilitada pelos contactos no submundo do crime, em especial nas áreas do furto e viciação de veículos, da falsificação de documentos, da facilitação de deslocações, da utilização de casas seguras – sendo ainda crucial para a execução das ações planeadas e concertadas;
- manuseamento de armas: os criminosos violentos têm conhecimento e experiência ao nível do uso de armas brancas e de armas de fogo, não necessitando de treino prévio;

- financiamento das operações: a prática de crimes de retorno financeiro imediato – furtos, roubos, burlas, fraudes, recorrendo cada vez mais ao cometimento destes ilícitos em ambiente cibernético – serve de fonte de financiamento das operações e obsta à necessidade de existência de redes de financiamento, mais facilmente rastreáveis pelas autoridades competentes.

O Estado Islâmico configura-se como uma fonte de inspiração junto de grupos de jovens desintegrados social e economicamente, com problemas anteriores com a Polícia e com a justiça e que veem na mensagem fundamentalista uma oportunidade de abraçarem uma demanda ou de pertencerem a uma organização que lhes dê importância e na qual possam sentir-se acolhidos. A narrativa utilizada pelo Estado Islâmico ou pela Al-Qaeda implica, por um lado, a legitimação da violência em torno de uma causa ou de um projeto social e político partilhado; a atividade criminal para facilitar a ação da organização terrorista encontra validação teológica na sua interpretação do conceito de *ghanimah*, ou seja, o direito de reclamar os despojos de guerra; a entrega à causa terrorista dos verdadeiros e justos muçulmanos, em nome do profeta e da sua palavra, assenta numa ideia de sacrifício e martírio, os quais serão recompensados com o paraíso e a salvação eterna – a promessa de redenção; os dilemas morais decorrentes da prática de crimes graves são legitimados, pois são ações praticadas em nome de Deus.

5. Propaganda e Radicalização

A propaganda de organizações terroristas como o Estado Islâmico ou a Al-Qaeda tem como objetivo a radicalização do maior número de pessoas possível, independentemente de os alvos terem ou não antecedentes criminais. Este processo de radicalização é, em geral, oportunista e instrumental, baseia-se no conhecimento pessoal, tendo por base os contactos e conhecimentos prévios adquiridos no meio criminal, com o objetivo de financiamento de atividades, de garantir recursos ou meios para a consecução da atividade terrorista. A radicalização e recrutamento tem sido identificada como simplificada pelos serviços de informações e policiais, na medida em que, muitas vezes, nem sequer se preocupa com a promoção dos fundamentos do Islamismo, mas sim com uma narrativa simplista e diabolizadora da cultura, usos e costumes ocidentais, descontextualizando episódios históricos e legitimando o ódio, a violência e a vingança em relação a situações passadas de alegada opressão ou de exploração por parte dos cristãos em relação aos muçulmanos.

5.1 Os (Diversos) Processos de Radicalização

Ashour (2009, p. 4) considera a radicalização como “um processo de mudança no qual um grupo/indivíduo passa por alterações ideológicas e/ou comportamentais que o levam à rejeição dos princípios democráticos (incluindo a alternância pacífica

do poder e a legitimidade de pluralismo ideológico e político), e à exigência de mudanças revolucionárias sociopolíticas, socioeconômicas e culturais, com a possibilidade de utilização da violência, ou aumento dos níveis de violência, para alcançar objetivos políticos”.

No quadro da propaganda e radicalização, a publicação de revistas *online* como a *Rumiyah*¹⁰, a *Dabiq*¹¹ ou a *Inspire*¹² obtém grande penetração nos públicos-alvo pretendidos pelas organizações terroristas em questão. Têm, em geral, elevada qualidade gráfica, são apelativas e abrangem diversas temáticas no contexto da doutrinação e da promoção de ideias fundamentalistas e radicais. Salientam-se ainda as revistas: *Al-Naba*, com 69 edições, publicada em árabe, desde 2014; a revista *Dar Al-Aslam*, com seis edições, publicada em francês, entre setembro de 2015 e fevereiro de 2016; a revista *Konstaninniyye*, com seis edições, publicada em turco entre junho de 2015 e abril de 2016 e ainda a revista *Istok*, publicada em russo, entre maio de 2015 e maio de 2016.

A revista *Rumiyah* foi publicada pela primeira vez em 5 de setembro de 2016 e foi editada em oito línguas – inglês, francês, alemão, russo, turco, uigur, indonésio e pashtun – e conta até hoje com sete edições. Esta revista veio substituir a *Dabiq* que teve quatro publicações em língua inglesa, tendo deixado de ser difundida em meados de 2016.

Um dos aspetos mais preocupantes da linha editorial da *Rumiyah* tem sido a difusão sucessiva de diversas táticas para o cometimento de atentados terroristas – na rubrica *Just Terror Tactics* –, no quadro do “terror justo” contra os infiéis, divulgando possíveis *modus operandi* de baixa complexidade e apelando à ação de lobos solitários predispostos e motivados para realizar atentados.

Assim, na segunda edição é dado destaque ao cometimento de ataques com armas brancas, descritos com maior detalhe na quarta edição. São efetuadas recomendações quanto ao tipo de armas a utilizar, quanto às zonas do corpo mais vulneráveis e referidos os efeitos esperados em função do tipo de alvos: vítimas isoladas, para campanhas de terror prolongadas e pequenos grupos para criar maior choque e impacto. Não são aconselhadas grandes multidões para esta tática.

A terceira edição da revista aborda os ataques com recurso a veículos pesados. O artigo descreve as características ideais do veículo para que o impacto seja o maior

10 O termo *Rumiyah* pretende referir-se à cidade de Roma (Itália), tornando assim expresso o objetivo de domínio do espaço europeu e alimenta a narrativa dos sucessos militares da organização terrorista Estado Islâmico, ocultando a sua progressiva perda de território na Síria e no Iraque.

11 A revista *Dabiq* terá merecido esta designação devido à natureza simbólica e apocalíptica da cidade com o mesmo nome situada entre a fronteira turca e Aleppo.

12 A revista *Inspire* é publicada em língua inglesa pela Al-Qaeda da Península Arábica e conta já com duas dezenas de edições.

possível, isto é, para causar o maior número de vítimas. É aconselhada a seleção de locais e de ocasiões com uma grande concentração de pessoas.

Na quinta edição são recomendados ataques com recurso a dispositivos incendiários. Esta fornece instruções detalhadas de fabrico e utilização de *cocktails molotov* e *napalm molotov* bem como quanto aos melhores locais para incendiar os engenhos, sublinhando o impacto da realização de ataques múltiplos em simultâneo.

A sexta edição não compreende a série *Just Terror Tactics*, mas, em contrapartida, inclui infografia sobre os efeitos do gás *sarin* sobre o corpo humano e recomendações sobre medidas a adotar em face de um ataque deste teor. Aparentemente, não se trata da apologia de realização de atentados com este ou outro tipo de armas químicas e biológicas contra alvos concretos, podendo inferir-se que se trata mais de uma perspetiva preventiva da organização terrorista Estado Islâmico.

A partir da décima edição a revista *Rumiyah* não voltou a publicar a série *Just Terror Tactics*. Porém, na décima terceira edição, publicada em setembro de 2017, faz-se apelo para ações de indivíduos isolados e sinalizam-se potenciais formas de ataque. Nesta edição são salientados os atentados da Catalunha, sendo sublinhadas as 16 vítimas mortais e mais de 130 feridos, entre “judeus e cruzados” e ainda o impacto provocado no setor turístico espanhol, bem como, “a lição política” sobre a necessidade de estarem preparados para perdas humanas e económicas.

A revista *Inspire* da responsabilidade da Al-Qaeda da Península Arábica incluiu também uma série designada por *Open Source Jihad*, um conjunto de artigos similares aos da *Rumiyah*, visando essencialmente alvos em território europeu e americano, também com um elevado grau de operacionalização imediata e de potencial inspiração para ação terrorista de lobos solitários. Na décima sétima edição a *Inspire* publicou um artigo subordinado à temática de operações de descarrilamento de comboios, direcionada para a ação direta sobre alvos no setor ferroviário, seja ao nível de troços, das composições ou das próprias estações e gares de transportes ferroviários. O foco é colocado no recurso a um instrumento de descarrilamento improvisado de betão armado, no processo de manufatura, no melhor local para a sua colocação em linhas férreas, sobre o tipo de locomotiva mais propício ao descarrilamento e a velocidade ideal a que deverão circular as composições – sendo aconselhadas velocidades superiores a 100 km/h para a obtenção de resultados mais catastróficos.

O artigo acaba por alargar o âmbito dos alvos, para além dos comboios e das infraestruturas respetivas, mencionando outros meios de transporte (autocarros, navios, aviões, automóveis ou outros), gares ou estações (incluindo aeroportos, estações de metro, gares rodoviárias), infraestruturas secundárias (transportes rodoviários e marítimos), assim como a utilização de armamento antiaéreo para atacar aeronaves em situação de descolagem ou de aterragem.

6. Prevenção e Reação ao Terrorista

Uma das questões hoje mais sedimentadas no seio das Forças de Segurança e Serviços de Informações internacionais consiste na noção de que existe uma relação estreita entre tipologias criminais diversas, muitas vezes, fundamentais para o financiamento, para o apoio, para a logística, para o recrutamento, formação e divulgação do ideário terrorista. A ligação entre o terrorismo e a atividade das redes de imigração ilegal, o tráfico de armas, o tráfico de drogas e a cibercriminalidade constam da maioria dos relatórios das organizações internacionais e das agências de aplicação da lei.

Este assunto tem consequências importantes na estratégia e tática adotada para a prevenção e reação às ameaças híbridas. Na perspetiva de Torres (2015, p. 15), “por mais planeamento e investimento que se faça em segurança, por mais meios que se empreguem, é impossível reduzir a zero o risco de concretização de uma qualquer ameaça”. Acrescenta ainda que existe sempre o fator de imprevisibilidade e um risco estrutural, ou seja, “aquele que permanece ativo independentemente da taxa de esforço garantida para o contrariar”. Podemos, pois, assumir que “a atividade de gestão de riscos acaba por ser uma forma de organizar algumas tradicionais fases de um planeamento de segurança (...) com a previsão de diversos cenários realistas com respostas ajustadas, segundo uma determinada estratégia previamente definida” (Torres, 2015, p. 21).

A Radicalisation Awareness Network (RAN) – Rede de Sensibilização para a Radicalização – da Comissão Europeia desenvolveu vários programas de formação para polícias: programas de sensibilização, compreensão, prevenção, intervenção e sinalização; programas sobre policiamento comunitário; programas de sensibilização cultural; programas de policiamento para todos e sobre direitos humanos; programas sobre cooperação entre a Polícia e a multiplicidade de agências na nossa sociedade; programas sobre polarização e tensões sociais; programas sobre o uso da internet e das redes sociais para a prevenção da radicalização; programas sobre comunicação interpessoal (atitudes, linguagem e linguagem corporal); programas sobre o papel da polícia na desradicalização e desmobilização de extremistas (Lenos e Keltjens, 2016).

Face ao exposto, as políticas de segurança e de justiça e as estratégias de deteção, prevenção e neutralização dos agentes da violência têm que ser holísticas, juntando o Estado, instituições públicas, entidades privadas e a sociedade civil.

Parece-nos fundamental a aposta no policiamento de proximidade e na inteligência (de segurança e policial), de forma a potenciar a deteção de indícios técnicos de radicalização e de preparação de ações violentas nas comunidades mais fragmentadas; o investimento no *spotting* policial junto aos *soft targets* para a deteção de manobras de reconhecimento, planeamento e de ensaio/treino; o direcionamento da inteligência policial e dos serviços de informações para a pesquisa de fontes aber-

tas, para fontes humanas e outras que potenciem a identificação de possíveis suspeitos e de operações de planeamento; a monitorização de indivíduos, grupos e locais potenciais, alvos de ações de radicalização e ainda a cooperação entre os órgãos de polícia criminal e os serviços de informações para a desarticulação precoce de organizações terroristas nas suas diversas dimensões.

O *spotting* consiste no empenho de equipas policiais na via pública, em missões de observação e de inserção de forma visível ou camaleónica na comunidade, para reconhecer ou recolher sinais – indícios técnicos de radicalização, de reconhecimento, de pré-incidente ou de possível execução de um crime. São de referir alguns exemplos de indicadores de possível preparação de um ato criminoso: comportamento/linguagem corporal; alteração da aparência; indumentária; interesse prolongado ou involuntário – objetos, pessoas, edifícios, Closed-Circuit Television (CCTV) ou videovigilância, mecanismos de segurança, etc.; perguntas a pessoas/seguranças, etc. sobre questões de segurança; suspeita de posse de facas, armas de fogo, mochilas, seringas, bisnagas, fios escondidos, etc.; observação de cúmplices, viatura(s) de apoio; filmagens suspeitas, etc.

O desenvolvimento tecnológico “criou uma ilusão no seio da comunidade de inteligência (policial e nos serviços de informações), de aposta e de confiança na inteligência técnica (TECHINT), assente sobretudo em conhecimento derivado de sinais (SIGINT), da interceção de comunicações, de satélites e do estudo geoespacial (IMINT)” (Neto, 2017, p. 9), de técnicas preditivas assentes em algoritmos e em muitas outras formas derivadas das ciências da computação, para a aquisição de conhecimento. Com isto, resultou uma desvalorização da inteligência humana (HUMINT), assim como no conhecimento da cultura, língua, religião e problemas das comunidades de risco. Conforme refere Sun Tzu (1974, p. 293), “a presciência ou previsão não podem ser deduzidas (...) por analogia com as atividades passadas, nem por cálculos. Elas devem ser obtidas dos homens que conhecem a situação do inimigo”.

É prioritário um esforço conjugado e proactivo entre a prevenção, a inteligência e a investigação criminal, dado que a panóplia de crimes e *modus operandi* em contexto terrorista é vasta, salientando-se:

- a difusão de mensagens ao público, incluindo por meio eletrónico ou através da internet, incitando à prática de crimes por organização terrorista;
- o recrutamento para a prática de crimes por organização terrorista;
- o treino ou instrução sobre o fabrico ou a utilização de explosivos, armas de fogo ou outras armas e substâncias nocivas ou perigosas ou sobre outros métodos e técnicas específicos para a prática de crimes previstos na lei como terroristas;
- as reuniões públicas, a utilização de meios de comunicação social, a divulgação por escrito ou por outros meios de reprodução técnica, a recompensar ou

- a louvar outra pessoa, grupo, organização ou associação pela prática de crimes de terrorismo;
- as viagens ou tentativas de viagem para territórios diferentes do seu Estado de residência ou nacionalidade, com vista ao treino, apoio logístico ou instrução de outrem;
- as viagens ou tentativas de viagem para um território diferente do seu Estado de residência ou nacionalidade, com vista à adesão a uma organização terrorista ou ao cometimento de crimes em contexto terrorista;
- a organização, financiamento ou facilitação de viagens ou tentativas de viajar;
- por quaisquer meios, direta ou indiretamente, o fornecimento, recolha ou detenção de fundos ou bens de qualquer tipo, bem como de produtos ou direitos suscetíveis de serem transformados em fundos, com a intenção de serem utilizados ou sabendo que podem ser utilizados, total ou parcialmente, no planeamento, na preparação ou para a prática de atos qualificados por lei como terroristas.

As estratégias de recrutamento e de gestão de recursos humanos em muitas Polícias em termos internacionais procuram cada vez mais, a diversidade, de modo a melhor perceberem a sociedade multicultural. A título de exemplo, o Departamento de Polícia de Nova Iorque, em 2017, tinha, nas suas fileiras, polícias de mais de 53 países – imigrantes e segundas e terceiras gerações –, os quais falavam 75 idiomas.

Conclusões

As políticas de prevenção e de combate ao terrorismo não cumpriram plenamente até hoje o objetivo de erradicar ou controlar fenómenos como o recrutamento, a radicalização, o financiamento de atividades terroristas e o cometimento de atentados. Apesar do diagnóstico profundo sobre o terrorismo efetuado pelas Forças de Segurança, Serviços de Informações e por diversos Centros de Investigação e *Think Tanks*, sobre o perfil das organizações e dos terroristas assim como acerca dos resultados obtidos no quadro de investigações criminais¹³, o fenómeno da radicalização e do terrorismo continua a representar uma ameaça permanente em diversos países do mundo e em particular na Europa.

Em primeiro lugar, há que compreender os fundamentos do terrorismo fundamentalista, em particular do salafismo, maioritário em países como a Arábia Saudita e o Qatar. Assumidamente, esta corrente radical do Islão considera o modelo de sociedade ocidental como incompatível com os seus valores e procura deslegitimar os regimes democráticos. Caberá aos Estados de direito ocidentais combaterem o fundamentalismo também ao nível da retórica e da propaganda, desmontando precon-

¹³ De acordo com o relatório da Europol (2018), foram detidos 1.002 indivíduos por crimes de terrorismo nos Estados-membros da UE.

ceitos e estereótipos. Uma das soluções consistirá em criar alianças com os países e líderes islâmicos moderados, sendo que um sinónimo de moderação consistirá na aceitação/defesa da compatibilidade entre a democracia e o islamismo.

Tendo em consideração o pragmatismo, a aleatoriedade, a incerteza, a diversidade de locais, atores, *modus operandi* e armas que caracterizam as ameaças terroristas atuais bem como a expansão da mensagem jihadista na internet, nas comunidades, no meio prisional, sem grandes entraves, constitui um desafio para os Estados de direito a adoção de políticas efetivas que garantam a liberdade, a segurança e justiça e, nomeadamente, a consolidação dos sistemas de prevenção, investigação e reação ao terrorismo.

A ineficácia das políticas públicas nas áreas social, económica, cultural, de segurança, de justiça e de integração nos países ocidentais tem gerado, por um lado, sentimentos anti-islâmicos, antirrefugiados e anti-imigrantes por parte de franjas extremistas nas sociedades ocidentais. E, por outro, o crescimento da radicalização no seio das comunidades muçulmanas residentes nos países ocidentais, como reação à desintegração, marginalização e hostilidade crescente das populações, nomeadamente nos países da UE que se constituem como destino por excelência dos migrantes.

A radicalização é, assim, hoje um fenómeno multidimensional, não só no seio da população islâmica mas também nas comunidades judaico-cristãs ocidentais, expressa nos atentados cometidos, por exemplo por Breivik em 22 de julho de 2011 na Noruega e por Brenton Tarrant em 15 de março de 2019 na Nova Zelândia. Ambas as tendências parecem estar assentes sobretudo na distorção de factos históricos, sociopolíticos, culturais e religiosos, aumentando sentimentos de insegurança, de desconfiança e de permeabilidade ao ódio em ambas as comunidades. O alheamento dos jovens ocidentais em relação à participação política nos Estados de direito democráticos e aos valores das sociedades abertas também está, por isso, a fazer crescer entre os adolescentes e jovens adultos europeus e norte-americanos, por um lado, os movimentos de extrema-direita, nacionalista, xenófoba e uma consciência anti-islâmica e, por outro, o fundamentalismo e jihadismo.

A imprevisibilidade e a capacidade disruptiva das ameaças e riscos contemporâneos têm de levar a que os sucessivos governos apostem no robustecimento dos sistemas de segurança interna e de justiça e dos sistemas de informações bem como a consolidação dos padrões de coordenação, cooperação e de prontidão entre as Forças e Serviços de Segurança. Esta conjuntura deve servir para alertar ainda mais as nossas autoridades para a necessidade de adoção de medidas consistentes de médio e longo prazo que permitam uma manutenção e reforço dos padrões de segurança, apostando nomeadamente na partilha e troca de informações e na implementação de modelos de policiamento que conjuguem a proximidade, a inteligência, a visibilidade e a musculação da resposta em caso de necessidade.

Centramos a nossa análise, em especial, no terrorismo de inspiração religiosa. Todavia, não pode ser menosprezado o recrudescimento de outras ideologias e organizações, nomeadamente o terrorismo de extrema-direita, de extrema-esquerda ou anarquista, nacionalista e separatista e, particularmente, o terrorismo ambientalista ou de defesa de causas como a dos direitos dos animais. Em termos prospetivos, será previsível um incremento do eco terrorismo ou terrorismo ambientalista, visando organizações e empresas consideradas como poluidoras, empresas identificadas com a utilização de materiais provenientes do abate de espécies animais protegidas, empresas madeireiras, laboratórios farmacêuticos, centrais nucleares, entre outros, atendendo à crescente visibilidade e preocupação pública com as alterações climáticas e o ambiente.

Tomé (2007) considera que “os grandes protagonistas da segurança internacional e da luta contra as ameaças continuam a ser os Estados soberanos, cujas funções e responsabilidades, direitos e obrigações estão consagrados na Carta das Nações Unidas. Simplesmente, a segurança internacional contemporânea implica, como nunca antes, uma abordagem coletiva: é indispensável contar com estratégias coletivas, instituições coletivas, mecanismos coletivos e um sentido de responsabilidade coletiva. (...) Isso será determinante para fazer prevalecer a ordem sobre a anarquia”.

O combate ao terrorismo não é algo que possa obedecer a estratégias unidimensionais e nem possa ser apoiado em meios exclusivamente militares (Simões, 2004), mas principalmente “uma tarefa das forças policiais e do sistema judicial, uma vez que o terrorismo é mormente uma forma de crime organizado” (Oeter, 2006, pp. 233-234), o que não prejudica a cooperação e trabalho conjunto das Polícias e dos Serviços de Informações com as Forças Armadas, Proteção Civil, Emergência Médica, Segurança Privada e da própria Sociedade Civil.

É de crucial relevância a aprovação de novos dispositivos legais para os Órgãos de Polícia Criminal e os Serviços de Informações, que permitam por exemplo a possibilidade de interceção de comunicações telefónicas, o acesso a metadados, a videovigilância em locais públicos para efeitos de prevenção e de segurança pública, a utilização de meios aéreos (tipo *drone*) para melhorar o comando, a coordenação e o controlo operacional.

Conforme previsto na *Estratégia Nacional de Combate ao Terrorismo*, impõe-se em Portugal a aprovação de um *Plano de Ação de Prevenção da Radicalização e do Recrutamento para o Terrorismo*; a atualização e aplicação de um *Plano de Ação Nacional contra Ataques Nucleares, Biológicos, Químicos e Radiológicos*; a adoção de um *Plano de Ação para a Proteção e Aumento da Resiliência das Infraestruturas Críticas*, nacionais e europeias, com os respetivos planos de segurança; a definição de um *Plano de Ação Nacional para a Proteção contra as Ciberameaças*, integrado numa estratégia nacional de cibersegurança; a aprovação de um *Plano para a Proteção das Comunidades Portuguesas e Interesses Nacionais no Exterior* e, igualmente, fundamental a definição de

um *Plano de Articulação Operacional*, que contemple medidas de coordenação e a interoperabilidade de sistemas e de equipamentos, das Forças e Serviços de Segurança (incluindo os Serviços de Informações), Proteção Civil, Emergência Médica e Forças Armadas.

A sedimentação de uma cultura e de padrões de segurança não pode ser concretizada através da descaraterização do Estado de direito. Os Estados têm que equilibrar a eficácia e eficiência da prevenção e do combate ao terrorismo, com a garantia dos direitos, liberdades e garantias dos cidadãos, dos direitos dos imigrantes e do direito de asilo, pelo que só quando se verifiquem razões ponderosas para provar que os imigrantes ou refugiados praticaram crimes contra a paz, crimes de guerra ou crimes contra a humanidade e crimes dolosos de direito comum puníveis com pena de prisão superior a três anos, fora do território nacional, antes de terem sido admitidos como refugiados, ou em território nacional, é que devem perder a proteção especial. De igual modo, quando se verifique que os requerentes de asilo ou de autorização de residência tenham deturpado ou omitido factos, incluindo a utilização de documentos falsos, decisivos para beneficiar do direito de asilo ou de proteção subsidiária e representem perigo para a segurança interna é que não devem ver satisfeitas as suas pretensões.

A adoção por parte das organizações internacionais e dos diferentes Estados de uma estratégia para contrariar a narrativa legitimadora do terrorismo de inspiração religiosa é crucial bem como a retirada de conteúdos fundamentalistas e radicais da *internet*. Estas medidas poderão minorar o impacto da propaganda em alvos mais permeáveis, assim como a glorificação da violência, de uma visão deturpada do Islão e de uma mensagem maniqueísta do mundo entre fiéis e infieis.

Preconizamos o desenvolvimento de ações de sensibilização nos bairros e comunidades, nas escolas, nos centros de acolhimento de imigrantes e de refugiados, de forma a dotar as populações mais vulneráveis de maior sentido crítico em relação a mensagem fundamentalista e de responsabilização dos jovens e adultos.

Defendemos o apoio aos líderes das comunidades para a deteção de situações de radicalização, para a participação nas ações de promoção do diálogo intercultural, para resolução de problemas de âmbito local e para a difusão de mensagens pacificadoras de convivência e de partilha entre os povos.

Consideramos necessária a aplicação de estratégias de saída, sempre que se detete um indivíduo ativo em grupos terroristas, com envolvimento de diversas entidades de saúde, educação, de segurança social, de segurança, entre outros.

Os terroristas preparam e executam os ataques através de um conjunto de passos, muitas vezes, previsíveis. Daí a importância das Forças e Serviços de Segurança aliarem as vertentes de policiamento de proximidade, com vista à criação de contactos e laços de confiança com as comunidades; de investigação criminal, de forma a investigar eventuais atos preparatórios ou condutas suspeitas; de informações

policiais, de modo a detetar e analisar indícios técnicos que configurem ações de propaganda, de recrutamento, de radicalização ou de preparação de ação direta; de ordem pública e de operações especiais, de modo a treinar a intervenção tática em caso de atentado.

Pugnamos pelo reforço da componente HUMINT (*Human Intelligence*) e por uma ligação estreita com a TECHINT (*Technical Intelligence*), de modo a permitir um melhor conhecimento das idiosincrasias sociopolíticas, culturais e religiosas, das ameaças, dos riscos, dos indícios técnicos de radicalização, de recrutamento e de planeamento de atentados. A tendência de desinvestimento global nas fontes humanas e de aposta na tecnologia poderá criar um conhecimento assético da realidade, a incapacidade de deteção de fenómenos subterrâneos e aumentar os vieses nas análises de inteligência.

É fundamental a formação nas Forças e Serviços de Segurança de *spotters* policiais para a identificação de sinais de recolha de *intelligence* (vigilância, aquisição de materiais, ensaios), como sejam: pesquisa de informação sobre potenciais alvos; avaliação de alvos potenciais em termos do valor simbólico ou de atenção pública; infraestruturas críticas; seleção de alvos considerados vulneráveis e outros.

Para além disso, será importantíssima a formação e treino (através de exercícios) dos designados *first responders* policiais bem como a articulação entre os recursos policiais generalistas e os especialistas – investigadores criminais, operações especiais, ordem pública, intervenção rápida, inativação de explosivos, negociadores –, os restantes atores relevantes da segurança interna, da justiça, da defesa, da saúde. A liberdade e segurança dos cidadãos, a salvaguarda dos direitos liberdades e garantias individuais, os padrões de qualidade de vida nas sociedades ocidentais são imperativos que devem ser garantidos e reforçados.

O Estados de direito democráticos, os respetivos governos, as instituições e os cidadãos têm de demonstrar a sua resiliência para fazer face a poderes erráticos que através do ódio e do fanatismo visam precisamente destruir a nossa liberdade e segurança, afetar a nossa qualidade de vida e aniquilar o modelo de sociedade por nós escolhido.

Bibliografia

Antinori, A., 2017. “*Jihaspóra*” and Millennials Complexity, Evolution, Change and Hybridisation of Terrorism in EU. European Union Agency for Law Enforcement Training (CEPOL), Research and Science Conference 2017 “Innovations in Law Enforcement: Implications for practice, education and civil society”, 28-30 November, Budapest, CEPOL/National University of Public Service (NUPS).

Ashour, O., 2009. *Votes and Violence: Islamists and The Processes of Transformation* [pdf], novembro, pp. 40. Londres: International Centre for the Study of Radicalisation and Political

- Violence (ICSR)/King's College. Disponível em ICSR [website] https://icsr.info/wp-content/uploads/2010/01/Votes-and-Violence_-Islamists-and-The-Processes-of-Transformation.pdf
- Borum, R., 2011. Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security*, 4(4), pp. 7-36.
- Combs, C., 2009. *Terrorism in the Twenty-First Century*. 5th Edition. Nova Iorque, Londres: Routledge.
- Curry, C., 2015. How Governments Are Fighting Security Threats In an Era of Soft Target Attacks. *Vice News* [em linha], 13 de janeiro. Disponível em: <https://news.vice.com/article/how-governments-are-fighting-security-threats-in-an-era-of-soft-target-attacks> [consultado em 12 de outubro de 2017].
- Della Porta, D., 1995. *Social Movements, Political Violence and the State: a Comparative Analysis of Italy and Germany*. Cambridge: Cambridge University Press.
- Dzhhekova, R. et al., 2016. *Understanding Radicalisation: Review of Literature* [pdf]. Sofia: Center for the Study of Democracy (CSD). Disponível em CSD [website] https://csd.bg/fileadmin/user_upload/publications_library/files/22778.pdf
- Elias, L., 2018. *Ciências Policiais e Segurança Interna. Desafios e Prospetiva*. Lisboa: ISCPSI
- Europol, 2018. *European Union Terrorism Situation and Trend Report 2018 (TESAT 2018)* [pdf], European Union Law Enforcement Agency (Europol). Disponível em Europol [website] <https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018>
- Federal Bureau of Investigation (FBI), 2006. *The Radicalisation Process: From Conversion to Jihad* [pdf]. Washington: FBI Counterterrorism Division. Disponível em FBI [website] <https://cryptome.org/fbi-jihad.pdf>
- Fernandes, L., 2014. *Intelligence e Segurança Interna*. Lisboa: ISCPSI.
- Forst, B., 2009. *Terrorism, Crime, and Public Policy*. Cambridge: Cambridge University Press.
- Gofas, A., 2012. 'Old' vs. 'New' Terrorism: What's in a Name? *Uluslararası İlişkiler*, 8(32), pp. 17-32. Disponível em: www.academia.edu/3588549/Old_vs._New_Terrorism_Whats_in_a_Name [consultado em 12 de agosto de 2016].
- Hesterman, J., 2014. Deterring and Mitigating Attack (Chap. 9). Em Hesterman, J., *Soft targets hardening: protecting people from attack*. Nova Iorque, Londres: CRC Press, pp. 201-238. Disponível em: <http://www.crcnetbase.com/doi/book/10.1201/b17914> [consultado em 11 de novembro de 2017].
- Hoffman, B., 2006. *Inside Terrorism*. Nova Iorque: Columbia University Press.
- Institute for Economics & Peace, 2018. *Global Peace Index 2018: Measuring Peace in a Complex World* [pdf], Sidney, junho. Disponível em: <http://visionofhumanity.org/app/uploads/2018/06/Global-Peace-Index-2018-2.pdf>
- Jenkins, B., 2009. Terrorists Can Think Strategically: Lessons Learned from the Mumbai Attacks [pdf], *Testimonies* CT-316, junho, Santa Monica. Disponível em RAND Corpora-

tion [website] https://www.rand.org/content/dam/rand/pubs/testimonies/2009/RAND_CT316.pdf

Jenkins, B. e Johnson, J., 1975. *International Terrorism: A Chronology, 1968-1974* [pdf], março, Santa Monica, RAND Corporation. Report prepared for Department of State and Defense Advanced Research Projects Agency. Disponível em National Criminal Justice Reference Service (NCJRS) [website] <https://www.ncjrs.gov/pdffiles1/Digitization/28210NCJRS.pdf>

Kalvach, Z. *et al.*, 2016. *Basics of Soft Targets Protection: Guidelines*. Praga: Soft Targets Protection Institute. Disponível em: <http://www.mvcr.cz/cthh/soubor/basics-of-soft-target-protection-guidelines.aspx+%cd=1&hl=pt-PT&ct=clnk&gl=pt> [consultado em 22 de outubro de 2017].

Koteweg, R. *et al.*, 2010. Background contributing factors to terrorism: Radicalization and recruitment. Em Magnus Ranstorp, ed., *Understanding Violent Radicalisation. Terrorist and Jihadist Movements in Europe*. Nova Iorque: Routledge.

Lei n.º 25/2008 de 5 de junho. Lei de Combate ao Branqueamento de Capitais e do Financiamento ao Terrorismo. *Diário da República*, 1.ª série, N.º 108, 5 de junho de 2008.

Lei n.º 49/2008 de 27 de agosto. Lei de Organização da Investigação Criminal. *Diário da República*, 1.ª série, N.º 165, 27 de agosto de 2008.

Lei n.º 74/2009, de 12 de agosto. Aprova o regime aplicável ao intercâmbio de dados e informações de natureza criminal entre as autoridades dos Estados-membros da União Europeia, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2006/960/JAI, do Conselho, de 18 de dezembro de 2006. *Diário da República*, 1.ª série, N.º 155, 12 de agosto de 2009.

Lenos, S. e Keltjens, M., 2016. *RAN POL's Guide on Training programmes for police officers in Europe* [pdf], setembro, pp. 36. Disponível em European Commission, Migration and Home Affairs [website] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/about-ran-pol/docs/ran_pol_guide_on_training_programmes_for_police_officers_en.pdf

Lloyd of Berwick, Lord, 1996. *Inquiry into Legislation Against Terrorism (Command Paper)*. Londres: Stationery Office Books.

Matos, J., 2016. *Terrorismo e Contraterrorismo: Sistemas de segurança interna*. Casal de Cambra: Caleidoscópio.

Mccauley, C. e Moskalenko, S., 2017. Understanding Political Radicalization: The Two-Pyramids Model. *American Psychologist*, 72(3), pp. 205-216. Disponível em: <https://doi.org/10.1037/amp0000062>

Moghaddam, F., 2005. The Staircase to Terrorism: A Psychological Exploration. *American Psychologist*, 60 (2), pp. 161-169. Disponível em: <https://doi.org/10.1037/0003-066X.60.2.161>

Morgan, M., 2004. The Origins of the New Terrorism. *Parameters*, 34(1), pp. 29-43. US Army War College. Disponível em: <https://ssi.armywarcollege.edu/pubs/parameters/articles/04spring/morgan.pdf> [consultado em 12 de agosto de 2016].

- Morris, E. e Hoe, A., 1987. *Terrorism: Threats and Response*. Londres: Macmillan Press.
- NATO, 2016. NATO's military concept for defence against terrorism. *NATO* [em linha], 15:50, 19 de agosto. Disponível em: https://www.nato.int/cps/en/natohq/topics_69482.htm
- Neto, J., 2017. *Fontes Humanas na PSP. Um contributo para um modelo de gestão*. Trabalho Individual Final do Curso de Direção e Estratégia Policial (CDEP). Lisboa: ISCPSI.
- Neuman, P., 2008. *Joining Al-Qaeda: Jihadist Recruitment in Europe*. Londres: Routledge.
- Oeter, S., 2006. O Terrorismo como um Desafio ao Direito Internacional. Comunicação à Conferência organizada pela Fundação C. Gulbenkian, *Terrorismo e Relações Internacionais*. Lisboa: Fundação Calouste Gulbenkian/Gradiva.
- Precht, T., 2007. *Homegrown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism*. Research report funded by the Danish Ministry of Justice, dezembro. Disponível em: http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/2011/2007/Home_grown_terrorism_and_Islamist_radicalisation_in_Europe_-_an_assessment_of_influencing_factors__2_.pdf
- Reinares, F., 2017. *Al-Qaeda's Revenge: The 2004 Madrid Train Bombings*. Woodrow Wilson Center Press/Columbia University.
- Resolução do Conselho de Ministros n.º 104/2017, de 17 de julho. Aprova a Estratégia Nacional de Gestão Integrada de Fronteiras. *Diário da República*, 1.ª série, N.º 136, 17 de julho de 2017.
- Resolução do Conselho de Ministros n.º 134/2017 de 27 de setembro que aprova a Estratégia para o Turismo 2027. *Diário da República*, 1.ª série, N.º 187, 27 de setembro de 2017.
- Roy, O., 2004. *Globalised Islam: The search for a new Ummah*. Nova Iorque: Columbia University Press.
- Sageman, M., 2008. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Filadélfia: University of Pennsylvania Press.
- Sageman, M., 2004. *Understanding Terror Networks*. Filadélfia: University of Pennsylvania Press.
- Schoeberl, R., 2016. Recognizing Radicalization. *Whelan Security* [em linha], 23 de junho. Disponível em: <http://www.whelansecurity.com/news/recognizing-radicalization/> [consultado em 20 de outubro de 2017].
- Silke, A., 2014. Risk Assessment of Terrorist and Extremist Terrorists. Em Andrew Silke, ed., *Prisons, Terrorism and Extremism: Critical Issues in Management, Radicalisation and Reform*. Nova Iorque: Routledge, pp. 108-121.
- Simões, M., 2004. Terrorismo(s) e Usos das Tecnologias da Informação e da Comunicação. Em Adriano Moreira, ed., *Terrorismo*, 2.ª edição. Coimbra: Almedina, pp. 509-511.
- Sistema de Segurança Interna (SSI), 2018. *Relatório Anual de Segurança Interna 2018*. Lisboa: Gabinete do Secretário-Geral do Sistema de Segurança Interna. Disponível em: <https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=ad5cfe37-0d52-412e-83fb-7f098448dba7>

- Sistema de Segurança Interna (SSI), 2016. *Relatório Anual de Segurança Interna 2016*. Lisboa: Gabinete do Secretário-Geral do Sistema de Segurança Interna. Disponível em: [http://www.ansr.pt/InstrumentosDeGestao/Documents/Relat%C3%B3rio%20Anual%20de%20Seguran%C3%A7a%20Interna%20\(RASI\)/RASI%202016.pdf](http://www.ansr.pt/InstrumentosDeGestao/Documents/Relat%C3%B3rio%20Anual%20de%20Seguran%C3%A7a%20Interna%20(RASI)/RASI%202016.pdf)
- The Fund for Peace, 2017. *Fragile States Index 2017* [pdf]. The Fund for Peace, Washington. Disponível em [website] ReliefWeb <https://reliefweb.int/sites/reliefweb.int/files/resources/951171705-Fragile-States-Index-Annual-Report-2017.pdf>
- Tomé, L., 2007. Alterações na Segurança Internacional. *Janus 2007, Anuário de Relações Exteriores*, pp. 18-19. Lisboa: Observare/Universidade Autónoma de Lisboa. Disponível em Janus Online http://www.janusonline.pt/arquivo/2007/2007_1_5.html
- Toolis, K., 1995. *Rebel Hearts: Journeys within the IRA's Soul*. Londres: Picador.
- Torres, J., 2015. *Gestão de Riscos no Planeamento, Execução e Auditoria de Segurança*. Lisboa: ISCPSI
- Tzu, S., 1974. *A Arte da Guerra*. Lisboa: Ed. Futura.
- União Europeia, 2015. *Agenda Europeia para a Segurança*. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões COM (2015) 185 Final, de 5 de maio. Disponível em EUR-Lex [website] <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0185&from=CS>
- União Europeia, 2015. Conclusões do Conselho sobre a Estratégia Renovada de Segurança Interna da União Europeia para 2015-2020. Doc. 9798/15, de 10 de junho, JAI 442 COSI 67. Disponível em: <http://data.consilium.europa.eu/doc/document/ST-9605-2015-INIT/pt/pdf>
- União Europeia, 2010. *Estratégia de Segurança Interna da União Europeia: Rumo a um Modelo Europeu de Segurança*. Comissão Europeia, março de 2010, Bruxelas. Disponível em: <https://www.consilium.europa.eu/media/30754/qc30101313ptc.pdf>
- União Europeia, 2003. *Estratégia Europeia em matéria de Segurança: uma Europa segura num mundo melhor*. Comissão Europeia, 12 de dezembro, Bruxelas. Disponível em: <https://www.consilium.europa.eu/media/30824/qc7809568ptc.pdf>
- União Europeia, 2002. Council Framework Decision of 13 June 2002 on combating terrorism, 2002/475/JHA [pdf]. *Official Journal of the European Communities*, L164, volume 45, 22 June, EN, pp. 3-7. Disponível em EUR-Lex [website] <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0475&from=EN>
- United Nations Security Council, 2004. *Resolution 1566 (2004) Adopted by the Security Council at its 5053rd meeting, on 8 October 2004* [pdf], United Nations. Disponível em United Nations [website] [https://undocs.org/S/RES/1566\(2004\)](https://undocs.org/S/RES/1566(2004))
- Wiktorowicz, Q., 2005. *Radical Islam Rising: Muslim Extremism in the West*. Oxford: Rowman & Littlefield.
- World Economic Forum, 2017. *The Global Competitiveness Report 2017-2018* [pdf]. Insight Report, Geneva. Disponível em World Economic Forum [website] <http://www3.weforum.org/docs/GCR2017-2018/05FullReport/TheGlobalCompetitivenessReport2017%E2%80%932018.pdf>

Extra Dossîe

Uma Nova Visão da Sustentabilidade da Marinha de Duplo-Uso

Teresa Vicente Rodrigues

Investigadora do Centro de Investigação Naval (CINAV)

Doutorada em Ambiente e Sustentabilidade (FCT-UNL)

Resumo

A Marinha Portuguesa é, indubitavelmente, a organização-chave para a gestão sustentável de um recurso fulcral para Portugal: o oceano. O presente artigo tem por objetivo fundamentar a pertinência do modelo de organização de duplo-uso da Marinha, à luz do conceito de sustentabilidade veiculado pela Comissão Mundial para o Ambiente e Desenvolvimento e vertido em 1987 no relatório Brundtland. O estudo sugere que em Portugal o duplo-uso é um modelo sustentável e, por conseguinte, recomendável para salvaguardar as necessidades das gerações atuais, sem invalidar as necessidades das gerações futuras, e assim garantindo os pilares do equilíbrio da dimensão social, económica e ambiental, em matéria de defesa e de segurança do uso do mar.

Abstract

A New Vision of the Dual-Use Navy Sustainability

The Portuguese Navy is a key organization for the sustainable management of a key resource for Portugal, the Ocean. The purpose of this article is to substantiate the relevance of the Navy's double-use Organization model, in the light of the concept of sustainability, issued by the World Commission on Environment and Development in 1987 in the Brundtland report. The study suggests that double-use in Portugal is a sustainable model and is therefore advisable to safeguard the needs of the current generations, without invalidating the needs of future generations, ensuring the balance of the social, economic and environmental dimension in defense and safety of the use of the sea.

Introdução

A terra é azul

Yuri Gagarin

Vista do espaço a terra continua azul e, prossegue imperturbavelmente, o seu duplo movimento simultâneo de rotação e de translação, garantindo a manutenção da vida na Terra. Porém, ao aproximar o nosso olhar, observamos que o mundo vive uma era de extremos com impactos profundos em matéria de sustentabilidade, um tempo de mudanças cada vez mais atípicas, uma encruzilhada de movimentos aleatórios resultantes de padrões estruturalmente alterados. Se aproximarmos o nosso olhar dos dois terços da superfície cobertos por oceanos e mares, observamos que as questões relacionadas com o mar apresentam um mesmo padrão de insustentabilidade. A pesca de acesso aberto, a ausência de regulamentação coerente e justa, as disparidades sociais e económicas das zonas costeiras, as questões relacionadas com a segurança alimentar de milhões de pessoas que dependem do mar, a pesca ilegal, a pirataria, o efeito das alterações climáticas sobre o aquecimento das águas e a sua acidificação, a poluição marinha e marítima, constituem ameaças incontornáveis e potenciadoras de desequilíbrios geoestratégicos, com consequências gravosas sobre a segurança, a proteção e a defesa das populações que dependem direta e indiretamente do mar.

Recentemente, de modo a responder aos desafios colocados por esta mudança global, as organizações internacionais e alguns Estados têm vindo a assumir uma nova estratégia centrada no conceito de resiliência. Com efeito, a pertinência deste conceito deve-se à imprevisibilidade de uma nova geração de choques e ameaças ao ambiente e à sustentabilidade, resultantes da complexidade e da interdependência dos sistemas ecológicos e sócio-ecológicos. Desencadeiam, assim, uma mudança conceptual na forma dos decisores perspetivarem a segurança e o desenvolvimento dos territórios e das instituições.

No âmbito nacional, esta questão merece alguma reflexão no sentido de compreender o elo existente entre a resiliência e a sustentabilidade relacionadas com a Marinha Portuguesa, enquanto organização-chave para a gestão de um recurso fulcral para Portugal: o oceano.

Com efeito, num mundo à procura de sustentabilidade, a Marinha Portuguesa, na sua dimensão sócio-ecológica, responsável pela autoridade do Estado no mar, oferece um campo de investigação privilegiado. Enquanto sistema intergeracional de interface entre a dimensão social, económica e ambiental, o estudo da Marinha permite compreender o seu modelo estrutural de duplo-uso e conferir-lhe a merecida posição de sustentabilidade.

Contexto

À escala global é impossível ignorar a impressionante convergência de parâmetros sociais, económicos e ambientais, limitadores à concretização dos indicadores de sustentabilidade consubstancializados nos “Objetivos do Milénio” (Boulanger, 2004; Guedes, 2014; Gambardella, 2017).

Os desafios colocados à sustentabilidade, entendida numa lógica geracional, como o equilíbrio dos pilares social, económico e ambiental, têm levado algumas organizações internacionais e alguns Estados a integrarem nas suas políticas o conceito de resiliência, enquanto capacidade para gerir mudanças significativas e criar novos ciclos mais robustos, que permitirão garantir a integridade dos sistemas ecológicos e sócio-ecológicos (Templeman e Bergin, 2008; Dreibelbis, 2008; The White House, 2011).

Este conceito está a ganhar cada vez mais relevância, sendo percecionado como uma possível chave para solucionar os problemas atuais. Entre os muitos discursos de alto nível, proferidos em favor da resiliência, referimos o discurso do ex-Secretário-Geral das Nações Unidas, Ban Ki-moon, na Conferência Internacional para a Redução de Catástrofes, em Sendai, mencionando que a resiliência é a chave para os Estados escolherem novas orientações que ditarão o futuro de grande parte da população mundial nas próximas décadas (Dalziell, 2004; Ban Ki-moon, 2015).

Paralelamente, nos últimos anos, a avaliar pela quantidade de publicações, conferências, congressos, e outros eventos nacionais e internacionais científicos, a resiliência organizacional tem vindo a afirmar-se de uma forma inequívoca, como um campo de estudo, em que é possível fazer progredir o conhecimento relativo à superação dos desafios colocados pelos eventos extremos, sociais, económicos e ambientais (Comfort, Boin e Demachak, 2010; Rodrigues *et al.*, 2015; Glaser, 2018).

A Resiliência: o Elo Perdido da Sustentabilidade

Perspetivar a resiliência, como o elo perdido da sustentabilidade, encontra a sua pertinência, no entendimento que durante algumas décadas, os arquitetos e construtores da sustentabilidade não reconheceram o valor transformador da resiliência na gestão da mudança, face a choques provocados por eventos extremos, sejam eles de natureza social, económica ou ambiental.

Tal circunstância impediu, por um lado, a mobilização de um conjunto de critérios de fiabilidade, de adaptação e de transformação que permitissem robustecer e equilibrar os pilares social, económico e ambiental a nível global. Por outro lado, impediu a concretização do lema intergeracional, expresso formalmente pela Comissão Mundial para o Ambiente e Desenvolvimento, vertido em 1987, no relatório Brundtland orientado para a satisfação das necessidades das gerações atuais sem comprometer as necessidades das gerações futuras (Brundtland, 1987).

Com efeito, perspetivar as necessidades das gerações futuras, sem ter em conta a capacidade de as gerações presentes enfrentarem e superarem o impacto dos choques, foi uma lição duramente aprendida, que levou recentemente centros de investigação, organizações internacionais, nacionais e empresas, a introduzirem o conceito de resiliência na nova equação.

Todavia, como pensaria Galileu, a verdade tem muita força. A expressão, “o que não é reconhecido não existe”, não se aplica, uma vez que o conceito de resiliência sempre caminhou discretamente na sombra do conceito de sustentabilidade, à espera do momento possível para mostrar ao mundo a sua pertinência. Foi precisamente, a emergência de choques e disrupções decorrentes do modelo produzido pela nossa sociedade e pelas dinâmicas geofísicas atuais, que levaram a comunidade científica e política a reconhecer a resiliência, como um dos conceitos incontornáveis para garantir a sustentabilidade dos sistemas ecológicos e sócio-ecológicos (ISDR, 2005; Dalziell, 2014).

Apesar dos primórdios da resiliência terem emergido com a revolução científica do séc. XVI, no âmbito da ciência dos materiais e sistemas sócio-ecológicos, foi na ecologia que o grande movimento que está em curso deu os seus primeiros passos. Com efeito, o conceito de resiliência ecológica foi introduzido por Holling (1973), na sequência de um debate em torno do conceito de estabilidade dos sistemas. Holling considerava que a discussão e análise tradicionalmente enunciada em torno do conceito de estabilidade, não permitia ser adotada pela ecologia, uma vez que nesta área, o conceito de estabilidade tendia a assumir uma perspetiva matemática definida, muito próxima da noção de pontos de equilíbrio.

Tendo em conta esta perspetiva, Holling publica em 1973 um artigo intitulado “Resilience and Stability of Ecological Systems”, no qual o autor identifica duas propriedades distintas para explicar o comportamento de um sistema ecológico face a uma perturbação. Ele enuncia os conceitos de estabilidade e de resiliência da seguinte forma:

- (1) O conceito de estabilidade é definido como: “a capacidade de um sistema retornar a um estado de equilíbrio após uma perturbação temporária”;
- (2) O conceito de resiliência é definido como: “a persistência de relações dentro de um sistema, uma medida da capacidade dos sistemas absorverem alterações das suas variáveis de estado, das suas variáveis determinantes e dos seus parâmetros, continuando a perdurar no tempo” (p. 18).

A literatura sugere que, a partir da década de 90, o conceito de resiliência ecológica começou a evoluir para uma nova abordagem orientada para a sócio-ecologia. É um facto que a passagem da evolução conceptual da resiliência ecológica para a resiliência socio-ecológica é consagrada por Holling e Gunderson (2001), com um artigo intitulado “Understanding the complexity of Economic, Ecological and

Social Systems”, para explicar as mudanças abruptas e por vezes inesperadas que um sistema enfrenta, mas também permite recuperar.

Neste artigo, os autores definem a resiliência sócio-ecológica como a dinâmica das interações entre sistemas ecológicos e sistemas sociais numa perspetiva de sustentabilidade ecológica, económica e social, definindo a sustentabilidade como um processo de desenvolvimento relacionado como a capacidade de criar, testar e manter a capacidade adaptativa de um sistema.

Baseado numa relativa estabilidade conceptual, e sob os bons auspícios da Resilience Alliance, criada em 1999, Folke publica um artigo intitulado “Resilience and Sustainable Development: Building Adaptive Capacity in a World of Transformations”, no qual, o conceito de resiliência é agora considerado uma estrutura compreensiva para manter e melhorar a capacidade de adaptação de um mundo em mudança (Folke *et al.*, 2002 e 2010).

Nesse artigo, orientado politicamente para a Conferência Mundial sobre o Desenvolvimento Sustentável em 2002, o autor discorda, em dois aspetos, da política de desenvolvimento. Em primeiro, o autor discorda da suposição implícita que a resposta dos ecossistemas para uso humano seria linear, previsível e controlável. Em segundo, que os sistemas humanos e naturais podem ser abordados de forma distinta e independente. Nesta nova abordagem, a resiliência é perspetivada e definida como uma construção dos sistemas socio ecológicos, através de cenários estruturados e de uma gestão adaptativa ativa, que permita considerar a possibilidade de desenvolvimento futuro.

Com o objetivo de clarificar cada vez mais o conceito, Walker *et al.* (2004), referem que a resiliência deve ser perspetivada ao nível dos atributos que determinam a dinâmica de um sistema. Os autores consideram que existem três atributos fundamentais que definem a trajetória dos sistemas sócio-ecológicos, nomeadamente: (1) a resiliência – a capacidade de um sistema absorver uma perturbação, reorganizando-se enquanto enfrenta um período de mudança significativa, prosseguindo com a mesma função, estrutura, identidade e *feedback*; (2) a adaptabilidade – a capacidade dos agentes do sistema gerirem as resistências; (3) a transformabilidade – a capacidade de criar um novo sistema, fundamentalmente quando as estruturas ecológicas, económicas e sociais são insustentáveis.

Nesta época, as grandes questões relacionadas com o desenvolvimento sustentável já estavam na Agenda das Nações Unidas. Aliás, desde a década de 70, vários documentos tinham sido elaborados no sentido de alertar a comunidade internacional para os riscos de um modelo de desenvolvimento arbitrário e sem regulamentação. Em 1973, o relatório intitulado *Os Limites do Crescimento* solicitado pelo Clube de Roma alertava para os problemas cruciais do futuro da humanidade, nomeadamente questões relacionadas com a energia, a poluição, a saúde, o ambiente, e crescimento populacional entre outras. A expressão “desenvolvimento sustentável” foi

referida em 1980 na introdução do relatório da International Union for Conservation of Nature and Natural Resources (IUCN), *World Conservation Strategy: Living Resource Conservation for Sustainable Development*. Apesar do impacto deste documento, o conceito de desenvolvimento sustentável, só seria consagrado sete anos mais tarde, no relatório de orientação política *O Nosso Futuro Comum*, publicado em 1987 pela World Commission on Environment and Development, das Nações Unidas, sob a direção de Gro Harlem Brundtland, primeira-ministra da Noruega, e que ficou conhecido como o relatório Brundtland. Na década de 90, destacam-se dois eventos internacionais, que representaram uma trajetória de mudança e de evolução para garantir a continuidade funcional do planeta face às ameaças emergentes. Consideramos que esses eventos ilustram a distinção salientada por Holling em 1973, para explicar o comportamento de um sistema para responder a uma perturbação através do desenvolvimento de duas dimensões, a estabilidade e a resiliência: (1) A dimensão de estabilidade seria desenvolvida pela Conferência das Nações Unidas sobre Meio Ambiente e Desenvolvimento no Rio de Janeiro (1992); (2) A dimensão da resiliência seria desenvolvida pela Década de Redução de Riscos de Catástrofes (1990-1999), promovida pelas Nações Unidas (Rodrigues, 2009 e 2010). A Conferência das Nações Unidas sobre Meio Ambiente e Desenvolvimento inaugurou a nível internacional, uma nova consciência baseada no modelo de desenvolvimento sustentável, isto é um modelo que permitisse garantir no tempo a estabilidade do planeta através do equilíbrio entre o progresso económico e a exploração dos recursos naturais.

Todavia, o foco orientado para a construção da resiliência dos sistemas socioeconómico emergiu quando as Nações Unidas declararam 1990-1999, a década de Redução de Riscos de Catástrofes Naturais.

Embora, o conceito de sustentabilidade tivesse representado um ponto de partida incontornável para uma nova visão de desenvolvimento formal, atualmente ele suscita leituras divergentes, que sugerem que a noção de sustentabilidade precisa de evoluir para uma nova configuração, na qual as necessidades das gerações presentes devem ser colmatadas urgentemente, para não invalidarem as necessidades das gerações futuras. Apesar, da invocação de alguns limites, não invalida a base paradigmática da sustentabilidade, que aponta para o imprescindível equilíbrio dos pilares de desenvolvimento, designadamente os pilares social, económico e ambiental.

A Marinha de Duplo-Uso: o Caso Paradigmático de um Sistema Sustentável Português

Enquanto sistema sócio-ecológico de interface, a Marinha Portuguesa apresenta o caso paradigmático de uma instituição portuguesa resiliente que, *avant la lettre*, respondeu aos critérios de sustentabilidade definidos pelo relatório Brundtland em 1987.

Com efeito, enquanto Organização de Alta Fiabilidade (OAF), a Marinha é resiliente, treinada para responder a choques. Porém, enquanto sistema organizacional de duplo-uso, a Marinha responde a um modelo histórico intergeracional, que se consubstancia em atividades militares e não militares, vinculados nos pilares social, económico e ambiental, ao serviço da defesa, e segurança das populações que fazem uso do mar (Documentação estruturante da Marinha, 2011).

A Resiliência da Marinha Portuguesa: uma Organização de Alta Fiabilidade

Como já foi referido, a Marinha, à semelhança de qualquer organização militar, é um sistema resiliente, treinada para enfrentar os maiores choques (Desnos, 2012; Cornum, Matthews e Seligman, 2011; Coste e Nexon, 2011). Embora, sem usar esta palavra, há cerca de 2.500 anos, na região considerada hoje o norte da China, uma linhagem de líderes militares expressou o pensamento do general Sun Tzu, que ainda hoje ecoa com grande atualidade e inspiração evocando a resiliência dos militares: “Realizar qualquer trabalho físico ou mental significa vencer a resistência que a oposição apresenta. Na guerra, esse atrito se torna extremo, difícil e extremamente desgastante. Os militares existem para trabalhar em tais situações. Além de representarem o princípio da proteção, as forças armadas são o meio pelo qual uma sociedade concentra os seus recursos para lidar com tempos de crise e de profunda mudança. Essas crises podem ser calamidades naturais, quando o inimigo é a enchente ou a fome. Pode ser o desastre humano da guerra” (Sun Tzu, Grupo de tradução DENMA, 2000, p. 48).

Mas o que é uma Organização de Alta Fiabilidade (OAF)? No âmbito do vasto painel tipológico das organizações, uma Organização de Alta Fiabilidade, designada em inglês por *High-Reliability Organisation* (HRO), constitui uma tipologia de organização à parte das organizações ditas convencionais. A título de exemplo, podemos referir a indústria nuclear, a aviação, todo o setor militar, o petróleo e gás, a indústria petroquímica e os hospitais. Estas organizações apresentam um perfil de alta exigência, tendo em consideração as consequências humanas e económicas que poderiam advir de uma perturbação destes sistemas de suporte à sociedade, aquilo que podemos designar como os últimos baluartes antes do possível colapso (Taphanel, 2010; Hollnagel, Journé e Laroche, 2009).

Vários autores sugerem que esta corrente de pensamento emergiu na década de 80, na sequência de uma reflexão interdisciplinar entre um grupo de investigadores compostos por La Porte, Roberts e Rochlin, da Universidade de Berkeley (Califórnia), com os responsáveis de três organizações cuja atividade ocorria em ambientes caracterizados pela incerteza e a imprevisibilidade e em que os altos desempenhos exigidos poderiam provocar erros operacionais de grande amplitude (Bovis, 2009; Deltort, 2014).

As OAF evidenciam aspetos diferenciados que nos ajudam a perceber o perfil destas organizações, como sistemas que se caracterizam pela fiabilidade das operações correntes, e não apenas pela maximização da eficiência. Os primeiros estudos da equipa de Berkeley levaram-nos a identificar nessas organizações determinados traços comuns que lhe permitem um desempenho resiliente:

- (1) Uma autoridade flexível com capacidade de modificar a estrutura organizacional em situações de crise e de urgência;
- (2) Um forte compromisso do pessoal, assim como um profundo respeito pela competência a todos os níveis da organização;
- (3) Um sistema de recompensa para a descoberta e a identificação dos erros.

De acordo com a teoria que emana das OAF, as tecnologias de risco podem ser dominadas, com toda a segurança pelas organizações, se elas cumprirem com quatro condições essenciais de forma perene:

- (1) As elites políticas e os dirigentes das organizações considerem a segurança e a fiabilidade como as suas primeiras prioridades;
- (2) As condições de redundância permitem a salvaguarda de unidades para compensar as disfuncionalidades;
- (3) As taxas de erro são reduzidas devido à descentralização da autoridade, uma forte cultura organizacional, o treino e a formação contínua;
- (4) A organização desenvolve uma cultura de lições aprendidas, graças a um processo de testes e de erros, reforçada pela simulação e a aplicação de uma cultura de antecipação.

De acordo com esta conceção teórica, as OAF não se limitam apenas a aspetos estruturais, mas apresentam um perfil da organização que reduz a adversidade dos eventos imprevisíveis e possibilita uma rápida recuperação resiliente. Embora as OAF respondam a critérios comuns, cada uma tem uma auto-organização inerente à sua missão (Weick e Sutcliffe, 2007).

Definindo a resiliência, de acordo com o Centre Risque & Performance, como a capacidade de manter e/ou restabelecer os níveis de funcionamento dos serviços disponibilizados às populações, a Marinha Portuguesa, na sua dupla função militar e não militar, tem uma área de responsabilidade de cerca de 3.858.431 km², e está dimensionada para utilizar os seus recursos e meios de modo a responder com prontidão a três pressupostos com vista a garantir o restabelecimento das ocorrências disruptivas:

- (1) 1.º Pressuposto: assegurar a sinergia de serviços de defesa e de segurança às populações costeiras, ribeirinhas ou que fazem uso do mar, face a um acontecimento corrente, perturbador ou disruptivo;
- (2) 2.º Pressuposto: garantir a autoridade do Estado no mar, através do fornecimento constante de serviços essenciais às populações costeiras, ribeirinhas ou que fazem uso do mar;

- (3) 3.º Pressuposto: acautelar quando a degradação ou indisponibilidade dos recursos e meio, ainda que temporária, possam gerar consequências negativas para a saúde, segurança e bem-estar social e económico das populações e salvaguarda do ambiente.

Todavia, a resiliência do duplo-uso da Marinha não se esgota em três pressupostos gerais. Para além, do duplo-uso estar ancorado a uma matriz comum de capacidades estruturantes, designadamente a doutrina, a organização, o treino, o material, a liderança, o pessoal e as infraestruturas, possibilitando assegurar compatibilidade, intermutabilidade e uniformidade, entre as tarefas de natureza militar e não militar, os trabalhos desenvolvidos por Ribeiro (2008), conferem ao modelo a base científica do processo adaptativo de transformação que vai permitir à Marinha prosseguir o seu propósito intergeracional, articulando a herança do passado com as exigências e os desafios do presente (Ribeiro, 2008; Documentação da Marinha, 2011).

De acordo com este autor, o desenvolvimento de uma visão estratégica permite conciliar a matriz da herança naval portuguesa com fatores inovadores de clareza, de precisão, baseado no método científico. Ribeiro refere que, para adaptar e transformar a Marinha aos tempos modernos, é fundamental edificar os meios, estruturar as suas capacidades, cumprir eficazmente a sua missão no presente e projetar-se para o futuro de uma forma sustentável, sublinhando ainda que, uma estratégia, nomeadamente naval, deve ser sustentada de uma forma determinante, pela decisão e pelo rigor de conceitos que emergem de metodologias comprovadas cientificamente.

Entre inúmeros contributos conceptuais e empíricos inovadores, formulados por Ribeiro e que contribuíram para a elaboração da estratégia naval, o conceito de paradigmas de transformação captou toda a nossa atenção, por se coadunarem com a integração dos conceitos de resiliência desenvolvidos na literatura.

Este autor considera que uma base paradigmática é fundamental para traduzir um modelo de representação que permita perceber com maior clareza o papel da Marinha. Os paradigmas de transformação foram construídos por este autor, de acordo com uma lógica sistémica, que permitisse respeitar “a observação do modelo de gestão estratégica, destinado a assegurar que o Estado está coerentemente organizado”.

Fazendo *jus* à história da herança portuguesa, os trabalhos desenvolvidos por este autor transformaram um modelo organizacional histórico, num constructo teórico de duplo-uso, onde é possível identificar a resiliência ao serviço da sustentabilidade.

Primeira Propriedade da Resiliência ao Serviço da Fiabilidade de Duplo-Uso: o Equilíbrio

No âmbito da resiliência, a dimensão genética manifesta-se mediante as inúmeras ligações que permitem criar uma estrutura que possibilite a ocorrência de sinergias

na edificação de novos meios, em pessoal e material, interligadas com capacidades diversificadas e conjugáveis, no sentido de constituir uma estrutura organizacional equilibrada que responda às necessidades.

Consideram-se os seguintes benefícios genéticos: o equilíbrio nas capacidades, a economia de escala, e a interoperabilidade de capacidades.

a) O Equilíbrio nas Capacidades

O equilíbrio nas capacidades está relacionado com uma lógica de proporcionalidade entre a ambição de responder à imprevisibilidade das ameaças do atual ambiente estratégico e a articulação com os meios e ações prioritárias, ou seja, decorre da justa conjugação entre os meios e as ações. Exemplo: capacidade de gerir a ambição com os recursos equitativamente distribuídos nas várias ações.

b) Economia de Escala

O conceito de economia de escala é empregue para explicar que, quanto mais um sistema produz em grande quantidade menor é o custo unitário do produto. No modelo de duplo-uso a economia de escala manifesta-se na produção de um grande leque de atividades produzidas por um número reduzido de pessoas. No âmbito dessas inúmeras atividades podemos identificar as principais áreas onde verificamos o conceito de economia de escala:

- (1) Pessoal: um mesmo indivíduo desempenha várias funções complementares;
- (2) Formação: o sistema de formação profissional está integrado para o desempenho de tarefas de âmbito militar e não militar;
- (3) Material: os navios da Marinha são aprontados para o desempenho de atividades militares de defesa e não militares de segurança;
- (4) Infraestruturas: a ocupação de espaços para fins militares e não militares;
- (5) Logística: a gestão partilhada de apoio é exercida ao nível dos sistemas e aquisição, manutenção e abastecimento de meios;
- (6) Administração de recursos financeiros: a gestão dos recursos financeiros decorre de uma única estrutura para o efeito;
- (7) Informação: a centralização dos processos de gestão da informação e da administração da tecnologia da informação.

Exemplo: todos os recursos obedecem a uma lógica de duplo uso, ou seja, todos os recursos materiais e humanos são utilizados simultaneamente para fins militares e não militares sem duplicação.

c) Interoperabilidade de Capacidades

A interoperabilidade de capacidades deriva do facto de a Marinha utilizar uma matriz comum de elementos funcionais tais como: a doutrina, a organização, o treino, o material, a liderança, o pessoal e as infraestruturas, no sentido de garantir

a compatibilidade, a intermutabilidade e uniformidade entre as capacidades militares e não militares. A interoperabilidade permite estabelecer uma comunicação de qualidade de modo a criar coerência entre os vários elementos do sistema. Exemplo: o papel da doutrina na inclusão de uma visão integrada militar e não militar em prol da defesa e segurança das populações.

Segunda Propriedade de Resiliência ao Serviço da Fiabilidade do Duplo-Uso: a Otimização

No âmbito da resiliência, a dimensão estrutural manifesta-se nas sinergias criadas na composição estrutural da organização, em articulação com os meios, o pessoal e o material, segundo capacidades interdependentes e colaborantes fundamentais para constituir uma Marinha otimizada. Consideram-se os seguintes objetivos estruturais: a economia de esforço, a coordenação do emprego dos meios e a articulação interdepartamental.

a) A Economia de Esforço

A economia de esforço é a predisposição da Marinha em adequar os meios, com vista ao seu emprego de forma ajustada à materialização dos objetivos nacionais no mar. Exemplo: o planeamento em matéria de vigilância e de fiscalização marítima.

b) A Coordenação do Emprego dos Meios

A coordenação do emprego dos meios é o resultado adequado da unidade de comando. Ao nível estratégico, a unidade de comando resulta do facto do Chefe do Estado-Maior da Armada ser, por inerência do cargo, Autoridade Marítima Nacional. Ao nível operacional regional, resulta do facto dos comandantes das Zonas Marítimas Norte, Sul, Açores e Madeira, serem simultaneamente chefes dos respetivos Departamentos Marítimos. Ao nível local, a coordenação do emprego de meios resulta da inerência funcional no exercício de polícia, no quadro da Autoridade Marítima Nacional, existente entre o Capitão do Porto e o Comandante Local da Polícia Marítima. Esta acumulação de funções constitui o mecanismo operacional e jurídico adequado que permite agilizar a eficácia da autoridade de polícia e de polícia criminal que a lei delega expressamente aos titulares dos cargos na estrutura da Autoridade Marítima, outorgando uma possibilidade facilitadora em termos de imposição da lei e da ordem nos espaços marítimos. Exemplo: os comandantes das Zonas Marítimas são simultaneamente os chefes dos respetivos Departamentos Marítimos, esta circunstância permite agilizar e integrar atuações em tempo oportuno.

c) A Articulação Interdepartamental

A articulação interdepartamental resulta da postura proactiva dos vários órgãos da Marinha e da intensa cooperação com os outros departamentos do Estado com

competências sobre os espaços marítimos e as atividades que neles operam. Todavia, a tradição, a vocação, o conhecimento, a competência e a capacidade da Marinha para atuar no mar, conferem-lhe um papel potenciador da ação do Estado no mar, assegurando coerência na atuação e racionalização dos custos, sempre muito dispendiosos, no que respeita à aquisição, manutenção e operações empregues. Exemplo: a cooperação intra e interdepartamental com todos os atores com competência sobre os espaços marítimos permite treinar e construir interdependências robustas. Em caso de catástrofes de grande amplitude podem refletir-se na capacidade de coordenar recursos materiais e humanos.

Terceira Propriedade de Resiliência ao Serviço da Fiabilidade do Duplo-Uso: a Flexibilidade

No âmbito da resiliência, a dimensão operacional expressa-se pelos ganhos conseguidos no emprego dos meios em pessoal e material, segundo capacidades de projeção de força, de proteção do mar e de colaboração, comando e controlo, essenciais para constituir uma Marinha de duplo-uso. Constituem benefícios operacionais, a flexibilidade de atuação, a gradação do uso das capacidades e a coerência na atuação.

a) A Flexibilidade de Atuação

A flexibilidade de atuação decorre de uma alargada gama de tarefas com um limitado conjunto de meios. Pautado pelo princípio da legalidade as unidades operacionais da Marinha são treinadas de modo a operarem no quadro do duplo uso, de modo a desempenharem várias tarefas, potenciando a polivalência e as interoperabilidades. Exemplo: a utilização dos recursos materiais e humanos no combate ao terrorismo, à poluição, ou ainda em missões de vigilância.

b) A Gradação do Uso das Capacidades

A gradação do uso das capacidades resulta da possibilidade de empregar em âmbito não militar, capacidades essencialmente vocacionadas para a atuação militar, respeitando os princípios da necessidade, da legalidade e da proporcionalidade no emprego da força. Deste modo, perante ameaças de âmbito securitário que requeiram uma intervenção mais musculada, ou perante catástrofes cuja resposta exija capacidades mais robustas, a Marinha tem a possibilidade de usar as unidades operacionais que ofereçam melhores garantias de eficácia. Exemplo: o uso das forças na Marinha, na catástrofe ocorrida na Madeira em 20 de fevereiro de 2010.

c) A Coerência na Atuação

A coerência na atuação decorre de três aspetos, que contribuem para garantir maior clareza e uniformidade à ação do Estado no mar. Em primeiro lugar, a abrangência de competências da Marinha de duplo-uso permite-lhe atuar num espectro muito

alargado e definido de tarefas. Em segundo lugar, o facto de essas competências se exercerem em todos os espaços marítimos sobre soberania ou jurisdição nacional e, mesmo, no alto mar permite-lhe atuar em *continuum*. Em terceiro lugar, a postura colaborativa da Marinha, relativamente a todos os outros intervenientes nos espaços marítimo, potencia a coerência da intervenção do Estado no mar. Exemplo: (1) a Marinha desempenhar tarefas militares e não militares; (2) essas tarefas são exercidas nos espaços de jurisdição que vão desde a faixa costeira até ao mar aberto; (3) a cooperação como os outros atores que atuam no espaço marítimo.

De acordo com o exposto as propriedades de resiliência identificada na Marinha permitem garantir, simultaneamente que o sistema absorva choques, mas também que garanta a sustentabilidade.

A Sustentabilidade da Marinha de Duplo-Uso

De acordo com Popper (2011), o conhecimento humano tem um valor provisório, até ser submetido ao processo de adaptação inerente a uma determinada conjectura ambiental por intermédio da experiência que lhe confere validade.

Como já foi referido, muito antes da Comissão Mundial para o Ambiente e Desenvolvimento (1987) ter associado a definição de sustentabilidade como a noção de garantir as necessidades das gerações presentes sem comprometer as necessidades das gerações futuras, num quadro de equilíbrio entre os pilares social, económico e ambiental, os monarcas portugueses lançaram as bases vanguardistas, do que seria um dia reconhecido como um sistema sustentável.

Historicamente, o duplo-uso encontra a sua validade nas mais antigas raízes marítimas da história de Portugal, numa época em que os monarcas portugueses descortinaram a oportunidade de alinharem estrategicamente os poucos recursos disponíveis, à capacidade estratégica de defesa e de segurança, com o conhecimento e uma grande visão de desenvolvimento marítimo e energia para conquistar os espaços marítimos (Pedrosa, Pereira e Guerreiro, 1997; Barros *et al.*, 1998; Pereira, 2010). Fillion (2010) refere que a visão de uma organização, é a imagem que ela projeta para o futuro. Este autor sustenta que essa visão está relacionada com a maneira de ser, de pensar, de agir ou de imaginar de uma pessoa ou de um grupo, que pretende conferir continuidade à sua organização. Para tal, o autor refere que é indispensável identificar situações oportunas, conceber, desenhar, criar valor nas oportunidades, para transformar a visão em realidade. De acordo com este autor, consideramos que a singularidade do duplo-uso responde a esta circunstância.

Com efeito, no caso português, a sustentabilidade deste modelo está vinculada à visão de uma geração de monarcas, cuja visão transitou para a república, evidenciando, assim, a pertinência nacional deste modelo ao serviço da otimização das interdependências organizacionais, que permitissem responder aos melhores desígnios de defesa, segurança e desenvolvimento do país.

Para tal, revisitar a história de Portugal, para compreender um pouco mais acerca do significado da Marinha na construção de Portugal, implica o encontro inevitável com a memória das grandes figuras históricas que povoam o nosso imaginário. Figuras como D. Afonso Henriques, D. Dinis, D. João I, D. João IV, que tiveram o mérito de garantir a emergência, o desenvolvimento e a consolidação do território terrestre, brilham ao lado de um outro conjunto de figuras emblemáticas, tais como, o Infante D. Henrique e D. João II, que abriram possibilidades científicas e políticas para que grandes pioneiros marítimos, tais como, João Zarco, Tristão Vaz Teixeira, Diogo de Silves, Diogo de Teive, Bartolomeu Dias, Vasco da Gama, Álvares Cabral, impulsionassem uma alteração e transformação radical da economia portuguesa e da Europa do Renascimento (Saraiva, 1978; Labourette, 2000; Matias, 2017).

Se, por um lado, sintetizar a história da Marinha Portuguesa em algumas linhas, no sentido de identificar a fundamentação do duplo-uso é uma tarefa árdua, por outro lado, esta síntese é compensada por oferecer uma imagem estilizada, uma “pinçelada” que nos permite captar a essência deste modelo, cujo destino contribuiu para conferir a Portugal prestígio e brilho e onde se consolidou a sua identidade marítima. Neste sentido, podemos afirmar que não é o mar que confere identidade marítima a um povo, mas a vontade e o engenho desse povo em conquistá-lo e forjar o seu carácter nessa conquista.

O modelo de organização naval, ancorado ao duplo-uso, consolidou-se de uma forma tão coerente e implícita ao longo do tempo, que foi necessário esperar o século XIX, para o modelo ser reconhecido numa época de crise, como um modelo de sustentabilidade, capaz de enfrentar eficazmente as turbulências económicas nacionais. Com efeito, o Decreto Ministerial de 6 de agosto de 1892 refere aquilo que podemos considerar como o reconhecimento do duplo-uso “possuindo o país, infelizmente, uma marinha pequena, aproveitar o que há na execução de serviços que podem praticar-se ao mesmo tempo e com a mesma despesa, não é só aconselhável, é uma obrigação indeclinável de quem pretende organizar e constituir com o pouco que há, a base do muito que há a fazer”. Porém a legitimidade do duplo-uso já estava em curso, apresentando pequenos laivos de afirmação. Diogo (2009) refere que o duplo-uso afirma a sua existência jurídica, na publicação do Alvará Real, de 15 de novembro de 1802, onde é determinado que os Patrões-Mores, a quem cabia a função do exercício de autoridade marítima, fossem selecionados entre os oficiais da Armada, devido às suas competências marítimas, estabelecendo assim, de acordo com este autor e grande conhecedor das questões jurídicas da Marinha, uma ligação indissociável entre os oficiais de Marinha e o exercício de funções de Autoridade Marítima, que permaneceu até aos nossos dias.

Apesar de Pereira (2010) ter abordado a história da Marinha numa perspetiva diacrónica, ao longo de 900 anos, foi Pacheco (2014) que traçou o perfil da Marinha na sua dimensão de resiliência, isto é, a capacidade de um sistema superar choques

mantendo a integridade dos seus pilares. Este autor identificou nove grandes períodos da história da Marinha (tabela 1), onde podemos identificar a presença de um padrão relativamente coeso no tocante, por um lado às funções exercidas pela Marinha, mas também podemos identificar que cada período é transformado por uma rutura que dá origem a uma mudança significativa, dando lugar a outro período de forma adaptativa, mantendo o padrão da sua identidade.

Tabela 1 – Síntese de Nove Períodos Históricos da Marinha Portuguesa

Períodos	Início	Caracterização do período	Fim do período
1.º	Era cristã e Fundação da Nacionalidade	Importância dos assuntos militares-navais orientados, criação de uma Marinha organizada para a conquista e defesa do território.	Nomeação oficial do primeiro almirante mor (1307)
2.º	1307	As potencialidades marítimas de Portugal levaram ao desenvolvimento económico e social do país.	Passagem do Cabo da Boa Esperança e morte do rei D. João II (1495)
3.º	1495	Grandes retornos comerciais dos descobrimentos levaram ao desenvolvimento da função securitária da Marinha, para responder à atividade de corso e pirataria.	Subida ao trono dos Filipes de Espanha (1580)
4.º	1580	Neste período em que Portugal foi governado pela monarquia espanhola, as muitas implicações estenderam-se às áreas económicas, incluindo grandes transformações ao nível dos meios e da organização da Marinha.	Restauração da Independência (1640)
5.º	1640	Portugal vive um período de grande empobrecimento, o que implicou uma retração nos meios, organização e atividades da Marinha.	A criação da Secretaria de Estado dos Negócios da Marinha e Ultramar (1743)
6.º	1743	Este período marcado por um turbilhão político e tecnológico ao nível da construção naval, a Marinha adquiriu o estatuto de órgão ministerial.	Implantação da República (1910)
7.º	1910	Período de grande avanço tecnológico que cobriu duas guerras mundiais e em que Portugal se tornou membro fundador da NATO.	Início da Guerra de África (1961)
8.º	1961	A resposta a esta guerra implicou o desenvolvimento e edificação de capacidades navais.	Instauração do regime democrático e fim do império ultramarino português (1974)
9.º	1974	Foram redefinidos os conceitos estratégicos navais, as missões, sistemas de força e os dispositivos.	Até aos nossos dias

Fonte: adaptado de Pacheco (2014).

Na tabela 2, podemos identificar que, ao longo de nove períodos da história naval, a Marinha Portuguesa pautou a sua atuação em função de três categorias funcionais: a defesa, a segurança e o desenvolvimento, no uso do mar. Ainda é possível identificar que a Marinha exerceu a função de defesa em quatro períodos chave de conquista e guerra e que a função de segurança é transversal a todos os períodos históricos, assim como a função de desenvolvimento.

Tabela 2 – Categorias Funcionais Identificadas ao Longo de Nove Períodos da História da Marinha

Categorias funcionais	Períodos mais relevante	Caracterização
Defesa	1.º, 2.º, 7.º e 8.º	Consolidação do território e Guerra Colonial
Segurança	1.º, 2.º, 3.º, 4.º, 5.º, 6.º, 7.º, 8.º e 9.º	Transversal a todos os períodos
Desenvolvimento	2.º, 3.º, 4.º, 6.º, 7.º, 8.º e 9.º	Transversal exceto na consolidação do território e pós restauração

Neste sentido, consideramos que, à luz do relatório Brundtland, a Marinha de duplo-uso enquadra-se na definição de sustentabilidade, segundo a qual esta é definida num quadro intergeracional, como a responsabilidade de satisfazer as necessidades das gerações presentes, sem invalidar as necessidades das gerações futuras, proporcionando o equilíbrio dos pilares social, económico e ambiental, com as prioridades políticas em matéria de defesa e segurança do uso do mar.

Atualmente, o pilar social continua a suportar toda a ação de defesa e de segurança das populações (Ribeiro, 2010; Documentação da Marinha, 2011). O pilar económico sustenta os novos *clusters* de desenvolvimento da economia do mar, com todas as variantes relacionadas com a economia azul e a futura gestão da Plataforma Continental estendida (Monteiro, 2011; Silva, 2012; Resende, 2017). O pilar ambiental garante a proteção ambiental do espaço marítimo (DGAM, 2011).

A tabela 3 apresenta uma síntese, na qual podemos observar uma relação inequívoca entre os pilares das funções estratégicas da Marinha de duplo-uso com os pilares da sustentabilidade. Podemos verificar que todos os critérios estão preenchidos, isto é, as funções dos pilares estratégicos da defesa, da segurança e da economia contribuem para o pilar social, económico e ambiental, conferindo à Marinha de duplo-uso um estatuto de sustentabilidade.

Tabela 3 – Intercessão dos Pilares das Funções Estratégicas de Duplo-Use com os Pilares de Sustentabilidade

Pilares das funções Estratégicas de duplo-uso	Pilares de Sustentabilidade		
	Pilar social	Pilar da economia	Pilar ambiental
Pilar da Defesa	X	X	X
Pilar da Segurança	X	X	X
Pilar do Desenvolvimento	X	X	X

A partir da representação das funções estratégicas e tarefas da função naval (figura 1), concebemos uma representação estrutural do modelo de duplo-uso que permitisse testar graficamente a coerência do modelo.

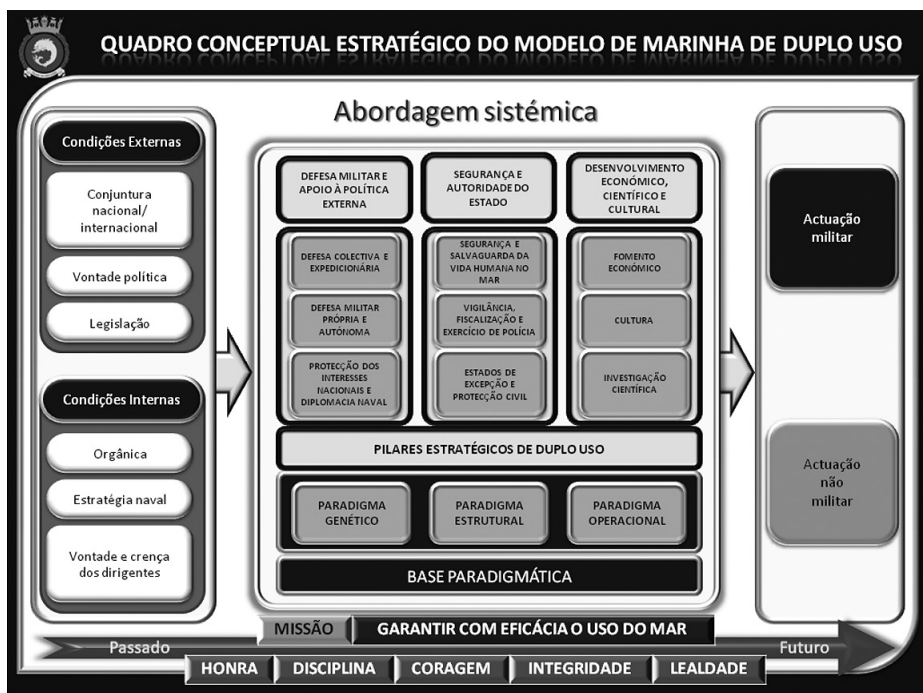
Figura 1 – Funções Estratégicas e Tarefas da Função Naval (2011)



Fonte: imagem cedida graciosamente pelo Estado-Maior da Armada.

De acordo com a abordagem sistémica de Bertalanffy, podemos identificar (figura 2) que estruturalmente, o modelo de duplo-uso está alicerçado numa base paradigmática constituída por três paradigmas de transformação, designadamente o paradigma genético, o paradigma estrutural e o paradigma operacional, onde assentam três pilares estratégicos: defesa militar e apoio à política externa, segurança e autoridade do Estado no mar e desenvolvimento económico, científico e cultural. Cada pilar estratégico é por sua vez constituído por três vertentes, designadamente: (1) o pilar da defesa militar e apoio à política externa é constituído pelas suas três vertentes, a defesa coletiva e expedicionária, a defesa militar própria e autónoma, a proteção dos interesses nacionais e diplomacia naval); (2) o pilar da segurança e autoridade do Estado no mar é constituído pelas suas três vertentes, a segurança e salvaguarda da vida humana no mar, a vigilância, fiscalização e exercício de polícia, os estados de exceção e proteção civil; (3) o pilar de desenvolvimento económico, científico e cultural é constituído pelas suas três vertentes, fomento económico, cultura e a investigação científica.

Figura 2 – Quadro Conceptual Estratégico do Modelo da Marinha de Duplo-Use (2011)



Fonte: elaborada pela autora com o apoio gráfico da Divisão de Planeamento do Estado-Maior da Armada.

Tendo como *input* as condições externas e as condições internas, e fundamentados nos valores de honra, disciplina, coragem, integridade e lealdade, na linha do tempo, a Marinha de duplo-uso tem como missão garantir a eficácia no mar através de um *output* constituído por uma atuação militar e não militar.

Tendo em conta a fundamentação desenvolvida neste artigo, em colocar a Marinha de duplo-uso na sua merecida posição de sustentabilidade, este modelo teórico, concebido por Ribeiro, e reinterpretado, no nosso trabalho de investigação, à luz dos conceitos de resiliência e de sustentabilidade, pretende evidenciar a coerência da construção do modelo, através da representação de uma figura geométrica (figura 3), no qual podemos observar a estrutura do duplo-uso materializado numa pirâmide, que por sua vez, sugere o grande equilíbrio das proporções do modelo.

Figura 3 – Representação Piramidal do Duplo-Uso



Fonte: elaborada pela autora com o apoio gráfico da Divisão de Planeamento do Estado-Maior da Armada.

Conclusão

Embora, numa primeira abordagem, o modelo de duplo-uso da Marinha Portuguesa possa suscitar alguns contornos paradoxais, resultantes da falta de compreensão do modelo que estabelece a harmonização entre a componente militar e a componente não militar, numa análise mais detalhada este modelo apresenta uma coerência sistémica que veicula uma visão de sustentabilidade.

Com efeito, numa época em que a ciência e a política estão a integrar a resiliência e a sustentabilidade para garantir a perenidade dos sistemas organizacionais, a Marinha Portuguesa representa um modelo intergeracional que soube integrar a visão de sustentabilidade, de modo a garantir a satisfação de defesa e segurança das gerações passadas, continuando a garantir as necessidades das gerações presentes e desenvolvendo um modelo cientificamente irrefutável, para o modelo continuar a garantir as necessidades e os desafios das gerações futuras.

Com efeito, à luz do relatório Brundtland, o duplo-uso é um modelo intergeracional sustentável, que garantiu, ao longo de mais de 700 anos, na Marinha Portuguesa, a integridade dos seus pilares social, económico e ambiental, mediante a capacidade de resiliência que definimos da seguinte forma: *a resiliência não é a adaptação, nem a continuidade operacional, a resiliência é a capacidade de um sistema restabelecer os processos de adaptação que foram interrompidos devido à*

ocorrência de uma choque destruturante, criando assim uma nova estrutura com maior amplitude.

A grande lição aprendida neste estudo e, seguramente, um dos contributos mais relevantes, é compreender que a resiliência é determinante para a fiabilidade de um sistema e consequentemente para a sua sustentabilidade.

Referências

- Ban Ki-moon, 2014. *Rapport de Synthèse du Secrétaire général des Nations Unies sur le programme de développement durable pour l'après 2015*, A/69/700. Nova Iorque: Nations Unies.
- Boulanger, P.-M., 2004. Les indicateurs de développement durable : un défi scientifique, un enjeu démocratique. Conférence donnée lors du Séminaire *Développement durable et économie de l'environnement*, organisé par l'Iddri et la Chaire Développement durable de l'Ecole polytechnique-EDF. Institut pour un développement durable, pp. 1-24.
- Brundtland, G., 1987. *Report of the World Commission on environment and Development: Our Common future*. Oxford: Oxford University Press.
- Carpenter, S., Walker, B., Anderies, J. e Abel, N., 2001. From Metaphor to Measurement: Resilience of What to What? *Ecosystems*, 4(8), pp. 765-781.
- Comfort, L., Boin, A., e Demachak, C., eds., 2010. *Designing Resilience: Preparing for Extreme Events*. University of Pittsburgh Press.
- Cornum, R., Matthews, M. e Seligman, M., 2011. Comprehensive Soldier Fitness: Building Resilience in a Challenging Institutional Context. *American Psychologist*, 6(1), pp. 4-9.
- Coste, F. e Nexon, E., 2011. *La contribution des armées à la résilience de la Nation : aspects humains e organisationnels*, Rapport n° 702/FRS, 17 de novembro. Relatório Final, Fondation por la Recherche Stratégique.
- Dalziell, E.P. e McManus, S.T., 2004. *Resilience, Vulnerability, and Adaptive Capacity: Implication for System Performance*. Paper presented at the 1st International Forum for Engineering Decision Making (IFED), 5-8 Dec 2004, Stoops, Switzerland.
- Derissen, S., Quaas, M. e Baumgärtner, S., 2009. *The relationship between resilience and sustainable development of ecological-economic systems*. Working paper series in Economics, University of Lüneburg.
- Desnos, V., 2012. « Royal Navy : Résilience passée, renoncement futur ? ». *Centre d'Étude Stratégique de la Marine*, pp. 1-10. Disponível em: <http://en.calameo.com/read/000151499c2d814885a58>
- Diogo, L., 2012. Mais de 210 anos de Capitania do Porto e uma década de Autoridade Marítima Nacional, *Revista da Armada*, n.º de abril.
- Diogo, L., 2009. O Capitão de Porto, mais de 4 séculos de Autoridade Marítima ao serviço das Comunidades. *Anais do Clube Militar Naval*, vol. CXXXIX, pp. 685-692.

- Direcção-Geral da Autoridade Marítima, 2011. *Guia de apoio ao combate à poluição do mar por hidrocarbonetos e outras substâncias perigosas*, Vol. 1. Lisboa: Direcção-Geral da Autoridade Marítima.
- Dreibelbis, C., ed., 2008. *Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy*. Washington: The Reform Institute, pp. 36.
- Duarte, D., Palma, J., Pereira, L., Ramalheira, S., Borges, L., Lemos, C., Cordeiro, J. e Filho, R., 2010. *A contextualização e a articulação do conceito de Marinha de Duplo-Uso no âmbito do planeamento estratégico marítimo, do planeamento estratégico naval e da doutrina estratégica naval portuguesa*. Lisboa: IESM.
- Fillion, L., 2012. *Oser intraprendre : Ces champions qui font progresser les organisations et les sociétés*. Presses Inter Universitaires.
- Folke, C., Carpenter, S., Walker, B., Scheffer, M., Chapin, T., e Rockström, J., 2010. Resilience Thinking: Integrating Resilience, Adaptability and Transformability. *Ecology and Society*, 15(4). Disponível em: art20. <http://doi.org/10.5751/ES-03610-150420>.
- Folke, C., Carpenter, S., Elmqvist, T., Gunderson, L., Holling, C., e Walker, B., 2002. Resilience and Sustainable Development: Building Adaptive Capacity in a World of Transformations. *AMBIO: A Journal of the Human Environment*, 31(5), pp. 437-440. Disponível em: <http://doi.org/10.1579/0044-7447-31.5.437>
- Fonseca, H. A., 1976. A divisa da armada. *Revista da Armada*, Lisboa.
- Gambardella, S., 2017. Océans et changements climatiques : Rechercher les interactions au sein de la fragmentation du droit international. *Revista de Direito Internacional*, 14(3), pp. 45-54. Disponível em: <http://doi.org/doi:10.5102/rdi.v14i3.4983>
- Glaser, M., Plass-Johnson, J., Ferse, S., Neil, M., Satari, D., Teichberg, M. e Reuter, H., 2018. Breaking Resilience for a Sustainable Future: Thoughts for the Anthropocene. *Frontiers in Marine Science*, 5, pp. 1-7. Disponível em: <http://doi.org/10.3389/fmars.2018.00034>
- Guedes, H., 2014. Pirataria Marítima: da Ficção à realidade. *Revista da Armada*, n.º 488, pp. 11-13. Disponível em: http://www.marinha.pt/Conteudos_Externos/RevistaArmada/_FlipVersion/2014/488/index.html
- Hamel, G. e Valikangas, L., 2003. Quest for Resilience. *Harvard Business Review*, pp. 1-13.
- Holling, C., 1973. Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4, pp. 1-23.
- Hollnagel, E., Journé B. e Laroche, H., 2009. Fiabilité et résilience comme dimension de la performance organisationnelle : introduction. *Management*, 12(4), pp. 224-229.
- Instituto Nacional de Estatística e Direcção-Geral de Política do Mar, 2014. Conta Satélite do Mar: Definição conceptual de “Economia do Mar”, Lisboa.
- ISDR, 2005. *Hyogo Framework for Action 2005- 2015: Building the Resilience of Nations and Communities to Disasters*. Extract from the final report of the World Conference on Disaster Reduction, A/CONF.206/6.

- Koninckx, G. e Teneau, G., 2010. *Résilience Organisationnelle*. Bruxelas: De Boeck Supérieur.
- Labourette, J.-F., 2000. *Histoire du Portugal*. Paris: Edition Fayard.
- Lagadeuc, Y. e Chenorkian, R., 2009. Les systèmes socio-écologiques : vers une approche spatiale et temporelle. *Natures Sciences Sociétés*, 17(2), pp. 194-196. Disponível em: <http://doi.org/10.1051/nss/2009032>
- Lallau, B., 2011. La résilience, moyen et fin d'un développement durable ? *Ethics and Economics*, 8(1), pp. 168-185. Disponível em: <hdl.handle.net/1866/4589>.
- Lemay, M., 1999. Réflexions sur la résilience. Em Marie-Paule Poilpot, ed., *Souffrir mais se construire*. Ramonville Saint-Agnès : Fondation pour l'Enfance Erès.
- Lima, J., 1950. *A marinha através dos tempos: Conferência proferida na Sociedade de Geografia de Lisboa*. Porto: [s.n.t.].
- Machado, S., 1973. A heráldica na Armada. *Revista da Armada*. Lisboa.
- Marinha Portuguesa, 2006. *Diretiva para as operações da Marinha (Paradigma Operacional. O conceito do Duplo Uso)*, Diretiva 002/2006 do CEMA.PAA32, Parte VIII. Documentação Estruturante da Estratégia Naval. Lisboa: Marinha.
- Marinha Portuguesa, 2011. *A Marinha ao Serviço de Portugal*. Estado-Maior da Armada. Atualmente Indisponível Online.
- Marinha Portuguesa, 2011. *A Marinha de Duplo Uso*. Estado-Maior da Armada. Atualmente Indisponível Online.
- Marinha Portuguesa, 2011. *Portugal, uma nação marítima*. Estado-Maior da Armada. Atualmente Indisponível Online.
- McManus, S., Seville, E., Vargo, J., e Brunson, D., 2008. Facilitated Process for Improving Organization Resilience. *Natural Hazards Review*, 9(2), pp. 81-90.
- Monteiro, N., 2011. A economia do mar e a segurança marítima I. *Revista Segurança e Defesa*.
- Paris, P., 1909. *Lexique des Antiquités Grecques*. Albert Fontemoing Éditeur.
- Pereira, J., 2010. *Marinha portuguesa: nove séculos de história*. Lisboa: Comissão Cultural da Marinha.
- Perrings, C., 2006. Resilience and sustainable development. *Environment and Development Economics*, 11, pp. 417-427, Cambridge University Press. Disponível em <doi:10.1017/S1355770X06003020>
- Popper, K., 1973. *La logique de la Recherche scientifique*. Edition Payot.
- Resende, C., e Direção-Geral de Política do Mar, 2017. *Conhecimento do mar: Mapa da Ciência e Tecnologias do mar em Portugal*. Lisboa.
- Ribeiro, A., 1998. *Elaboração da Estratégia de Defesa Militar: Contributo para um Novo Modelo*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.

- Ribeiro, A., Silva, F., Palma, J. e Monteiro, N., 2010. Estratégia Naval Portuguesa – O processo, o contexto e o conteúdo. *Cadernos Navais*, n.º 34. Lisboa: Grupo de Estudos e Reflexão Estratégica/Edições Culturais da Marinha.
- Rodrigues, T., 2010. A Estratégia Internacional de Redução de Desastres. *Revista Territorium*, n.º 17, pp. 223-227.
- Rodrigues, T., 2009. *Quadro de Ação de Hyogo: a resposta internacional para a redução de riscos de desastres*. 6.º Simpósio de Meteorologia e Geofísica da APMG, 10.º Encontro Luso-Espanhol de Meteorologia. APMG.
- Rodrigues, T., Ribeiro, A., Vasconcelos, L. e Robert, B., 2017. Teste diagnóstico de resiliência potencial: o radar da resiliência organizacional. *Revista de Gestão dos Países de Língua Portuguesa*, 16(1), pp. 44-64. Disponível em: <http://www.scielo.mec.pt/pdf/rpbg/v16n1/v16n1a04.pdf>
- Silva, J., 2012. A Plataforma Continental Portuguesa: Análise do Processo de Transformação do Potencial Estratégico em Poder Nacional. *Cadernos Navais*, 43. Lisboa: Edições Culturais da Marinha. Disponível em: file:///C:/Users/MPdAbreu/Downloads/cadernos_navais_n43_outubro_dezembro_2012.pdf.
- Sun Tzu, 2001. *A arte da Guerra*. Lisboa: Editora Campus.
- Taphanel, L., 2010. *Les organisations à haute fiabilité : un terrain d'apprentissage pour le DRH des entreprises cotées ?* Laboratoire PRISM, Sorbonne, Université Paris I. Panthéon Sorbonne.
- Templeman, D. e Bergin, A., 2008. *Taking a punch: Building a more resilient Australia* [pdf]. Strategic Insights ASPI 39, Australian Strategic Policy Institute. Disponível em ASPI [website] https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/SI39_Taking_a_punch.pdf?vcIJUhU3L9HG1gmbj04jrjQFW3YIOUj
- The White House, 2011. *Presidential Policy Directive/PPD-8: National Preparedness*. March 30, Washington.
- UN/ISDR (2005). *Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters*. Extract from the final report of the World Conference on Disaster Reduction, A/CONF.206/6. New York and Geneva.
- United Nations General Assembly, 2015. *Resolution 70/226. United Nations Conference to Support the Implementation of Sustainable Development Goal 14: Conserve and sustainably use the oceans, seas and marine resources for sustainable development*, Vol. A/RES/70/2.
- Walker, B., Holling, C., Carpenter, S. e Kinzig, A., 2004. Resilience, adaptability and transformability in social-ecological systems. *Ecology and Society*, 9(2), Art. 5. Disponível em: <http://www.ecologyandsociety.org/vol9/iss2/art5/>
- Weick, K., e Sutcliffe, K., 2007. *Managing the Unexpected Resilient Performance in an Age of Uncertainty*. San Francisco: Jossey-Bass.
- Weick, K., Sutcliffe, K. e Obstfeld, D., 1999. Organizing for high-reliability: processes of collective mindfulness. Em R.S. Sutton e B.M. Staw, eds., *Research in Organizational Behavior*, Vol. 1. Stanford: Jai Press, pp. 81-123.

O Conceito de Emprego das Forças Armadas em Matérias de Segurança Interna

Nuno Imperial

Capitão de Artilharia e investigador da Academia Militar. Doutorando em Direito e Segurança na Faculdade de Direito na Universidade Nova de Lisboa.

Resumo

O artigo tem por finalidade descrever e analisar o enquadramento jurídico do emprego das Forças Armadas em matérias de segurança em Portugal, para validar a sua legitimidade de emprego em circunstâncias específicas.

Apresenta-se um quadro teórico, assente na legislação nacional em vigor, que permite descrever a realidade do emprego das Forças Armadas em contextos de segurança interna.

Abstract

The Armed Forces' Deployment Concept in a Domestic Security Framework

The article describes and analyze the legal framework concerning the deployment of Armed Forces in domestic security situations in Portugal, to validate its legitimacy under specific circumstances.

It presents a theoretical framework, based on the national legislation, capable of providing a proper understanding of such possibility.

Introdução

O presente artigo analisa os aspetos que relacionam o emprego das Forças Armadas (FA), em contextos de segurança interna, com o enquadramento jurídico português que permite às FA apoiarem, com carácter supletivo e em complementaridade, as Forças e Serviços de Segurança (FSS), no âmbito das outras missões de interesse público preconizadas para as FA.

O objetivo é apresentar um quadro teórico, assente na legislação nacional em vigor, que permita descrever a realidade do emprego das FA em contextos de Segurança “no espaço sujeito aos poderes de jurisdição do Estado Português”¹.

O tema enunciado merece posições bem distintas e diferentes entre personalidades do meio académico, das FA e das FSS. No entanto, há pontos de convergência e linhas de pensamento, em determinados aspetos, que são consensuais.

Pelo acima mencionado, orientou-se a investigação no sentido de se conseguir refletir e conhecer, em que medida é legítimo o emprego das FA em contextos de segurança interna.

O tema ora tratado é importante e pertinente no que toca à compreensão do potencial contributo das FA para um Sistema Nacional de Segurança que compreenda a Defesa Nacional (DN) e também a Segurança Interna (SI), através da atividade das próprias FA, em *subsidiariedade* e complementaridade das FSS, em Portugal.

Adotou-se uma abordagem qualitativa e desenhou-se um modelo de análise que delimitou, como objeto de estudo, o conceito de emprego legítimo das FA na segurança interna, enquanto facto observável.

Neste âmbito, a questão da legitimidade² é entendida como:

“O suporte da noção de obediência voluntária que leva a um sentimento de obrigação, de dever ou de vontade de obedecer às normas e às leis e naturalmente às autoridades consideradas legítimas.” (Lourenço, 2012, p. 183).

Para definir este conceito – o emprego legítimo das FA em situações de segurança interna – criou-se um modelo teórico assente na metodologia de investigação em Ciências Sociais. Para o efeito, recorreu-se a Quivy e Campenhoudt (2013, pp. 259-275) para se determinar a forma de eleger os critérios de racionalidade capazes de definirem o conceito ora estudado.

Assim, elegeram-se três critérios, os quais equivalem aos critérios de legitimidade que são definidos consoante as ameaças à segurança, da seguinte forma:

1 Considerando o âmbito territorial para o desenvolvimento da Segurança Interna, nos termos do Artigo 4.º da Lei de Segurança Interna, Lei n.º 53/2008, de 29 de agosto, alterada pela Lei n.º 59/2015, de 24 de junho e pelo D.L. n.º 49/2017, de 24 de maio.

2 Segundo Nélson Lourenço (2012, p. 190), “a legitimidade e a confiança nas polícias são elementos significativos, (...) na definição de políticas de segurança”.

- (a) um critério jurídico, com indicadores de observação, tais como a legislação nacional em vigor, as normas e regulamentos militares e as opções políticas de DN e de SI;
- (b) um critério operacional, observável através da existência de exercícios de treino e formação dedicados, da existência de operações das FA levadas a cabo em apoio das FSS, das capacidades e competências existentes nas FA, e ainda, da presença institucional de elementos militares das FA em estruturas de Segurança tuteladas pela DN³;
- (c) por fim, um critério social e securitário, com indicadores de observação tais como a avaliação da ameaça, o contexto social de insegurança e a falta de determinados meios nas FSS, necessários para responder a eventuais ameaças à segurança.

Relativamente ao método de recolha de dados, escolheu-se o método de análise de conteúdo para testar a hipótese: “Quanto mais os critérios de legitimidade se verificam perante uma determinada ameaça à segurança, mais se torna legítimo o emprego das FA, e vice-versa”.

Da hipótese avançada, recorrendo a uma matriz de análise estruturada em Heuer e Pherson (2011, pp. 59-63) formulou-se o seguinte:

- (a) quando os três critérios considerados se verificam – é completamente legítimo o emprego das FA na segurança interna;
- (b) quando o critério jurídico e outro se verificam – em caso de necessidade, é legítimo e razoável o emprego das FA na segurança interna;
- (c) quando só o critério jurídico se verifica – em circunstâncias específicas é legítimo e pontual o emprego das FA na segurança interna;
- (d) quando nenhum dos critérios considerados se verifica – não é legítimo e é nulo o emprego das FA na segurança interna.

Tendo presente neste estudo que em circunstâncias de exceção há lugar à atuação das FA em complemento das FSS, defende-se que “sem segurança não há liberdade, mas a segurança terá de ser assegurada num quadro de plena legitimidade democrática” (Lourenço, 2012, p. 194).

O presente artigo tece algumas considerações sobre o conceito de segurança e sobre o emprego das FA em contextos de segurança interna. Posteriormente descreve o enquadramento jurídico que permite o emprego das FA nestas circunstâncias, especificando as principais missões neste âmbito e mostrando as capacidades das FA

3 Consideram-se as estruturas de Segurança (organismos públicos/autoridades) tuteladas pelo Ministério da Defesa Nacional e que têm responsabilidades no Sistema de Segurança Interna, e.g. a Autoridade Marítima Nacional, a Autoridade Aeronáutica e o Chefe do Estado-Maior-General das Forças Armadas. Vd. Lei n.º 53/2008, de 29 de agosto, alterada pela Lei n.º 59/2015, de 24 de junho e pelo Decreto-Lei n.º 49/2017, de 24 de maio.

face às principais ameaças. Por fim, analisa os aspetos do emprego das FA em complementaridade das FSS, relativamente ao caso português, e remete para as considerações finais do estudo.

1. Considerações sobre o Conceito de Segurança

No mundo de hoje, o conceito de segurança é interpretado em várias dimensões. Com a globalização⁴ e perante a atual sociedade do conhecimento, os Estados soberanos e o indivíduo em si, estão expostos a novos riscos e ameaças, para além das tradicionais manifestações de insegurança e de violência perpetradas ao longo da História. Decorrentes desse contexto, as respostas de segurança passaram a ser multidisciplinares, em diversos setores e sem estanquidades geográficas.

Segundo Barry Buzan, no fim da Guerra Fria, o conceito de segurança começa a sofrer mutações, que o fizeram desprender-se da tradicional associação às questões militares e de política de defesa. Por essa altura, surgem novas perspetivas de entendimento, onde cabem definições de segurança mais alargadas, tais como a de segurança económica e a de segurança ambiental. Estas já não se restringem ao papel do Estado.

A partir dos anos 90 do século XX, juntam-se ao conceito de segurança, também as definições de segurança humana, de segurança societal, segurança energética e de segurança alimentar.

Por consequência, o ideal de segurança atual é concebido pela visão do conceito de segurança humana. No entanto, podendo-se abandonar a conceção mais tradicionalista de Segurança, assente em polos distintos entre a segurança externa e a segurança interna, ou entre os assuntos de defesa e os assuntos de manutenção da ordem pública; é considerado hoje unânime, que se deve entender os fenómenos securitários com o recurso aos conceitos que conseguem operacionalizar essa mesma segurança.

Assim, verifica-se que antes se tinha uma perspetiva tradicionalista, político-militar e que, agora se assiste a uma perspetiva construtivista da segurança (Buzan e Hansen, 2009, p. 4).

A Escola de Copenhaga e o seu núcleo duro, constituído por Barry Buzan e Ole Wæver, foram os grandes impulsionadores do conceito de segurança societal e de securitização (Buzan e Hansen, 2009). O conceito de segurança societal foi lançado inicialmente para responder a uma série de conflitos nacionais que ocorreram na

4 “Anthony Giddens (...) define a globalização “como a intensificação das relações sociais à escala mundial, relações que ligam localidades distantes de tal maneira que as ocorrências locais são moldadas por acontecimentos que [ocorrem] a muitos quilómetros de distância” (Giddens, 1995, p. 52 *apud* Lourenço, 2013, p. 13).

ex-Jugoslávia e na ex-URSS (Buzan e Hansen, 2009). Deste modo, a segurança societal é entendida como sendo:

“A capacidade de uma sociedade permanecer com o seu caráter essencial sob condições variáveis e ameaças possíveis ou reais. (...) A Segurança Societal limitou o possível objeto referente a duas unidades coletivas, Estado e Sociedade, e excluiu o indivíduo e o global.” (Buzan e Hansen, 2009, p. 213)

Segundo Néelson Lourenço (2015), também é importante uma nova visão da segurança, diferente da segurança das fronteiras, com preocupações ao nível das ameaças derivadas do terrorismo transnacional, do crime organizado e centradas na cibersegurança⁵.

“Entende-se por segurança a busca da libertação da ameaça e a capacidade dos Estados e das sociedades para manter a sua identidade independente e a sua integridade funcional contra as forças de mudança que consideram hostis.” (Buzan, 1991, p. 432).

Uma outra dimensão de segurança diz respeito ao conceito preconizado pelas Nações Unidas, designado por segurança humana, em que o referencial teórico deixa de ser só o Estado e passa a ser também o indivíduo (Garcia e Ferro, 2013). O Secretário-Geral das Nações Unidas, Ban Ki-Moon refere em março de 2014 o seguinte:

“O entendimento comum sobre segurança humana, acordado pela Assembleia Geral na resolução 66/290 em setembro de 2012, oferece uma maneira útil de pensar sobre como responder aos desafios do século XXI. (United Nations Human Security Unit, 2014, p. 3)

A segurança humana complementa a Segurança Nacional (SN) em quatro aspetos: na preocupação com o indivíduo e com a comunidade; na identificação de ameaças à segurança das pessoas e às suas condições de vida; na identificação da gama de atores que promovem a segurança, para além do Estado; na proteção das pessoas, mas também na capacidade de as pessoas conseguirem defender-se sozinhas (Commission On Human Security, 2003, p. 4):

“A segurança humana reúne os ‘elementos humanos’ da segurança (...) reconceptualiza a segurança de uma maneira fundamental: (i) afastando-se das conceções de segurança tradicionais, centradas no Estado, que se focam principalmente na segurança dos estados da agressão militar, para um que se concentra na segurança dos indivíduos, na sua proteção e capacitação; (ii) chamar a atenção para uma multiplicidade de ameaças transversais a diferentes aspetos da vida humana e, assim, destacar a ligação entre segurança, desenvolvimento e direitos humanos; e (iii) promover uma nova abordagem integrada, coordenada e centrada nas pessoas para difundir a paz, a

5 “O ciberespaço criou novos bens jurídicos que carecem de proteção, novos tipos de crimes e, ainda, novas formas de realizar crimes antigos”. Conforme a Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, referente à Estratégia Nacional de Segurança do Ciberespaço.

segurança e o desenvolvimento dentro e através das nações.” (United Nations Trust Fund for Human Security, 2009, pp. 5-6)

Com efeito, o conceito de emprego das FA na Segurança deve ser observado à luz das diferentes perspetivas conhecidas e aceites sobre o conceito da Segurança. Nesse sentido, é importante considerar num horizonte nacional, aquando de uma necessária revisão do Conceito Estratégico de Defesa Nacional (CEDN), o enquadramento das FA no conjunto das ações que permitam concretizar os conceitos de Segurança Humana⁶ e os de Segurança Societal (figura 1).

Figura 1 – Friends of Europe: Jam’s top 10 Recommendations



Fonte: *Friends of Europe* [online], disponível em: <http://www.friendsofeurope.org/sites/default/files/media/uploads/2016/05/SECJAM-recommendations1.jpg>

6 “People-centered; Comprehensive; Context-specific; Prevention-oriented; Protection (top-down) and Empowerment (bottom-up)” (United Nations Human Security Unit, 2014).

A segurança, entendida enquanto conceito operacional, permite dar significado à atividade de um conjunto de elementos de um sistema de segurança em concreto. Na realidade nacional, esse conceito compreende a segurança interna, a segurança externa, as Informações da República e a Proteção Civil, as quais devidamente integradas, enformam o conceito de Segurança Nacional⁷.

Figura 2 – Compromisso das FA Portuguesas



Fonte: Estado-Maior-General das Forças Armadas [website] disponível em:
<http://www.emgfa.pt/pt/home/>

A atividade de segurança, ou o produto operacional desses elementos do referido sistema, materializa-se no emprego das FSS, das FA (figura 2), dos Serviços de Informações da República e dos Agentes de Proteção Civil, para que, no cumprimento das suas atribuições e missões distintas, consigam fazer face aos riscos e ameaças que surjam, em sintonia com o quadro legal vigente e respeitando os princípios constitucionais.

7 "Security is facing new challenges. In the past, security threats were assumed to emanate from external sources. State security focused mainly on protecting the state – its boundaries, people, institutions and values – from external attacks" (Commission On Human Security, 2003, p. 5).

Portanto, uma noção de SN⁸ enquadra:

“A condição que se traduz pela garantia de sobrevivência da nação em paz e liberdade, ou seja, a garantia dos interesses nacionais vitais: soberania, independência e unidade, integridade do território” (Ferreira, 2015, p. 35).

Por seu turno,

“A Defesa Nacional tem por objetivo garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas” (Ferreira, 2015, p. 35).

Desta forma o CEDN⁹ prevê que:

“O sistema de segurança interna não deve ser considerado isoladamente, mas antes integrado no sistema mais amplo e abrangente da segurança nacional, que faz apelo aos princípios da complementaridade e da interdependência entre todas as suas componentes” (p. 1992).

Quanto ao conceito de SI, ele está definido no Artigo 1.º, n.º 1, da Lei de SI¹⁰, com a seguinte redação:

“A Segurança Interna é a atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática.”

Neste século, a grande diferença ao nível do conceito, é que se passou da segurança do Estado para a segurança centrada no indivíduo. A definição de segurança em sentido restrito deixou de ter capacidade para explicar o conceito. As fronteiras da segurança alteraram-se, ficou para trás o paradigma realista das fronteiras físicas de um Estado. Os limites são alargados e as fronteiras da segurança não são só os limites geográficos. A segurança é aquilo que se percebe e não tanto as questões consideradas pela defesa e segurança propriamente ditas (Lourenço, 2015).

Noutra perspetiva, a arquitetura de segurança coletiva pode ser entendida em três vertentes: *hard*, *soft* e *smart power*.

8 “Com efeito, o quadro constitucional desvaloriza a utilização formal do termo Segurança Nacional, não adotando o enfoque anglo-saxónico que atribui ao termo ‘Segurança’ o mesmo significado de ‘Defesa Nacional’, numa perspetiva abrangente. Este regime tem motivado algumas críticas oriundas de especialistas em questões de segurança que consideram pertinente a consagração constitucional do termo Segurança Nacional” (Feiteira, 2006, p. 85).

9 Aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril.

10 Lei n.º 53/2008, de 29 de agosto, alterada pela Lei n.º 59/2015, de 24 de junho.

Segundo Nuno Severiano Teixeira (2009, pp. 11, 12 e 15), “A Defesa e a Segurança são instrumentos de uma Estratégia Nacional – são instrumentos decisivos para a existência dos Estados”. O conceito de segurança nos dias de hoje, não se baseia exclusivamente na segurança do Estado e no uso da força.

“A problemática da segurança (...) e da defesa (...) só pode, hoje em dia, ser eficazmente abordada numa perspectiva simultaneamente holística, que vai da segurança individual à da Humanidade, e sistémica, que encara e integra todos os vectores do poder (militar, económico, científico, diplomático, cultural, etc.)” (Couto, 2009, p. 21).

2. As Forças Armadas em Contextos de Segurança

Segundo o documento *Defesa 2020*,¹¹ no atual contexto de segurança, os governantes de Portugal reconhecem que se deve: “Reformular a cadeia operacional das Forças Armadas, de modo a potenciar a capacidade de planeamento e a execução de operações, quer em missões externas, quer em missões no interior do país, previstas na lei”.

De acordo com o CEDN, o Estado deve promover políticas de DN e de segurança no sentido de:

- (a) “Aprofundar a cooperação entre as Forças Armadas e as Forças de Segurança em missões no combate a agressões e às ameaças transnacionais, através de um Plano de Articulação Operacional”;
- (b) “Garantir a capacidade de vigilância e controlo do território nacional”, e a “fiscalização do espaço aéreo e marítimo”;
- (c) “Desenvolver as capacidades militares necessárias à mitigação das consequências de ataques terroristas, cibernéticos, NBQR (Nuclear, Bacteriológico, Químico ou Radiológico) e de catástrofes e calamidades”;
- (d) “Montar a estrutura responsável pela cibersegurança, através da criação dos órgãos técnicos necessários”;

Ao nível da União Europeia, um grupo de reflexão denominado *Friends of Europe* (2016), defende entre vários outros tópicos o seguinte:

“Toda a defesa é segurança, mas nem toda a segurança é defesa. Se quisermos combinar os orçamentos, o *benchmark* deve ser superior a 2%”.¹²

“Esta integração precisa de ser sincronizada e devidamente institucionalizada. As lideranças civil e militar existentes precisam adotar um nível de relacionamento mutuamente benéfico”.¹³

11 Aprovado pela Resolução do Conselho de Ministros n.º 26/2013, de 19 de abril.

12 Sandy Johnston antigo funcionário do Ministério da Defesa britânico, citado em *Friends of Europe* (2016, p. 33).

13 Thierry Balzacq, diretor científico no Institute for Strategic Research (IRSEM) citado em *Friends of Europe* (2016, p. 62).

Não obstante o acima descrito, alguns autores defendem entendimentos menos convergentes com esta visão que se considera integradora. É o caso do exposto acerca da intervenção das FA, em ações junto da população civil:

“Com efeito, os meios necessários para a prevenção e combate das ameaças transnacionais à Segurança Interna, mesmo quando possam ter consequências duras para a sociedade e exijam um acrescido esforço de coordenação, não fazem apelo a uma lógica de guerra, como é o caso do crime organizado e das organizações de tipo máfias, dos actos que cabem na figura de desordem social, do cibercrime ou do terrorismo” (Lourenço, 2015, p. 34).

A linha de pensamento anterior apresenta ainda o argumento de que “o uso da força não é o meio de ação por excelência das polícias”; e que “pelo contrário, o equipamento e armamento militar obedece a um racional de máxima eficácia em termos de alcance, poder de destruição e precisão”, direcionado prioritariamente para a “eliminação física do inimigo” (Lourenço, 2015, pp. 34-35).

Por outro lado, pode-se evidenciar em sentido contrário que “o disposto na LSI, na LOBOFA e na LDN constitui uma extensão (para fazer face às novas ameaças) do disposto na alínea 6) do art.º 275.º da CRP” (Borges, 2013, p. 29).

Nesse sentido, o emprego das FA em território nacional pode apoiar as FSS e “sem prejuízo da sua missão primária de defesa militar da República” (Borges, 2013, p. 29). Segundo o General Pinto Ramalho (2011, p. 110):

“Face aos novos riscos à segurança global e, em particular, numa perspetiva de combate ao terrorismo e ameaças não tradicionais (...), deixaram de existir fronteiras definidas entre a Segurança Interna e externa, o seu carácter é difuso e reconhece-se a indispensabilidade da atuação supletiva das Forças Armadas em muitas situações de carácter interno, onde as Forças de Segurança não dispõem de capacidades adequadas ou se revelaram insuficientes.”

Outros autores (Garcia, 2015, p. 26) consideram por sua vez que as FA “irão, nas próximas décadas, ser empregues na ordem interna”.

3. Enquadramento Jurídico do Emprego das Forças Armadas na Segurança

Em termos constitucionais, denota-se uma distinção entre SI e DN conforme as origens internas ou externas, respetivamente. No entanto, face à complexidade das ameaças atuais, “a perspectiva bipartida parece não responder satisfatoriamente” (Feiteira, 2006, p. 85).

No que respeita à legitimidade de um eventual emprego das FA, terá que ser sempre respeitado o pressuposto aplicado às FSS.¹⁴

14 Apresenta-se aqui um paralelismo possível: “quatro orientações são essenciais: assegurar o reconhecimento por parte dos cidadãos da legitimidade da ação policial e simultaneamente conseguir um elevado nível de confiança dos indivíduos e das comunidades nas polícias;

Da pesquisa efetuada verifica-se que o Chefe do Estado-Maior-General das FA, atualmente tem assento no Conselho Superior de Defesa Nacional¹⁵, no Conselho Superior de Informações¹⁶ e no Conselho Superior de Segurança Interna¹⁷.

Relativamente à Unidade de Coordenação Antiterrorismo (UCAT), as FA podem ser representadas nos seguintes termos: “a convite do Secretário-Geral do Sistema de Segurança Interna, conforme as matérias a tratar, podem participar em reuniões da UCAT representantes das seguintes entidades: a) Chefe do Estado-Maior-General das Forças Armadas”¹⁸.

A segurança coletiva é uma tarefa fundamental do Estado. A segurança é por um lado, um direito individual e, por outro, um dever do Estado.

A tabela seguinte mostra as referências à legislação portuguesa, pesquisadas durante a presente investigação, onde consta o papel ativo das FA em contextos de segurança.

A Constituição da República Portuguesa (CRP), fixa o regime da DN no Artigo 273.º, e das FSS no Artigo 272.º:

Tabela 1 – Legislação Portuguesa com Referência às Forças Armadas na Segurança

Lei Constitucional n.º 1/2005 de 12 de agosto (CRP)	
Artigo 273.º (Defesa Nacional)	É obrigação do Estado assegurar a Defesa Nacional. A Defesa Nacional tem por objetivos garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas.
Artigo 272.º (Polícia)	A polícia tem por funções defender a legalidade democrática e garantir a Segurança Interna e os direitos dos cidadãos.
Lei de Segurança Interna – Lei n.º 53/2008 de 29 de agosto Artigo 35.º Forças Armadas	
As Forças Armadas colaboram em matéria de Segurança Interna nos termos da Constituição e da lei, competindo ao Secretário-Geral do Sistema de Segurança Interna e ao Chefe do Estado-Maior-General das Forças Armadas assegurarem entre si a articulação operacional.	

aumentar a eficiência da ação das polícias; diminuir o sentimento de insegurança e o medo do crime; aumentar a eficiência da justiça contribuindo para a confiança no sistema judicial e para a diminuição da perceção de impunidade” (Lourenço, 2012, p. 192).

15 Lei Orgânica n.º 1-B/2009, de 7 de julho, Lei de Defesa Nacional.

16 Lei n.º 30/84, de 5 de setembro, alterada pela Lei Orgânica n.º 4/2014, de 13 de agosto, Lei Quadro do Sistema de Informações da República Portuguesa.

17 Lei n.º 53/2008, de 29 de agosto alterada pela Lei n.º 59/2015, de 24 de junho, Lei de Segurança Interna.

18 Decreto Regulamentar n.º 2/2016 de 23 de agosto, Organização e Funcionamento da Unidade de Coordenação Antiterrorismo.

Lei de Defesa Nacional – Lei Orgânica n.º 5/2014 de 29 de agosto

Artigo 5.º Objetivos permanentes da política de Defesa Nacional

b) A liberdade e a segurança das populações, bem como os seus bens e a proteção do património nacional;

Artigo 10.º Comandante Supremo das Forças Armadas

c) Direito de ser previamente informado pelo Governo, através de comunicação fundamentada, sobre o emprego das Forças Armadas em missões que envolvam a colaboração com as Forças de Segurança contra agressões ou ameaças transnacionais;

Artigo 24.º Missões das Forças Armadas

1 – Nos termos da Constituição e da lei, incumbe às Forças Armadas:

a) Desempenhar todas as missões militares necessárias para garantir a soberania, a independência nacional e a integridade territorial do Estado;

e) Cooperar com as Forças de Segurança tendo em vista o cumprimento conjugado das respetivas missões no combate a agressões ou ameaças transnacionais;

f) Colaborar em missões de proteção civil e em tarefas relacionadas com a satisfação das necessidades básicas e a melhoria da qualidade de vida das populações.

2 – As Forças Armadas podem ser empregues, nos termos da Constituição e da lei, quando se verifique o estado de sítio ou de emergência.

Lei Orgânica de Bases da Organização das Forças Armadas – Lei Orgânica n.º 6/2014 de 1 de setembro

Artigo 26.º Articulação operacional entre as Forças Armadas e as Forças de Segurança

1 – As Forças Armadas e as Forças de Segurança cooperam tendo em vista o cumprimento conjugado das suas missões para os efeitos previstos na alínea e) do n.º 1 do artigo 4.º.

2 – Para assegurar a cooperação prevista no número anterior, são estabelecidos os procedimentos que garantam a interoperabilidade de equipamentos e sistemas, bem como a utilização de meios.

3 – Compete ao Chefe do Estado-Maior-General das Forças Armadas e ao Secretário-Geral do Sistema de Segurança Interna assegurar entre si a implementação das medidas de coordenação, para os efeitos previstos nos números anteriores, sem prejuízo do disposto na Lei de Segurança Interna.

Segundo o Relatório Anual de Segurança Interna (RASI) de 2016, o Estado-Maior-General das FA (EMGFA), no âmbito da partilha de informações, manteve ligações com os Órgãos de Polícia Criminal (OPC) no quadro das atividades necessárias à avaliação das ameaças à Segurança militar (Sistema de Segurança Interna, 2016, p. 179).

Autoridade Aeronáutica Nacional (AAN) – Lei n.º 28/2013 de 12 de abril

Artigo 3.º Autoridade Aeronáutica Nacional

O Chefe do Estado-Maior da Força Aérea é, por inerência, a AAN e, nesta qualidade funcional, depende do Ministro da Defesa Nacional.

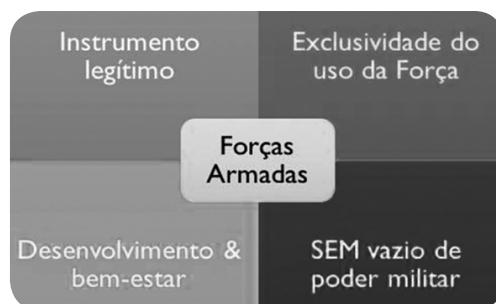
Segundo o RASI de 2016, no que diz respeito ao combate à criminalidade e ao tráfico internacional de estupefacientes, a Força Aérea “efetou 278:05 HV” [horas de voo] dedicadas a este tipo de ameaça (Sistema de Segurança Interna, 2016, p. 182).

<p>Polícia Marítima (PM) – Decreto-Lei n.º 235/2012 de 31 de outubro Artigo 1.º</p> <p>2 – A PM é uma força policial armada e uniformizada, dotada de competência especializada nas áreas e matérias legalmente atribuídas ao SAM e à AMN, composta por militares da Armada e agentes militarizados.</p> <p>Segundo o RASI de 2016, no âmbito do combate ao narcotráfico, foram efetuadas três operações militares em colaboração com a Polícia Judiciária (Sistema de Segurança Interna, 2016, p. 181).</p>
<p>Polícia Judiciária Militar (PJM) – Lei n.º 97-A/2009 de 3 de setembro Artigo 2.º Natureza</p> <p>A PJM, corpo superior de polícia criminal auxiliar da administração da justiça, organizado hierarquicamente na dependência do membro do Governo responsável pela área da Defesa Nacional e fiscalizado nos termos da lei, é um serviço central da administração directa do Estado, dotado de autonomia administrativa.</p> <p>De notar que a PJM, composta por elementos militares das FA, segundo o RASI de 2016, é um dos oito Órgãos de Polícia Criminal do Sistema de Segurança Interna que fornece a este, dados da criminalidade participada por si investigada. (Sistema de Segurança Interna, 2016, p. 24)</p>

4. Missões e Finalidade das Forças Armadas¹⁹

Às FA compete a exclusividade do uso da força na gestão organizada da violência. Enquanto componente essencial do poder, as FA quando em conflito, apenas devem desempenhar as seguintes missões: melhorar ou conter uma situação; compelir comportamentos; desorganizar estruturas ou destruir; e impor uma situação (Garcia, 2015). No entanto, as FA têm uma finalidade pública que ultrapassa a exclusividade do uso da força, nomeadamente a promoção da Segurança e o desenvolvimento e bem-estar da sociedade (figura 3).

Figura 3 – Referências sobre a Finalidade das FA



Fonte: elaborado a partir de Garcia (2015).

¹⁹ As Missões das Forças Armadas decorrem do Conceito Estratégico Militar (CEM) 2014.

Para o tema em estudo, importa referir as seguintes missões das FA:

- Defesa convencional do território nacional;
- Ciberdefesa;
- Cooperação com as Forças de Segurança;
- Vigilância e controlo, incluindo a fiscalização e o policiamento aéreo, dos espaços sob soberania e jurisdição nacional.

5. Capacidades das Forças Armadas

Conforme o CEDN: “É importante maximizar as práticas de duplo uso e de partilha de recursos, bem como eliminar todas e quaisquer formas de duplicação de meios públicos”. De destacar para o tema em estudo, são os meios necessários às capacidades seguintes das FA: “capacidade nas áreas de comando, controlo, comunicações e informações; capacidade de ciberdefesa; capacidades de vigilância e controlo dos espaços aéreo e marítimo à nossa responsabilidade; e capacidades indispensáveis para fazer face às consequências de ataques terroristas, NBQR e de catástrofes e calamidades”.

Com o documento *Defesa 2020*²⁰, o Estado português afirmou a necessidade de constituir nas FA, três conjuntos de forças e meios, com a seguinte ordem de prioridade: uma “Força de Reação Imediata”, um conjunto de “Forças Permanentes em Ação de Soberania” e um “Conjunto Modular de Forças”.

Destaca-se aqui, o conjunto de Forças Permanentes em Ação de Soberania, que de acordo com esse documento estão:

“Orientadas para missões, designadamente, de defesa aérea, patrulhamento, vigilância e fiscalização marítima e aérea, e quando determinado, vigilância terrestre, busca e salvamento, defesa Nuclear Biológica Química e Radiológica (NBQR), de interesse público e de resposta a catástrofes, em continuidade no território nacional e nas áreas de jurisdição ou responsabilidade nacional” (p. 9).

Destacam-se também as seguintes capacidades das FA:

- (a) Armada – “garantir, simultânea e continuamente, o controlo e vigilância do espaço marítimo sob responsabilidade e jurisdição nacional, as missões de interesse público e as atribuições cometidas à Armada no âmbito do Sistema de Autoridade Marítima”;
- (b) Exército – “continuadamente cumprir missões no âmbito da segurança e defesa do território e da população e do apoio militar de emergência”;
- (c) Força Aérea – “Garantir, simultânea e continuamente, a vigilância e controlo do espaço aéreo (...) fiscalização e intervenção nos espaços de soberania sob responsabilidade e jurisdição nacional, bem como missões de interesse

²⁰ Aprovado pela Resolução do Conselho de Ministros n.º 26/2013, de 11 de abril.

público e a execução das ações cometidas no âmbito do Sistema de Autoridade Aeronáutica”.

Decorrente da participação das FA nas Operações de Apoio à Paz, em vários teatros de operações internacionais, nos últimos anos, houve uma mudança na postura do militar. “Este, nestas operações, deixa de ser o ‘combatente’ (*warrior*) para passar a ser o “construtor da paz” (*peacekeeper*), o que leva à necessidade de controlo da sua agressividade e à assunção de um comportamento disciplinado e isento” (Sousa, 2011, p. 292).

“Nestas missões e teatros, muitas vezes, os militares, mesmo os de baixa patente, têm de tomar decisões que podem colocar em causa o nome do País que servem, o que tem exigido um esforço acrescido da Instituição na formação dos seus elementos, que lhes dê a capacidade para discernir quais os resultados das suas atitudes e as repercussões que delas podem resultar, não só para a sua pessoa, mas, em especial, para o País que representa.” (Sousa, 2011, p. 293).

Segundo o General Loureiro dos Santos (2016, p. 158), as FA têm “condições para suplementar a ação das Forças de Segurança, quando for necessário o emprego de capacidades de que só elas dispõem.” Com a existência das FA em permanência e operacionais, dotadas dos meios necessários aos fins a que se destinam, o Estado permite que os cidadãos e as instituições possam confiar nas capacidades das FA, que “em última instância, garantirá a lei e a ordem,” a estabilidade democrática e a paz.

6. Identificação das Principais Ameaças

No presente artigo foram consideradas as principais ameaças à segurança onde se prevê uma possível intervenção das FA “no espaço sujeito aos poderes de jurisdição do Estado português”. Com esse intuito, tendo em conta os critérios de legitimidade de emprego das FA na segurança, as ameaças previstas no CEDN, entre outras, são a referência essencial:

- (a) Ciberterrorismo e a cibercriminalidade;²¹
- (b) Crimes estritamente militares e crimes comuns ocorridos no interior das FA
- (c) Criminalidade transnacional organizada;
- (d) Espionagem;
- (e) Pirataria²², na Zona Económica Exclusiva;

21 “Os ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (...) podem fazer colapsar a estrutura tecnológica de uma organização social moderna”. Ver nota 9.

22 “Não só pela dependência energética e alimentar e pela importância do transporte marítimo para a economia nacional, mas também pelas crescentes responsabilidades nacionais na segurança cooperativa dos recursos globais”. Ver nota 9.

- (f) Proliferação de armas de destruição massiva;²³
- (g) Sabotagem;
- (h) Subversão;²⁴
- (i) Terrorismo transnacional.²⁵

Numa perspetiva mais tradicionalista, pode-se entender o termo ameaça, como sendo “qualquer acontecimento ou ação – em curso ou previsível – que contraria a consecução de um objetivo e que, normalmente, é causador de danos materiais ou morais” (Couto, 1987, p. 329 *apud* Feiteira, 2006).

Num contexto sociológico, o termo ameaça pode configurar o seguinte:

“Probabilidade de ocorrência de um evento que, num determinado contexto, tem potencial de gerar risco; enquanto risco, corresponde à probabilidade de danos – mortes, ferimentos, destruição de bens materiais, diminuição de rendimento, ruptura da actividade económica ou degradação ambiental – em resultado da ocorrência de um determinado evento num determinado contexto” (Lourenço, 2013, p. 19).

De acordo com as Nações Unidas, o termo ameaça é reconhecido como:

“Qualquer acontecimento ou processo que possa levar a um grande número de mortes ou à diminuição das probabilidades de vida ou ponha em causa o Estado como unidade basilar do sistema internacional pode ser considerada uma ameaça à segurança internacional” (Garcia e Ferro, 2013, p. 40).

Para Barry Buzan, o termo ameaça comporta cinco tipos: militar, político, societal, económico e ecológico (Buzan, 1991 *apud* Garcia e Ferro, 2013, p. 40).

7. Análise do Conceito de Emprego das Forças Armadas na Segurança

O método de análise de conteúdo integra um conjunto de critérios de legitimidade, que por sua vez, constituem os componentes do conceito de emprego legítimo das FA na Segurança Interna. Para os componentes do conceito foram definidos os seguintes indicadores:

Critério jurídico:

- (a) legislação nacional em vigor;

23 “Na medida em que tal leve à sua eventual posse por grupos terroristas ou resulte em crises sérias na segurança regional de áreas vitais”. Ver nota 9.

24 “Acontecimentos de subversão e delinquência grupal, como por exemplo os incidentes ocorridos em França, em 2006 e os recentes incidentes, em S. Paulo, no Brasil, podem configurar-se, em consequência da sua dimensão, traduzida em ações violentas generalizadas, apesar de territorialmente circunscritas, como uma ameaça que se enquadraria no âmbito da noção de Defesa Nacional, equiparada ao conceito de Segurança Nacional” (Feiteira, 2006, p. 88).

25 “Existe entre os académicos um razoável entendimento sobre alguns traços nucleares do terrorismo. A violência ou a ameaça de violência estão sempre presentes. O terrorismo procura criar um clima de medo, obter efeitos psicológicos para além das vítimas directas. O terrorismo persegue objetivos políticos” (Pereira, 2016, p. 54).

- (b) normas e regulamentos militares;
- (c) opções políticas de DN e de SI.

Critério operacional:

- (d) existência de exercícios de treino e formação;
- (e) existência de operações das FA levadas a cabo em apoio das FSS;
- (f) capacidades e competências existentes nas FA;
- (g) presença institucional de elementos das FA²⁶.

Critério social e securitário:

- (h) avaliação da ameaça;
- (i) contexto social de insegurança;
- (j) falta de determinados meios nas FSS²⁷.

Relativamente à confirmação da hipótese “quanto mais os critérios de legitimidade se verificam perante uma determinada ameaça à segurança, mais se torna legítimo o emprego da FA, e vice-versa”, recorreu-se a uma matriz de análise estruturada (Heuer e Pherson, 2011, pp. 59-63).

As FA sendo parte do Estado, devem seguir os mesmos princípios de legitimidade previstos para as FSS, numa eventual atuação em complementaridade, para alcançar a paz social e a manutenção da ordem pública. Conforme afirma Nelson Lourenço (2012, p. 188):

“O Estado deve demonstrar a capacidade de prevenir e combater a criminalidade e a insegurança subjectiva no quadro do respeito dos direitos fundamentais sob pena de perder a sua legitimidade e as suas instituições a confiança que os indivíduos nele depositam.”

Na tabela seguinte apresenta-se o modelo de verificação dos critérios de legitimidade de emprego das FA perante uma dada ameaça que possa ocorrer.

Tabela 2 – Critérios de Legitimidade

Verificação dos critérios de legitimidade SIM=1 NÃO=0	Ameaças ²⁸				
	I	II	III	IV	V
Jurídico – J	SIM	SIM	SIM	SIM	NÃO
Social e securitário – S	SIM	SIM	NÃO	NÃO	NÃO
Operacional – O	SIM	NÃO	SIM	NÃO	NÃO

Fonte: elaborada pelo autor a partir de Quivy e Campenhoudt (2013, p. 264).

²⁶ Consideram-se as estruturas de Segurança tuteladas pela DN.

²⁷ Consideram-se os necessários para responder contra eventuais ameaças à Segurança.

²⁸ Para cada grupo de ameaças levantado em determinado cenário, de entre as acima vistas em “Identificação das principais ameaças”, são verificados os critérios de legitimidade que estão presentes.

Na tabela seguinte consta a atribuição de pesos a cada critério de legitimidade, necessária para validar o modelo teórico, em ordem ao grau de importância dado a cada um deles, para legitimar o emprego das FA na Segurança, (e.g. o critério jurídico em relação ao critério social e securitário, pesa duas vezes mais):

Tabela 3 – Ordem de Importância dos Critérios de Legitimidade

Critérios de legitimidade	J	S	O	PESO 100% = 10		
jurídico – J		J	J	2J	67%	6
social e securitário – S			S	1S	33%	3
operacional – O				0O	0%	1

Fonte: elaborada pelo autor a partir de *Paired Comparasion Matrix* (Heuer e Pherson, 2011, p. 61).

A partir da matriz de análise estruturada abaixo, formulou-se o seguinte:

- Quando os três critérios considerados se verificam – é completamente legítimo o emprego das FA na segurança interna;
- Quando o critério jurídico e outro se verificam – em caso de necessidade, é legítimo e razoável o emprego das FA na segurança interna;
- Quando só o critério jurídico se verifica – em circunstâncias específicas é legítimo e pontual o emprego das FA na segurança interna;
- Quando nenhum dos critérios considerados se verifica – não é legítimo e é nulo o emprego das FA na segurança interna.

Como limite superior nesta escala de legitimidade, consideram-se as circunstâncias previstas no “regime do estado de sítio e do estado de emergência”, as quais não vão ser aqui tratadas por se entender que não carecem deste tipo de análise.²⁹

²⁹ *Vd.* Artigos 8.º e 9.º, da Lei n.º 44/86, de 30 de setembro, alterada pela Lei Orgânica n.º 1/2012, de 11 de maio: “Artigo 8.º (...) Estado de sítio (...) 1 – O estado de sítio é declarado quando se verifiquem ou estejam iminentes atos de força ou insurreição que ponham em causa a soberania, a independência, a integridade territorial ou a ordem constitucional democrática e não possam ser eliminados pelos meios normais previstos na Constituição e na lei. (...) 2 – Nos termos da declaração do estado de sítio será total ou parcialmente suspenso ou restringido o exercício de direitos, liberdades e garantias, sem prejuízo do disposto no artigo 2.º, e estabelecida a subordinação das autoridades civis às autoridades militares ou a sua substituição por estas. (...) 3 – As Forças de Segurança, durante o estado de sítio, ficarão colocadas, para efeitos operacionais, sob o comando do Chefe do Estado-Maior-General das Forças Armadas, por intermédio dos respetivos comandantes-gerais. (...) Artigo 9.º (...) Estado de emergência (...) 1 – O estado de emergência é declarado quando se verifiquem situações de menor gravidade, nomeadamente quando se verifiquem ou ameacem verificar-se casos de calamidade pública. (...) 2 – Na declaração do estado de emergência apenas pode ser determinada a suspensão parcial do exercício de direitos, liberdades e garantias, sem prejuízo do disposto no artigo 2.º, prevendo-se, se necessário, o reforço dos poderes das autoridades administrativas civis e o apoio às mesmas por parte das Forças Armadas.”

Tabela 4 – Matriz de Análise Estruturada para o Emprego das FA na Segurança

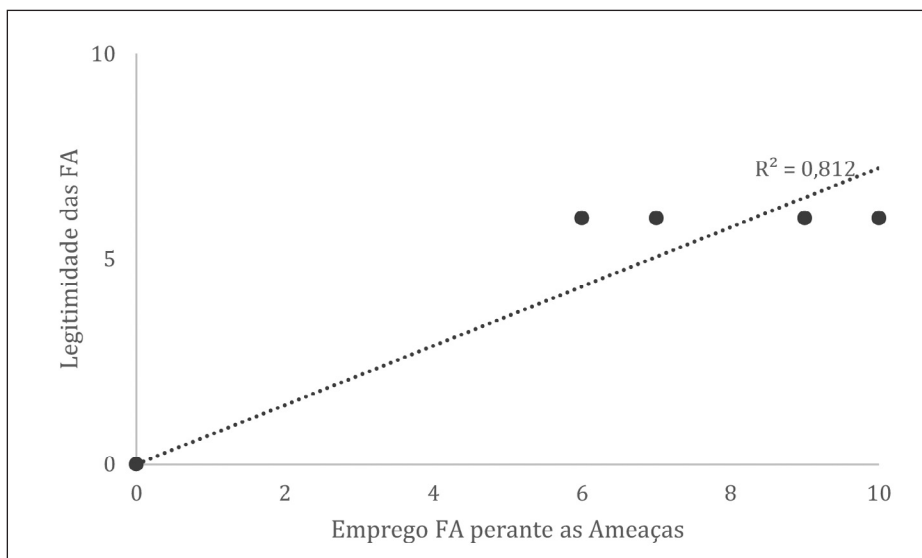
Critérios de legitimidade	Peso	ameaça I	ameaça II	ameaça III	ameaça IV	ameaça V
jurídico – J	6	6	6	6	6	0
social e securitário – S	3	3	3	0	0	0
operacional – O	1	1	0	1	0	0
total	10	10	9	7	6	0
percentagem	100%	31%	28%	22%	19%	0

Coefficiente de correlação (r) = 0,914

Fonte: elaborada pelo autor a partir de *Weighted Ranking Matrix* (Heuer e Pherson, 2011, p. 63).

Na matriz acima estão registados os dados que se obtiveram para determinar em que circunstâncias é legítimo o emprego das FA perante uma dada ameaça. Do conjunto de ameaças identificadas, aquelas que ocorram em circunstâncias prováveis do parâmetro I, o emprego das FA tem um índice de legitimidade de 31%; no parâmetro II, 28%; no parâmetro III, 22%; no parâmetro IV, 19%; sendo o índice de legitimidade 0% para as ameaças que ocorram em circunstâncias onde não se verificam qualquer dos critérios de legitimidade.

Gráfico 1 – Relações no Modelo de Análise

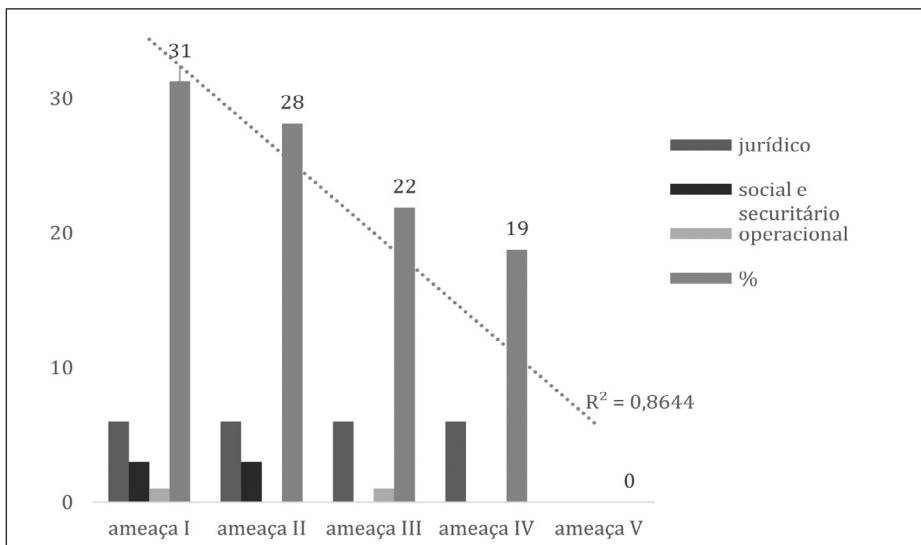


Fonte: elaborado pelo autor a partir de Quivy e Campenhoudt (2013, p. 270).

No gráfico acima pode-se observar uma relação entre as variáveis do modelo e o índice de legitimidade das FA, bem como a reta de regressão e o valor de $R^2=0,812$

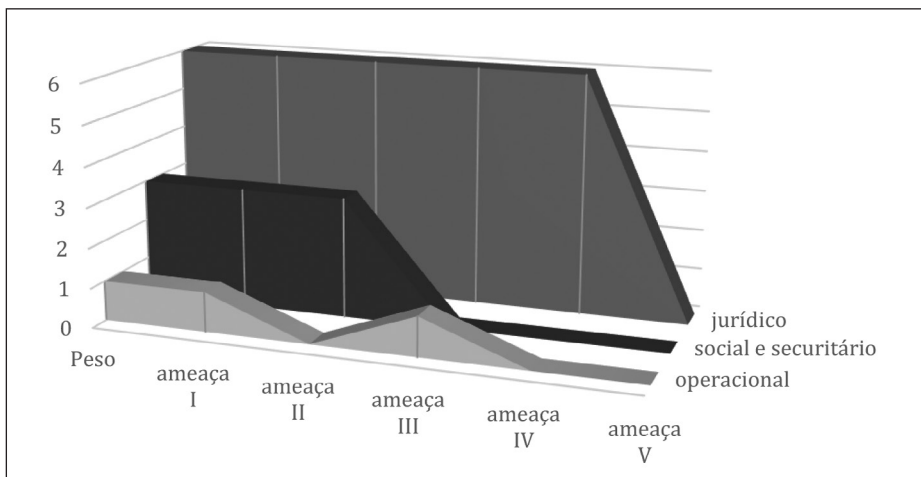
onde se demonstra a variação do índice de legitimidade, ($y > 5$ emprego legítimo; $y < 5$ emprego não legítimo), mediante a confirmação da presença dos critérios numa dada ameaça. Os pontos representam cada uma das ameaças tipo.

Gráfico 2 – Emprego das FA na Segurança, por Ameaças à Segurança



Fonte: elaborado pelo autor.

Gráfico 3 – Peso dos Critérios de Legitimidade por Ameaças à Segurança



Fonte: elaborado pelo autor.

No gráfico 2 acima representado, pode-se constatar que, em circunstâncias prováveis de ameaça I e II, o peso é maior, devido à necessidade de apoio e complementaridade às FSS, independentemente de, em II, não se verificar nas FA o critério operacional em pleno. Já no caso de circunstâncias prováveis de ameaça III, só se verificará esse apoio, quando ocorra um fenómeno de tal modo imprevisível e novo, que leva à confirmação de falta nas FSS, do critério social e securitário – por exemplo, num contexto social de insegurança muito grave, ou devido à falta de um meio nas FSS, necessário para responder contra a ameaça.

No mundo multipolar em que hoje se vive, assiste-se a uma escalada da violência nas sociedades modernas, motivada pelas mais variadas razões. Os conflitos atuais têm origem difusa, podem provocar danos em vários locais do mundo, em simultâneo e constituir ameaças em diferentes dimensões.

O emprego das FA justifica-se principalmente face a ameaças transnacionais à segurança, tais como o terrorismo transnacional, o crime transnacional organizado, os ciberataques e a proliferação de armas de destruição massiva.

Sobre a ameaça do terrorismo transnacional, convém referir que:

- (a) “Só da União Europeia terão partido, até meados de 2015, mais de 6000 jihadistas para se juntarem ao EI na Síria e no Iraque” (Tomé, 2015, p. 139).
- (b) “por muito chocantes que sejam as suas manifestações, o terrorismo obedece geralmente a uma racionalidade política” (Couto, 2009, p. 45).
- (c) “Por outro lado, há o risco crescente da chamada “proliferação não-estatal”, [armas de destruição massiva] por grupos terroristas, seitas fanáticas ou organizações de banditismo, capazes de lançarem o terror ou o pânico em grandes centros urbanos” (Couto, 2009, p. 45).

As FA têm uma grande responsabilidade na contribuição para a segurança em Portugal. A par das responsabilidades inerentes a DN cabe às FA um papel importante, no plano estratégico e operacional que é delineado para as questões de segurança. Segundo o general Loureiro dos Santos (2016, pp. 157-158), o papel das FA “não se limita à defesa militar do Estado face a ameaças que se perfilam contra ele, (...) Elas constituem também a garantia última da autoridade do Estado”.

O Estado português, relativamente à SI, reconhece a intervenção das FA no quotidiano das populações portuguesas, sendo que os princípios orientadores da proporcionalidade, legalidade e mínimo uso da força, para evitar danos colaterais, estão assegurados. O emprego das FA na segurança pressupõe, acima de tudo, um carácter de complementaridade, de uma forma supletiva, mediante as necessidades de apoio das FSS. Aquelas Forças são capazes de produzir segurança e defesa, de acordo com as decisões do poder político.

A capacidade de emprego operacional e flexível das FA garante aos Estados condições de segurança, a prossecução dos seus interesses estratégicos, a afirmação de soberania e o desenvolvimento e bem-estar da sociedade.

Considerações Finais

O artigo confirma a hipótese formulada na sua introdução. O ideal de segurança é hoje concebido pela visão do conceito de segurança humana e complementa a SN.

O conceito de emprego das FA na segurança interna deve ser observado à luz de diferentes perspetivas sobre o conceito da segurança.

Os critérios de legitimidade – jurídico, operacional, social e securitário – permitem verificar a legitimidade do emprego das FA na segurança interna. Deste modo, quando nenhum dos critérios considerados tem peso na avaliação da provável ameaça, não é legítimo o seu emprego.

O emprego das FA na segurança interna justifica-se especialmente face a ameaças transnacionais à SN, tais como o terrorismo transnacional, o crime transnacional organizado, os ciberataques e a proliferação de armas de destruição massiva.

A ideia de uma arquitetura comum de segurança vislumbra-se no curto prazo, tendo em conta a atualidade da figura do Chefe do Estado-Maior-General das FA, uma vez que a legislação prevê a sua presença nos principais conselhos superiores dedicados à segurança e defesa, inclusivamente, por representação na Unidade de Coordenação Antiterrorismo.

Os meios de duplo uso das FA são uma mais-valia para todos os intervenientes.

O tema do emprego das FA na Segurança, particularmente em contextos de SI, está longe de obter perceções unânimes. Porém, a presente investigação procurou estabelecer os pontos de convergência e apresentar argumentos para um debate de ideias salutar sobre o assunto.

Assim, considera-se o presente texto como um elemento de investigação válido para aprofundar o conhecimento sobre o emprego das FA em contextos de segurança interna. E nesse sentido, propõe-se uma pesquisa futura acerca de uma estratégia comum para as FA e as FSS no âmbito da Segurança e Defesa em Portugal.

Referências

- Borges, J. V., 2013. As Forças Armadas na Segurança Interna: Mitos e Realidades. *Revista Militar*, N.º 2532, pp. 25-41.
- Buzan, B. e Hansen, L., 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.
- Buzan, B., 1991. New Patterns of Global Security in the Twenty-First Century. *International Affairs*, 67(3), pp. 431-451.
- Commission On Human Security, 2003. *Human security now*. New York: Commission on Human Security.
- Couto, A. C., 2009. Que Visão para a Defesa? Portugal-Europa-NATO. *Nação e Defesa*, N.º 124, pp. 19-86.

- Decreto Regulamentar n.º 2/2016, de 23 de agosto. Estabelece o regime aplicável à organização e funcionamento da Unidade de Coordenação Antiterrorismo. *Diário da República*, 1.ª série, N.º 161, 23 de agosto de 2016.
- Decreto-Lei n.º 121/2014, de 7 de agosto. Procede à segunda alteração o Decreto-Lei n.º 44/2002, de 2 de março, e ao Decreto-Lei n.º 135/2009, de 3 de junho, com o objetivo de clarificar e regulamentar, respetivamente, as competências do capitão de porto, e os termos em que é Série-A, N.º 52 admissível o funcionamento das concessões balneares e respetivos serviços complementares e ou acessórios, fora da época balnear. *Diário da República*, 1.ª série, N.º 151, 7 de agosto de 2014.
- Decreto-Lei n.º 235/2012, de 31 de outubro. Procede à segunda alteração ao Decreto-Lei n.º 248/95, de 21 de setembro, que cria, na estrutura do Sistema da Autoridade Marítima, a Polícia Marítima, e à primeira alteração ao Decreto-Lei n.º 44/2002, de 2 de março, que estabelece, no âmbito do Sistema da Autoridade Marítima, a estrutura, organização, funcionamento e competências da Autoridade Marítima Nacional. *Diário da República*, 1.ª série, N.º 211, 31 de outubro de 2012.
- Decreto-Lei n.º 248/95, de 21 de setembro. Cria, na estrutura do Sistema da Autoridade Marítima, a Polícia Marítima. *Diário da República*, I Série-A, N.º 219, 21 de setembro de 1995.
- Decreto-Lei n.º 3/2012, de 16 de janeiro. Aprova a orgânica do Gabinete Nacional de Segurança. *Diário da República*, 1.ª série, N.º 11, 16 de janeiro de 2012.
- Decreto-Lei n.º 44/2002, de 2 de março. Estabelece, no âmbito do sistema da autoridade marítima, as atribuições, a estrutura e a organização da autoridade marítima nacional e cria a Direção-Geral da Autoridade Marítima. *Diário da República*, I, 2 de março de 2002.
- Decreto-Lei n.º 49/2017, de 24 de maio. Cria, no âmbito do Sistema de Segurança Interna, na dependência e sob coordenação da/o Secretária/o Geral do Sistema de Segurança Interna, o Ponto Único de Contacto para a Cooperação Policial Internacional (PUC –CPI), procedendo à segunda alteração à Lei n.º 53/2008, de 29 de agosto, alterada pela Lei n.º 59/2015, de 24 de junho. *Diário da República*, 1.ª série, N.º 100, 24 de maio de 2017.
- Decreto-Lei n.º 69/2014, de 9 de maio. Procede à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, que aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança. *Diário da República*, 1.ª série, N.º 89, 9 de maio de 2014.
- Decreto-Lei n.º 9/2012, de 18 de janeiro. Aprova a orgânica da Polícia Judiciária Militar. *Diário da República*, 1.ª série, N.º 13, 18 de janeiro de 2012.
- Feiteira, A., 2006. Segurança e defesa: um domínio único? *Segurança e Defesa*, n.º 1, pp. 81-88.
- Ferreira, J. B., 2015. A importância constitucional dada ao vector da Defesa Nacional como pilar fundamental do Estado. *A Instituição Militar*. *Revista Militar*, n.º 2556, pp. 33-78.
- Friends of Europe, 2016. *2016 Security Jam: Beyond Conventional Security Challenges*. Report of the global online brainstorming, junho. Bruxelas: Friends of Europe. Disponível em: https://www.sipri.org/sites/default/files/SECJAM_REPORT_full_report_HIRES.pdf

- Garcia, F. P., 2015. O Instrumento Militar e as Forças Armadas. *Revista Militar*, n.º 2556, pp. 17-32.
- Garcia, F. P. e Ferro, M., 2013. A Crise do Estado e a Segurança Internacional. *Revista de Direito e Segurança*, N.º 1, pp. 37-61.
- Heuer, R. J. e Pherson, R. H., 2011. *Structured analytic techniques for intelligence analysis*. Washington: Cq Press.
- Lei Constitucional n.º 1/2005, de 12 de agosto. Sétima revisão constitucional. *Diário da República*, I Série-A, N.º 155, 12 de agosto de 2005.
- Lei n.º 28/2013, de 12 de abril. Define as Competências, a Estrutura e o Funcionamento da Autoridade Aeronáutica Nacional. *Diário da República*, 1.ª série, N.º 72, 12 de abril de 2013.
- Lei n.º 30/84, de 5 de setembro. Lei Quadro do Sistema de Informações da República Portuguesa. *Diário da República*, I Série, N.º 206, 5 de setembro de 1984.
- Lei n.º 44/86, de 30 de setembro. Regime do estado de sítio e do estado de emergência. *Diário da República*, I Série, N.º 225, 30 de setembro de 1986.
- Lei n.º 53/2008, de 29 de agosto. Aprova a Lei de Segurança Interna. *Diário da República*, 1.ª série, N.º 167, 29 de agosto de 2008.
- Lei n.º 59/2015, de 24 de junho. Primeira alteração à Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna, modificando a composição do Conselho Superior de Segurança Interna e a organização e o funcionamento da Unidade de Coordenação Anti-terrorismo. *Diário da República*, 1.ª série, N.º 121, 24 de junho de 2015.
- Lei n.º 97-A/2009, de 3 de setembro. Define a natureza, a missão e as atribuições da Polícia Judiciária Militar, bem como os princípios e competências que enquadram a sua ação enquanto corpo superior de polícia criminal auxiliar da administração da justiça. *Diário da República*, 1.ª série, N.º 171, 3 de setembro de 2009.
- Lei Orgânica n.º 1/2012, de 11 de maio. Segunda alteração à Lei n.º 44/86, de 30 de setembro (Regime do estado de sítio e do estado de emergência). *Diário da República*, 1.ª série, N.º 92, 11 de maio de 2012.
- Lei Orgânica n.º 1-A/2009, de 7 de julho. Aprova a Lei Orgânica de Bases da Organização das Forças Armadas. *Diário da República*, 1.ª série, N.º 129, 7 de julho de 2009.
- Lei Orgânica n.º 1-B/2009, de 7 de julho. Aprova a Lei de Defesa Nacional (publicada pela Declaração de Retificação n.º 52/2009, de 20 de julho). *Diário da República*, 1.ª série, N.º 138, 20 de julho de 2009.
- Lei Orgânica n.º 4/2014, de 13 de agosto. Quinta alteração à Lei n.º 30/84, de 5 de setembro, que aprova a Lei Quadro do Sistema de Informações da República Portuguesa. *Diário da República*, 1.ª série, N.º 155, 13 de agosto de 2014.
- Lourenço, N., 2015. As novas fronteiras da Segurança. *Segurança e Defesa*, N.º 31, pp. 26-37.
- Lourenço, N., 2013. Globalização e insegurança urbana. *Revista Angolana de Sociologia*, N.º 11, pp. 11-34.

- Lourenço, N., 2012. Legitimidade e confiança nas polícias. *Revista do Ministério Público*, 129, pp. 181-198.
- Ministério Público, 2016. *Legislação Documentação – Pesquisar*. [Online] Available at: <http://www.ministeriopublico.pt/iframe/pesquisar> [Acedido em 30 de maio de 2016].
- Pereira, J., 2016. Terrorismo Transnacional. Em: João Vieira Borges e Teresa Ferreira Rodrigues, coord., *Ameaças e Riscos Transnacionais no novo Mundo Global*. Porto: Fronteira do Caos, pp. 51-69.
- Quivy, R. e Campenhoudt, L. V., 2013. *Manual de Investigação em Ciências Sociais*, 6.ª Edição. Lisboa: Gradiva.
- Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril. Aprova o Conceito Estratégico de Defesa Nacional. *Diário da República*, 1.ª série, N.º 67, 5 de abril de 2013.
- Resolução do Conselho de Ministros n.º 26/2013, de 19 de abril. Aprova as linhas de orientação para a execução da reforma estrutural da defesa nacional e das Forças Armadas, designada por Reforma «Defesa 2020». *Diário da República*, 1.ª série, N.º 77, 19 de abril de 2013.
- Resolução do Conselho de Ministros n.º 7-A/2015, de 20 de fevereiro. Aprova a Estratégia Nacional de Combate ao Terrorismo. *Diário da República*, 1.ª série, N.º 36, 20 de fevereiro de 2015.
- Santos, J. L., 2016. *A Guerra no meio de nós: A realidade dos conflitos do século XXI*. Lisboa: Clube do Autor.
- Sistema de Segurança Interna, 2016. *Relatório Anual de Segurança Interna 2016*. [Online] Disponível em: [http://www.ansr.pt/InstrumentosDeGestao/Documents/Relat%C3%B3rio%20Anual%20de%20Seguran%C3%A7a%20Interna%20\(RASI\)/RASI%202016.pdf](http://www.ansr.pt/InstrumentosDeGestao/Documents/Relat%C3%B3rio%20Anual%20de%20Seguran%C3%A7a%20Interna%20(RASI)/RASI%202016.pdf) [Acedido em 17 Maio 2017].
- Sousa, F., 2011. A Participação de Portugal nas Operações de Paz e a Segurança Nacional. *Revista Militar*, N.º 2509/2510, março, pp. 271-297.
- Teixeira, N. S., 2009. Que Visão para a Defesa? Desafios que se Colocam a Portugal. *Nação e Defesa*, N.º 124, pp. 9-18.
- Tomé, L., 2015. “Estado Islâmico” percurso e alcance um ano depois da auto-proclamação do “Califado”. *Janus.net*, Volume 6, N.º 1, pp. 125-149. Disponível em: https://www.academia.edu/14142387/_ESTADO_ISL%C3%82MICO_PERCURSO_E_ALCANCE_UM_ANO_DEPOIS_DA_AUTO-PROCLAMA%C3%87%C3%83O_DO_CALIFADO_
- United Nations Human Security Unit, 2014. *Strategic Plan 2014-2017*. New York: Human Security Unit.
- United Nations Trust Fund for Human Security, 2009. *Human Security in Theory and Practice*. New York: United Nations.

REVISTA NAÇÃO E DEFESA

Números temáticos publicados

1998	84	Inverno	Uma Nova NATO numa Nova Europa
	85	Primavera	Portugal e o Desafio Europeu
	86	Verão	O Desafio das Águas: Segurança Internacional e Desenvolvimento Duradouro
	87	Outono	O Estado em Mudança
1999	88	Inverno	Mulheres nas Forças Armadas
	89	Primavera	Portugal na NATO: 1949-1999
	90	Verão	Economia & Defesa
	91	Outono	Operações de Paz
2000	92	Inverno	Portugal e as Operações de Paz na Bósnia
	93	Primavera	Novos Rumos da Educação para a Cidadania
	94	Verão	Democracia e Forças Armadas
	95/96	Outono-Inverno	Prevenção de Conflitos e Cultura da Paz
2001	97	Primavera	Nova Ordem Jurídica Internacional
	98	Verão	Forças Armadas em Mudança
	99	Outono	Segurança para o Século XXI
	100	Inverno	De Maastricht a Nova Iorque
2002	101	Primavera	Europa e o Mediterrâneo
	102	Verão	Repensar a NATO
	103	Outono-Inverno	Novos Desafios à Segurança Europeia
	Extra	Dezembro	Cooperação Regional e a Segurança no Mediterrâneo (C4)
2003	104	Primavera	Evolução das Nações Unidas
	Extra	Abril	A Revolução nos Assuntos Militares
	105	Verão	Soberania e Intervenções Militares
	106	Outono-Inverno	A Nova Carta do Poder Mundial
2004	107	Primavera	Forças Armadas e Sociedade. Continuidade e Mudança
	Extra	Julho	Educação da Juventude. Carácter, Liderança e Cidadania
	108	Verão	Portugal e o Mar
	109	Outono-Inverno	Segurança Internacional & Outros Ensaios
2005	110	Primavera	Teoria das Relações Internacionais
	111	Verão	Raymond Aron. Um Intelectual Comprometido
	112	Outono-Inverno	Número não Temático
2006	113	Primavera	Número não Temático
	114	Verão	Segurança na África Subsariana
	115	Outono-Inverno	Portugal na Europa Vinte Anos Depois

2007	116	Primavera	Número não Temático
	117	Verão	Número não Temático
	118	Outono-Inverno	Políticas de Segurança e Defesa dos Pequenos e Médios Estados Europeus
2008	119	Primavera	Transição Democrática no Mediterrâneo
	120	Verão	Número não Temático
	121	Outono-Inverno	Estudos sobre o Médio Oriente
2009	122	Primavera	O Mar no Pensamento Estratégico Nacional
	123	Verão	Portugal e a Aliança Atlântica
	124	Outono-Inverno	Que Visão para a Defesa? Portugal-Europa-NATO
2010	125	Primavera	Visões Globais para a Defesa
	126		O Conceito Estratégico da NATO
	127		Dinâmicas da Política Comum de Segurança e Defesa da União Europeia
2011	128		O Mar no Espaço da CPLP
	129		Gestão de Crises
	130		Afeganistão
2012	131		Segurança em África
	132		Segurança no Mediterrâneo
	133		Cibersegurança
2013	134		Ásia-Pacífico
	135		Conselho de Segurança da ONU
	136		Estratégia
2014	137		Reflexões sobre a Europa
	138		Brasil
	139		Portugal na Grande Guerra
2015	140		Nuclear Proliferação
	141		Arquipélago dos Açores
	142		Índia
2016	143		Terrorismo Transnacional
	144		The EU Comprehensive Approach: Concepts and Practices
	145		Leituras da Grande Guerra
2017	146		Drones
	147		Brexit
	148		Grupos Islamistas Radicais
2018	149		Europe and Refugees
	150		European Defence
	151		Geopolítica Aplicada

Política Editorial

Nação e Defesa é uma publicação periódica do Instituto da Defesa Nacional que se dedica à abordagem de questões no âmbito da segurança e defesa, tanto no plano nacional como internacional. Assim, *Nação e Defesa* propõe-se constituir um espaço aberto ao intercâmbio de ideias e perspectivas dos vários paradigmas e correntes teóricas relevantes para as questões de segurança e defesa, fazendo coexistir as abordagens tradicionais com as problemáticas de segurança mais recentes.

A Revista dá atenção especial ao caso português, sendo um espaço de reflexão e debate sobre as grandes questões internacionais com reflexo em Portugal e sobre os interesses portugueses, assim como sobre as grandes opções nacionais em matéria de segurança e defesa.

Editorial Policy

Nação e Defesa (Nation and Defence) is a quarterly journal published by the National Defence Institute of Portugal, focused on security and defense issues at the national and international levels. *Nação e Defesa* is a forum to exchange ideas and views concerning the various theoretical and empirical approaches relevant to security and defence issues.

The journal pays special attention to the Portuguese situation, being a space for reflection and debate over the broad choices that Portugal faces in terms of security and defence, as well as other international security issues with potential impact on Portuguese interests.

NORMAS DE COLABORAÇÃO

O artigo proposto para publicação deverá ser enviado via correio eletrónico para idn.publicacoes@defesa.pt

O texto terá de observar as seguintes normas:

- Ter entre 30.000 a 50.000 caracteres (espaços incluídos) em Word for Windows.
- Ser acompanhado de um resumo em português e em inglês (até 1000 caracteres cada).
- Ser redigido de acordo com a norma de Harvard disponível em <http://libweb.anglia-ac-uk/referencing/harvard.htm>

O artigo, sem indicação do autor e acompanhado pela Ficha de Identificação (disponível em <http://www.idn.gov.pt/conteudos/documentos/FichadeAutor.pdf>) devidamente preenchida, será apreciado em regime de anonimato pelo Conselho Editorial da revista.

Os artigos aprovados pelo Conselho Editorial pressupõem o direito de publicação exclusiva na revista Nação e Defesa.

A revista Nação e Defesa poderá publicar artigos já editados noutras publicações mediante autorização por parte da respetiva Editora.

Todo o artigo publicado é da inteira responsabilidade do autor, sendo a revisão das provas tipográficas da responsabilidade do Instituto da Defesa Nacional.

O pagamento dos honorários aos autores (150 € por artigo) será efetuado por transferência bancária. Cada autor receberá três exemplares da revista na morada indicada.

Os casos não especificados nestas Normas de Colaboração deverão ser apresentados ao Coordenador Editorial da Nação e Defesa.

PUBLICATION NORMS

The submitted article will have to be sent by email to idn.publicacoes@defesa.pt

The text should obey to certain requirements:

- It should have between 30.000 and 50.000 characters (spaces included), and must be presented as a Microsoft Word document.
- The author should provide an abstract of the article (until 1000 characters).
- Written according to the Harvard reference system available at <http://libweb.anglia.ac.uk/referencing/harvard.htm>

The article should not contain any reference to its author. The sole means of identifying the author is a duly filled ID form (<http://www.idn.gov.pt/conteudos/documentos/FichadeAutor.pdf>), so its submission is compulsory.

The journal's Editorial Board, on an anonymous basis, will appraise the text. The article's approval by the Editorial Board implies the possession of exclusive publishing rights by *Nação e Defesa*. The publication of non-exclusive articles by this journal depends upon acknowledgment of the legitimate holder of the article's publishing rights.

The author shall hold full responsibility for the content of the published article. The *Instituto da Defesa Nacional* is responsible for the article's typographical revision.

The author's honorarium for each published article (150 €) will be paid by bank transfer. Three issues of the journal will be sent to the address indicated in the ID form.

All cases not envisioned in these Norms should be presented to the Editorial Coordinator of *Nação e Defesa*.



NAÇÃO E DEFESA

Revista quadrimestral

Nome/Name _____

Morada/Address _____

Localidade/City _____

Cód. Postal/Zip _____ NIF _____

Country _____

E-mail _____

Tel./Phone _____

Renovação/Renewal – Assin. nº/Subscrip. nr. _____

Nova assinatura/New subscription

Assinatura/Signature _____

Data/Date _____

INSTITUTO DA DEFESA NACIONAL
Caíada das Necessidades, 5, 1399-017 Lisboa
PORTUGAL

Assinatura Anual/Annual Subscription (3 nºs /issues)

Instituições/Institutions 40,00 €

Individuais/Individuals 25,00 €

Estudantes/Students 20,00 € (anexar comprovativo deste ano)

Números Anteriores/ Previous Issues – 8,50 € cada/each + portes/
/postage charges

Pré-Pagamento/Prepayment

Numerário

Cheque nº _____ Banco _____ à ordem do IDN

Transferência Bancária NIB 0781 0112 0000 000 7777 20
(anexar comprovativo da Transferência)

Bank Transfer (compulsory for foreign subscriptions)

IBAN – PT50 0781.0112 0000 000 7777 20

BIC (SWIFT) – IGCPTPL

www.idn.gov.pt

ids.publicacoes@defesa.pt

tel. + 351 21 392 46 00 Fax + 351 21 392 46 58

EXTRA DOSSIÊ

TERESA VICENTE RODRIGUES UMA NOVA VISÃO DA SUSTENTABILIDADE DA MARINHA
DE DUPLO-USO NUNO IMPERIAL O CONCEITO DE EMPREGO DAS FORÇAS ARMADAS EM
MATÉRIAS DE SEGURANÇA INTERNA

