Universidade da Maia
Departamento de Ciências Sociais e do Comportamento

A Deteção Comportamental Enquanto Ferramenta de Prevenção do Terrorismo

Alexandra Ferreira Leite

Criminologia

Orientador Institucional

Professor Doutor António Leitão da Silva

Setembro2021

Universidade da Maia

Departamento de Ciências Sociais e do Comportamento

2º Ciclo de Estudos em Criminologia

A Deteção Comportamental Enquanto Ferramenta de Prevenção do Terrorismo

Dissertação de Mestrado em Criminologia

Alexandra Ferreira Leite

(a032273@ismai.pt)

Trabalho realizado sob a orientação do Professor Doutor António Leitão da Silva

Setembro, 2021

"With guns we can kill terrorists, with education we can kill terrorism."

- *Malala Yousafzai*

Agradecimentos

A elaboração de uma dissertação de mestrado é uma caminhada longa e difícil que só é possível com a ajuda e o apoio daqueles que nos rodeiam.

Ao orientador desta dissertação, o Professor Doutor António Leitão da Silva, os meus agradecimentos por ter aceitado este compromisso, pela orientação prestada e pelo contributo com os seus conhecimentos e conselhos, sem os quais este trabalho não teria sido possível.

A toda a minha família, especialmente aos meus pais, que sempre alimentaram os meus sonhos e apoiaram as minhas decisões, e à minha tia Laurinda, que possibilitou que esses mesmos sonhos se tornassem realidade, um "obrigada" nunca será suficiente para expressar a gratidão que sinto.

Ao Vasco, por apresentar sempre um sorriso nos momentos mais difíceis e me relembrar diariamente do potencial que acredita que tenho e inspirar a fazer mais e melhor, obrigada.

Aos meus amigos, que tornaram este percurso menos solitário, contribuindo com o apoio e carinho que caracteriza a nossa amizade.

À Universidade da Maia (ISMAI), que me acolheu há cinco anos atrás cheia de sonhos e vontade de os concretizar e me viu crescer académica e pessoalmente, expresso a minha gratidão com muito carinho e saudade.

A Deteção Comportamental Enquanto Ferramenta de Prevenção do Terrorismo

Resumo

O crime de terrorismo configura uma das maiores ameaças à segurança e soberania de um Estado. Os ataques de 11 de setembro forçaram os líderes mundiais a reunir esforços para reforçarem a segurança interna dos seus países e protegerem os seus cidadãos. Ao longo dos anos, o terrorismo foi assumindo diversas formas e acompanhando a evolução social e tecnológica, surpreendendo com novas vertentes. Se outrora este tipo de criminalidade era esperado por atores estrangeiros, hoje, o terrorismo doméstico é um desafio para qualquer Estado. As tecnologias passaram também a fazer parte das estratégias de grupos e/ou organizações terroristas, servindo não só como estratégia de ataque, como também de recrutamento. E o *modus operandi* foi evoluindo e transformando-se, podendo hoje passar pela utilização de explosivos altamente complexos, a armas de fogo, armas brancas ou a simples utilização de um veículo.

Neste seguimento, elaborou-se uma revisão de literatura extensiva sobre a Deteção Comportamental e o seu papel na prevenção de atos terroristas. Foram analisados textos estrangeiros e nacionais e recolhidas informações chave que, posteriormente, foram organizadas num guia de boas práticas para a utilização da deteção comportamental como ferramenta preventiva do terrorismo.

Behavioral Detection as a Tool to Prevent Terrorism

Abstract

Terrorism is one of the main threats to national security and sovereignty of Nations. The September 11 attacks forced global leaders to reunite forces and fortify their countries' national security and protect their citizens. Throughout the years, terrorism has assumed different shapes and follow social and technological evolution, surprising with new aspects that have been arising over the years. If in the past these types of crime were expected to be committed by foreign agents, nowadays, domestic terrorism is a great challenge to any nation. Technologies have also become of new terrorist groups or organizations' strategies, serving as method of attack and has a recruitment platform. Also, the *modus operandi* has evolved *and transforming*, being now possible to be the use of complex explosive devices, fire weapons, bladed weapons, or the simple use of a vehicle.

In this regard, an extensive literature review about Behavior Detection and its role on terrorism prevention has been undertaken. Foreign and national texts were analyzed, and the most important information was collected and, later, organized into a guide for the use of Behavior Detection as a tool to prevent terrorism.

Índice

Lista de abreviaturas, siglas e acrónimos

- ACLU *(American Civil Liberties Society)*
- ACT *(Action Counters Terrorism)*
- BDO *(Behavior Detection Officer)*
- CELT (Centro Europeu de Luta Contra o Terrorismo)
- CPNI *(Centre for the Protection of National Infrastructure)*
- CRP (Constituição da República Portuguesa)
- DHS (*Department of Homeland Security)*
- EI (Estado Islâmico)
- ENCT (Estrutura Nacional de Combate ao Terrorismo)
- FBI *(Federal Bureau of Investigation)*
- ILP *(Intelligence-led policing)*
- ISE-SAR *(Information Sharing Environment – Suspicious Activity Report)*
- MP (Ministério Público)
- NSI *(National Suspicious Activity Reporting Initiative)*
- SAR *(Suspicious Activity Report)*
- SPOT *(Screening of Passsengers by Observation Techniques)*
- RAN *(Radicalisation Awareness Network)*
- TSA *(Transportation Security Administration)*
- UE (União Europeia)
- US *(United States)*

Lista de figuras

Capítulo I

Introdução

O terrorismo é um fenómeno criminal que tem causado alarme em todos os países, por ser uma das maiores ameaças à segurança interna. A Europa, tem sido, nos últimos anos, alvo de vários ataques terroristas, nomeadamente de natureza jihadista, praticados por atores externos, mas também, muito frequentemente, por cidadãos naturais do país atacado.

Assim, e uma vez que a criminologia entende o ser humano como um ser biopsicossocial, cujos comportamentos são influenciados por um conjunto de fatores biológicos, psicológicos e sociais, entendeu-se que seria importante estudar a Deteção Comportamental enquanto uma ferramenta preventiva a ser utilizada, nomeadamente pela polícia de proximidade e pela comunidade, no contexto do terrorismo.

O comportamento humano pauta-se pela sua imprevisibilidade, seja este comportamento normativo, desviante ou patológico. Isto torna a antecipação do comportamento humano um desafio, contudo, também enaltece a necessidade de antecipação do comportamento desviante sempre que possível, de modo a preveni-lo (Silva, 2017).

A palavra terrorismo, surgiu pela primeira vez durante Revolução Francesa, com os atos praticados pelos agentes revolucionários (Martins, 2010). Não existe um consenso sobre a sua definição. No entanto, a literatura refere que este se carateriza pelo uso constante da violência, com o intuito de implementar o terror numa determinada sociedade, tendo como finalidade atingir o Estado e produzir uma mudança política (Rezende & Schwether, 2015).

Com o 11 de setembro de 2001, a conceção de terrorismo alterou-se a nível global. Este evento veio desvendar as grandes fragilidades da segurança aérea e a imprevisibilidade do terrorismo moderno. Com isto, os Estados Unidos e todo o Ocidente, viram a sua segurança interna ameaçada. Consequentemente, o terrorismo passou a ser uma temática prevalente em todos os debates de política internacional (Martins, 2010).

Este novo mundo globalizado e as oportunidades que criou para grupos extremistas e terroristas, obrigou a adoção de medidas repressivas e preventivas inovadoras por parte dos

Estados, destacando-se a Deteção Comportamental como uma ferramenta preventiva que se foca na identificação de comportamentos atípicos, mas possivelmente com traços comuns no contexto destes ataques.

Tendo em conta este enquadramento, passaremos a analisar qual o papel da Deteção Comportamental na prevenção e no combate à radicalização e ao terrorismo, através de dois grandes atores principais: a polícia de proximidade e a comunidade.

Para isso, iremos abordar alguns temas chave como o conceito de segurança interna, a temática da radicalização e do terrorismo; a realidade mundial, europeia e portuguesa no que toca a estes fenómenos; as estratégias de prevenção mais comumente utilizadas; as teorias científicas relativas ao processo de radicalização e aos comportamentos adotados; e, finalmente, o papel da polícia de proximidade e da comunidade na prevenção do terrorismo, nomeadamente através da Deteção Comportamental.

A investigação

Nota Introdutória

Em Portugal, não existem estudos sobre a Deteção Comportamental utilizada no contexto da prevenção do crime de terrorismo, pelo que se entendeu que seria importante dar um contributo para a compreensão desta abordagem.

Passaremos à apresentação da metodologia utilizada para a realização do estudo, seguida de uma contextualização conceptual do tema.

Objetivos e Pergunta de Partida

Este projeto tem como objetivo geral, analisar a possibilidade da utilização da abordagem da deteção comportamental enquanto ferramenta de prevenção do terrorismo.

Para se concretizar este objetivo geral, elencam-se como objetivos específicos: a) definir e desenvolver o conceito de terrorismo e radicalização; b) compreender a Deteção Comportamental; c) conhecer e desenvolver o papel da polícia na implementação da Deteção Comportamental; e) estudar a comunidade enquanto *"screener"* de comportamentos.

Desta forma, a pergunta de partida deste projeto é: Como pode a deteção comportamental ser utilizada como ferramenta de prevenção do terrorismo em Portugal?

Paradigma e Metodologia

A presente investigação seguiu o paradigma qualitativo ou interpretativo. Este paradigma caracteriza-se pela intenção de compreender *"o mundo complexo do vivido desde o ponto de vista de quem vive"* (Coutinho, 2014, p. 18). Isto é, compreender e interpretar a ação humana no seu contexto social. Neste sentido, dá-se uma busca pelos significados dos comportamentos, o investigador e o investigando assumem, simultaneamente, o papel de "interpretes" e "construtores de sentidos" (Coutinho, 2014, p. 18).

Para o objetivo da investigação - analisar a possibilidade da utilização da abordagem da deteção comportamental enquanto ferramenta de prevenção do terrorismo – ser alcançado, foi utilizada a metodologia qualitativa, já que esta está relacionada com a investigação dos significados das ações individuais e das interações sociais a partir da perspetiva dos intervenientes. A metodologia qualitativa nasce da perspetiva de que o comportamento humano não é regido por leis universais (Coutinho, 2014). Este tipo de metodologia procura compreender o fenómeno do ponto de vista do participante, ou seja, focar-se no significado que o participante atribui aos eventos ou as ações a serem estudadas (McMillan & Shumacher., 2014).

A investigação qualitativa tem algumas características que a distinguem dos restantes tipos de investigação. Na investigação qualitativa, o estudo do comportamento acontece no seu estado natural, isto é, não há manipulação ou controlo dos comportamentos nem do contexto em que estes são estudados, os investigadores acreditam que a única forma de compreender um fenómeno é permitindo que ele aconteça no seu contexto natural. Acreditam também que a ação humana é fortemente influenciada pelo contexto em que ocorre, e, portanto, é essencial tê-lo em consideração durante o estudo. O entendimento do investigador é que os significados estão condicionados for um conjunto de fatores sociais, políticos, de género, raciais, de classe e tecnológicos (Gomez et al., 1996)

Neste tipo de investigação, parte-se do pressuposto de que nada é irrelevante. Todos os detalhes são estudados aprofundadamente para que haja um entendimento completo do fenómeno a ser estudado. Os estudos qualitativos procuram entender o processo através do qual

o fenómeno acontece, ao invés de procurarem apenas os resultados (McMillan & Shumacher, 2014).

Tratam-se também de estudos indutivos, e que, portanto, não formulam hipóteses que procuram confirmar ou refutar. Procuram antes recolher informação e, apenas mais tarde, formular generalizações (McMillan & Schumacher, 2014).

Uma característica que marca profundamente a metodologia qualitativa é a crença de que o mundo é demasiado complexo e não existem explicações simples para o comportamento humano. Desta forma, é essencial examinar várias perspetivas para que o entendimento seja o mais próximo da realidade possível. No entanto, os investigadores acreditam que não é possível encontrar uma explicação que consiga compreender na totalidade a situação em estudo (Gomez et al., 1996).

No que diz respeito ao nível metodológico, a investigação qualitativa baseia-se no método indutivo, pois tenta compreender a situação com a qual se confronta sem impor ideias pré-concebidas, procurando interpretar e atribuir significados com base no estudo da ação. Na investigação qualitativa, a teoria é posterior aos factos e desenvolve-se com base nos dados recolhidos e analisados. Este tipo de investigação privilegia a diversidade individual ao invés de procurar generalizações (Coutinho, 2014).

Procedimento e recolha de dados

Relativamente ao procedimento e recolha de dados, foi decidido realizar-se uma revisão de literatura extensiva.

Como critérios de inclusão incluíram-se todos os estudos encontrados que retratavam a temática da Deteção Comportamental e do Terrorismo. Foram incluídos estudos em inglês e português.

Para a identificação da literatura relevante utilizara-se as palavras-chave *"Deteção Comportamental", "Behavioral Detection", "Terrorismo", "Terrorism", "Terrorism Prvention", "Prevenção do Terrorismo", "Behavior and Terorism", "TSA", "Terrorist Attacks", "Terrorist" e "Behavioral Detection Officers"*. Para cada texto foi inicialmente analisado e título e o resumo para determinar se seria importante para o estudo a ser realizado.

As bases de dados utilizadas foram o *Google Scholar*, a base de dados da Procuradoria-Geral da República, o Repositório do Instituto Superior de Ciências Policiais e Segurança Interna. Estas bases de dados estas, comumente utilizadas para a realização de revisões literárias nas mais diversas áreas científicas. Durante a pesquisa delimitou-se a janela temporal entre 2001 e 2021, de modo que as informações fossem o mais atuais possíveis.

Para avaliar a qualidade e a elegibilidade dos estudos encontrados, os textos foram lidos na integra. Procurou-se priorizar os materiais de autores com maior reputação ou pulicados por entidades de relevância de modo a assegurar-se a qualidade das informações adquiridas.

No total, 47 estudos e/ou textos foram lidos e analisados.

Capítulo II

Conceitos

1.1 Terrorismo

A *Global Terrorism Database*, define terrorismo como *"o uso ameaçador ou real de força e violência ilegais por um ator não governamental para atingir uma meta política, económica, religiosa ou social através do medo, coerção ou intimidação"* (Henne, 2019, p.14).

O conceito antigo limitava a sua dimensão a níveis regionais e a espaços delimitados. Atualmente, o conceito de fronteiras tem vindo a desvanecer devido ao fenómeno da globalização, e, por esse motivo, a nova realidade permite aos movimentos terroristas ir além-fronteiras, constituindo uma ameaça global. Assim, este fenómeno, nos moldes atuais, ameaça, não só a ordem, mas também a paz e segurança mundiais (Rezende & Schwether, 2015).

1.2 Radicalização

O termo "radicalização" é comumente utilizado, contudo, não existe uma definição clara do mesmo. Este termo é então complexo e controverso. Desde 2004 que é um termo central em estudos e legislações relativas ao terrorismo e ao contraterrorismo (Schmid, 2013). Este termo carece de uma definição universal, já tendo sido descrito de várias e diferentes formas – *"socialização extremista que se manifesta no terrorismo*", *"radicalização enquanto um*

processo escalado que leva à violência", "processo caracterizado pelo aumento de comprometimento e uso de meios e estratégias violentas em conflitos políticos" (Schmid, 2013, pp. 5,6).

1.3 Deteção Comportamental

É com dificuldade que na literatura nacional e internacional se encontra uma definição clara e concreta do que significa deteção comportamental.

Muitas vezes, este método é também conhecido por outros termos, entre eles: análise comportamental ou consciência comportamental (HM Government, 2020).

A análise comportamental, é definida pela Associação do Novo México como o estudo científico dos princípios da aprendizagem e do comportamento. Segundo esta associação, trata-se um campo científico que se debruça sobre a descrição, compreensão, predição e alteração do comportamento. O objetivo principal é compreender o comportamento e alterá-lo através de fatores biológicos e comportamentais.

Por sua vez, o FBI refere-se, por exemplo, à avaliação de ameaças através do comportamento, como uma avaliação sistémica, baseada em factos, que combina informações recolhidas a partir de várias fontes de informação como a investigação científica e a experiência profissional de modo a identificar os padrões de pensamento e comportamento, com o intuito de determinar se um individuo está a planear ou a tentar implementar um ataque (Amman et al., 2015).

No entanto, é o governo do Reino Unido que oferece uma definição mais clara, referindo-se à deteção comportamental enquanto um método de deteção de indivíduos com intenções hostis a partir dos seus comportamentos e atitudes (HM Government, 2020).

Desta forma, e uma vez que não existe uma definição universal de deteção comportamental na literatura, decidiu-se que seria essencial sugerir uma definição no âmbito do presente trabalho. Assim, este estudo entende deteção comportamental enquanto uma técnica de observação de comportamentos, que, com base na investigação científica dos padrões comportamentais e na experiência, identifica indivíduos com comportamentos ou atitudes atípicas e inapropriados que indicam a presença de uma potencial ameaça para a segurança pública. Para a utilização deste método deve-se ter em conta diversos fatores como o contexto, a cultura e o comportamento esperado para o ambiente em que o individuo está inserido.

1.4 Segurança Interna

De acordo com a Lei nº 53/2008, a Segurança Interna entende-se por uma *"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".*

Trata-se pois da proteção, através do Estado, do território, cidadãos e bens nacionais, de modo a assegurar a paz e a segurança do país assim como o exercício das liberdades e dos direitos plasmados na Constituição.

1.5 Soft Targets

Os *soft targets* são locais públicos ou privados, relativamente vulneráveis a ataques terroristas devido às duas características de funcionamento e segurança (ex: aeroportos, centros comerciais, ruas muito movimentadas, escolas, eventos culturais, etc.). São locais que, devido à sua natureza, concentram um grande número de pessoas e fazem parte das atividades quotidianos da comunidade, podem também ter um significado simbólico e são normalmente escolhidos para ataques terroristas por proporcionarem um maior número de casualidades (Cuesta et al., 2019).

Na Europa, têm acontecido vários ataques terroristas a *soft targets*, o que comprova a preferência destes locais por parte deste tipo de ofensores.

1.6 Lone wolves

O termo *lone wolf* surge no séc. XIX, associado aos movimentos anarquistas e à resistência sem líder. Esta é uma das características mais importantes do terrorismo *lone wolf* (Rego, 2017).

No séc. XX, vários indivíduos levaram a cabo ataques terroristas individuais, como George Metesky e o conhecido *"Unambomber"*. Eram considerados *lone wolves* por se tratar

de indivíduos que operavam de forma solitária, implementando ataques de iniciativa anti estatal sem terem afiliações a grupos ou organizações terroristas (Rego, 2017).

Burton e Stewart (2008), definem *lone wolf* enquanto um individuo que implementa ataques terroristas de forma individual e solitária, sem se estar sob a hierarquia ou a tutela de uma ação ou grupo terrorista (Rego, 2017).

O terrorismo islâmico

O terrorismo islâmico é uma das maiores ameaças à segurança interna dos Estados e à democracia europeia. Ameaça esta que tem vindo a surpreender os Estados pelo aumento de radicais naturais e residentes na Europa (Costa e Pinto, 2012).

Não só se torna cada vez mais complexo assegurar a segurança devido ao desenvolvimento feroz das novas tecnologias e aos novos sistemas de comunicação como as organizações e os grupos terroristas se adaptam cada vez mais rápido e criam novas estratégias e métodos de ataque (Costa e Pinto, 2017).

O movimento jihadista surgiu no início da década de 70 e construiu uma linha fundamentalista de uma visão mítica do islamismo. Nesta altura, surgiu uma nova geração de islamitas radicais que passou a justificar o uso da violência política transnacional como meio para restaurar o tão desejado califado (Chaliand e Blin, 2017).

Atualmente, é o terrorismo *mujahidden* islâmico, baseado nos princípios do salafismo (com origem sunita) a maior ameaça mundial (Chaliand e Blin, 2017).

O movimento *mujahideen*, também conhecido por "islamismo jihadista", pode ser mais bem explicado pela expressão "jihade pela espada" (Chaliand e Blin, 2017).

Não existe uma definição única de Islamismo, contudo, podemos defini-la como *"a afirmação e a promoção de crenças, leis, políticas e preceitos com carácter islâmico"* (Costa e Pinto, 2012, p. 174). O Islamismo pauta-se também pela oposição à modernidade e ao Ocidente (Costa, 2016).

Os povos do Islão mantêm até hoje uma relação estreita entre a religião e o Estado, estes fundem-se de modo a que haja uma defesa do "verdadeiro Islão" (Barata, 2017). Desta forma, os islamistas acreditam que uma verdadeira sociedade islâmica passa pela existência de um Estado islâmico e pela prática da *Sharia* (Lei) (Costa, 2016).

O Islamismo assenta em cinco princípios fundamentais. O primeiro é a unidade com Deus, isto é, Alá é o único Deus e Muhammad o Seu Profeta. Segue-se a *salat,* que significa oração; esta ocorre cinco vezes por dia, numa das quais o profeta se vira para Meca, e à sexta-feira (dia santo) é realizada na mesquita, liderada pelo imã (guia religioso) que se posiciona de frente para os devotos que se alinham de ombro a ombro. O terceiro princípio é o *zakat,* que se traduz na esmola para os necessitados; para o islão todos os bens pertencem a Deus, que os empresta, mas exige solidariedade entre os crentes. Em quarto lugar está o *saum,* o jejum que acontece durante o mês do Ramadão, do nascer ao pôr do sol. Por último, o *hajj*, a peregrinação a Meca que deve acontecer pelo menos uma vez na vida (Chaliand e Blin, 2017).

No entanto, eram conferidas dispensas especiais àqueles que tinham a possibilidade de espalhar o islão (marinheiros, soldados, comerciantes). Estas dispensas foram aproveitadas pelo movimento jihadista de modo a justificar a luta contra os infiéis. O Corão enumera também os momentos mais importantes da vida de um muçulmano, sendo estes o nascimento, a circuncisão, o(s) casamento(s), a vida familiar, a morte e o legado (Chaliand e Blin, 2017).

Dentro do mundo islâmico coexistem duas vertentes do islão com diferenças na doutrina, rituais, leis, organização e teologia. E, apesar de coexistirem, vivem em conflito (BBC News Brasil, 2020).

A recolocação da religião como força, motivação e até justificação da resistência tem reavivado a oposição entre os xiitas e sunitas que vai para lá de uma oposição religiosa ou étnica. O crescimento do xiismo e a sua luta para ser tornar uma potencia regional, acompanhado com o declínio dos sunitas em países como o Egipto e a Arábia Saudita, bem como a violência interétnica têm contribuído para o aumento a tensão entre as duas posições do islão (Barata, 2007).

A divisão entre estas duas posições remonta à origem do Islão e foca-se sobretudo nas divergências no que respeita à sucessão legitima do Profeta (Barata, 2017).

Falamos agora dos xiitas e dos sunitas e dos principais trações históricos que os caracterizam. Esta divisão teve origem no ano de 632 com a morte de Maomé (profeta), que originou uma luta pela liderança dos muçulmanos (BBC News Brasil, 2020).

Os sunitas representam a maioria dos muçulmanos e consideram-se o ramo mais tradicional e puro do islão. Este nome tem origem na expressão *"Ahl al-Sunna"*, que significa "o povo da tradição". Os sunitas veneram todos os profetas do Alcorão, no entanto, Maomé é

particularmente adorado e é considerado o profeta supremo. Os professores e líderes sunitas têm fortes ligações com o Estado e com os governos (BBC News Brasil, 2020).

A sua relação próxima com as figuras de liderança religiosas e governamentais favoreceu o sunismo ao longo dos tempos e ajudou a que se tornasse a corrente islâmica com mais força (Barata, 2017).

Este ramo do islão tem especial representatividade na Arabia Saudita (BBC News Brasil, 2020).

Já os xiitas, surgem da expressão *"Shiat Ali"*, que significa "o partido de Ali", começando, portanto, como uma fração política. Estes acreditam que o sucessor do profeta Maomé deve ser Ali (Barata, 2017).

Ali era genro de Maomé, e, para os xiitas era a Ali e aos seus descendentes que pertencia o direito de liderar os muçulmanos. Ali morreu na sequência dos acontecimentos violentos (guerras civis e intrigas) que marcaram o seu califado e foi negado aos seus filhos, Hassan e Hussein, o direito de lhe suceder (BBC News Brasil, 2020).

Segundo as crenças xiitas, Hassan terá sido envenenado pelo primeiro califa, Muawiyah. E o seu irmão, terá falecido num campo de batalha. É em consequência destes dois eventos que surgem os rituais de luto e o conceito xiita de martírio (BBC News Brasil, 2020).

Este ramo do Islão, tem a sua origem no Iraque, no entanto, é o Irão o único estado cuja religião oficial é o xiismo (Barata, 2017). Os xiitas têm também um caracter messiânico e adotam uma hierarquia de clérigos (BBC News Brasil, 2020).

Os xiitas, são tradicionalmente povos oprimidos e ligados à vocação messiânica, já que creditam que o 12º imã, descendente de Ali, voltará no fim dos tempos para restabelecer a justiça e a igualdade. De modo a sobreviverem a esta opressão, foram-se comportando com algum quietismo e dissimulação enquanto esperavam ser libertos pelo 12º imã (Barata, 2017).

A maior parte dos fiéis xiitas são populações do Irão, Iraque, Bahrein, Azerbaijão e do Iémen. No entanto, existem populações xiitas também no Afeganistão, na Índia, no Kuwait, Líbano, Paquistão, Catar, Síria, Turquia, Arabia Saudita e Emirados Árabes Unidos (BBC News Brasil, 2020).

Os confrontos entre sunitas e xiitas são especialmente notórios do Iraque (Barata, 2017).

Na verdade, mais do que uma batalha religiosa, esta trata-se de uma luta pelo poder e pela liderança do povo muçulmano (Barata, 2017).

Falamos em terrorismo islâmico para descrever a utilização do terrorismo pelos ativistas islâmicos para impor os pontos de vista da sua política identitária (Chaliand e Blin, 2017).

Atualmente, é difícil definir se o terrorismo islâmico que conhecemos se trata de terrorismo religioso ou terrorismo revolucionário. No entanto, é notório que o principal objetivo do terrorismo islâmico tal como o conhecemos nos dias de hoje é a radicalização em massa. Assim, pode-se entender que o seu carater é muito mais revolucionário do que religioso (Chaliand e Blin, 2017).

É importante mencionar que, tal como será posteriormente explicado com mais detalhe, devemos distinguir a radicalização de radicalização violenta, pelo que, tal como em todas as formas de radicalismo, o radicalismo Islâmico assume várias formas na Europa e no resto do Mundo (Costa e Pinto, 2012).

Salienta-se também que o Islamismo não implica sempre um caráter violento, a vertente violenta de alguns grupos não representa o Islão e é importante também explicar que a violência utilizada por estes grupos teve origem, na grande parte dos casos, na opressão a que foram submetidos ao longo dos tempos (Costa, 2016).

Jihadismo

O termo "jihad" em árabe, refere-se a "esforço" e "luta". No Islão significa a luta interna do ser humano contra os seus instintos básicos; ou seja, a vida é uma batalha contínua para se ser um bom muçulmano. No contexto radical, ser um bom muçulmano pode ser interpretado como uma guerra contra os não crentes (BBC, 2014).

O terrorismo jihadista é um movimento associado à Al-Qaeda e aos movimentos a este grupo associados. Surge a partir da interpretação de Bin Laden da doutrina islâmica, que a entende como uma luta contra os países ocidentais com o intuito de construir uma Jihad global (Martins, 2018).

A Jihad é uma guerra em nome de Deus, que o pretende enaltecer através do sacrifício do próprio individuo. Ou seja, trata-se de um mecanismo de proliferação da ordem política e social islâmica, aniquilando as outras fés (Martins, 2018).

O termo "jihadista" passou a ser comumente utilizado nos países ocidentais nos anos 90 e com ainda mais frequência depois dos ataques às torres gémeas a 11 de setembro de 2001, como uma forma de distinguir os islamistas violentes dos não violentos (BBC, 2014).

Não raramente o termo islamista é confundido com jihadista. Enquanto os islamistas pretendem uma reorganização governamental e social de acordo com a lei islâmica, os jihadistas vêm a violência como necessária para erradicar os obstáculos na reposição das ordens de Deus na Terra e para defender a comunidade muçulmana dos infiéis. Se as regras de Deus estão sob ameaça, os jihadistas vêm a jihad não só como uma obrigação coletiva, mas também como um dever individual de todos os muçulmanos como qualquer outro ritual religioso (BBC, 2014).

Capítulo III

Segurança Interna e Terrorismo

Ao falar de segurança é inevitável não falar também em liberdade. O direito à liberdade e à segurança está plasmado na Constituição da República Portuguesa, no art. 27º. Estes dois conceitos constituem um binómio, já que abdicamos de parte da nossa liberdade em nome da segurança, enquanto que é a segurança que nos confere a liberdade. Assim, a liberdade e a segurança condicionam-se mutuamente e estão muitas vezes no centro de debates políticos, éticos e sociais.

Tal como supramencionado, a segurança interna é definida na Lei nº 53/2008 de 28 de agosto e refere-se a uma atividade da tutela do Estado na procura pela segurança e tranquilidade publicas e pela prevenção e repressão da criminalidade.

A sua ligação ao terrorismo é inegável já que, após o fim da Guerra Fria as grandes ameaças deixaram de ter atores e motivações bem definidas. Em consequência da globalização, da livre circulação de pessoas e bens e do desvanecer das fronteiras, as ameaças outrora externas passaram a ser da tutela de todos os Estados, nomeadamente dentro da União Europeia, nomeadamente, dentro do Espaço Schengen (Costa, 2016).

Neste sentido, o terrorismo e, mais concretamente o terrorismo de motivação jihadista, em conjunto com outro tipo de criminalidade (ex: tráfico de seres humanos, tráfico de armas, tráfico de estupefacientes, etc.) tem vindo, nos últimos anos a ameaçar a soberania dos Estados e à segurança pública. O terrorismo destaca-se pela sua imprevisibilidade e pela instabilidade do seu *modus operandi* e dos seus alvos (Costa, 2016).

Com isto, passaremos a analisar os textos legais existentes no nosso ordenamento jurídico que se dirigem à problemática do terrorismo.

Segundo a Decisão Quadro de 13 de junho de 2002 do Conselho da União Europeia, um grupo terrorista é qualquer organização composta por duas ou mais pessoas, prolongada no tempo, que atua com o intuito de cometer atos terroristas (Portela, 2009).

À semelhança da definição dada pela Decisão Quadro de 13 de Junho de 2002 do Conselho da União Europeia, também na lei nº 52/2003 de 22 de agosto do nosso ordenamento jurídico, é considerado *"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, forçar a autoridade pública a praticar um ato, a abster-se de o praticar ou a tolerar que se pratique, ou ainda a intimidar pessoas, grupos de pessoas ou a população em geral"* (Lei nº 52/2003 de 22 de agosto, 2003).

A Lei de Combate ao Terrorismo, retrata também de que forna este tipo de crime deve ser combatido. No nosso ordenamento jurídico, o terrorismo é visto segundos duas perspetivas: o da organização terrorista e o do terrorismo *stricto sensu*. Estes dois prismas em conjunto resultam no terrorismo tal como este é conhecido, a *"formação, promoção, adesão, apoio, chefia e direção de grupo terrorista (...) e (...) prática de atos terroristas individuais"* (Portela, 2009, pp. 492, 493).

Define ainda a moldura penal aplicável aos infratores de acordo com o seu grau de participação. Assim, e de acordo com o estatuído na Lei, "*quem promover ou fundar um grupo terrorista é púnico com pena de prisão de 8 a 15 anos; quem chefiar um grupo terrorista é punido com pensa de prisão de 15 a 20 anos; quem praticar atos preparatórios para a constituição de grupo terrorista é punido com pena de prisão de 1 a 8 anos"* (Lei nº 52/2003 de 22 de Agosto, 2003). No entanto, pode haver atenuação da pena quando existir um rompimento voluntário da atividade criminosa, fizer diminuir o perigo provocado por ela ou auxiliar as autoridades no decorrer da investigação, nomeadamente através da identificação ou captura de suspeitos ou da recolha de meio de prova (Lei nº 52/2003 de 22 de agosto, 2003).

A ameaça terrorista no território europeu

A União Europeia criou, em 2007, o *"Terrorism Situation and Trend Report (TE-SAT)"*. Trata-se de um relatório anual que caracteriza o fenómeno do Terrorismo na União Europeia,

nomeadamente através da análise do número de ameaças ou ataques realizados, ao número de detenções relacionadas com este tipo criminal, o perfil dos terroristas, entre outras informações.

Para este relatório, terrorismo implica atos violentos intencionais que, de acordo com a sua natureza e contexto, têm o poder de lesar profundamente um país ou organização internacional e o objetivo intimidar a população, forçar um governo ou organização internacional a realizar ou a abster-se de realizar atos, e, destabilizar ou destruir aa base política, constitucional, económico ou as estruturas sociais de um país ou organização internacional (Europol, 2020).

Apesar de todos os Estados Membros terem diretivas no que respeita à definição de terrorismo e à sua tipificação legal, existe uma grande ambivalência neste sentido entre os vários Estados Membros. Durante o ano de 2019, vários Estados Membros sofreram atos violentos extremistas que não foram investigados e julgados como atos terroristas por não se adequarem à tipificação legal nacional de Terrorismo (Europol, 2020).

Em 2019, dez pessoas perderam a vida e vinte e sete ficaram feridas em resultado de ataques terroristas de motivação jihadista na UE. Mais três pessoas morreram e várias outras ficaram feridas em dois grandes ataques extremistas violentos na Alemanha. Fora da União Europeia, dezassete civis originários de países que dela fazem parte morreram no Sri Lanka, no dia 21 de agosto de 2019 fruto de um ataque terrorista (Europol, 2020).

Passaremos agora, a nomear alguns dos ataques terroristas mais marcantes em território europeu nos últimos 10 anos.

De 11 a 19 de março de 2012, viveu-se um autêntico clima de terror em França. Mohamed Merah, um homem de 23 anos, matou três militares em Toulouse e Montauban nos dias 11 e 15 desse mês. No dia 19, tirou a vida a três crianças e um professor numa escola judaica. O individuo responsável por estes ataques foi morto pelas autoridades no dia 22 (JN, 2017).

A 07 de janeiro de 2015, Paris depara-se com a ameaça terrorista após um ataque à sede da revista *Charlie Hebdo,* perpetrado por dois irmãos em representação do Estado Islâmico. Este ataque vitimou 23 pessoas, das quais 12 perderam a vida (DN, 2019).

Apenas dois dias depois, quatro pessoas morrem num ataque a um supermercado na mesma cidade. O assaltante, que na véspera matara um polícia, tinha ligações ao autoproclamado Estado Islâmico (DN, 2019).

Desta vez em Copenhaga, é no dia 14 de fevereiro do mesmo ano que um dinamarquês de origem palestina fiel ao mesmo grupo terrorista supramencionado, atira sobre os presentes num centro cultural, acabando por tirar a vida a um cineasta, presente numa conferência cujo tema era a liberdade de expressão. Na mesma noite, tirou mais uma vida em frente a uma sinagoga. (DN, 2019).

A 13 de novembro de 2015, França enfrenta a maior onda de terror da sua história. Nessa noite, ataques terroristas simultâneos em diferentes locais (no Bataclan, nos arredores do estádio nacional e em bares e restaurantes de Paris), aterrorizam França e o resto da Europa. Destes ataques resultaram 130 mortos e mais de 350 feridos (DN, 2019).

Quase um ano depois, no dia 22 de março de 2016, são o metro de Maelbeek e o aeroporto de Zaventem, em Bruxelas, Bélgica, os novos alvos do Estado Islâmico. Nesse dia contaram-se mais de 34 vítimas mortais (JN, 2017).

14 de julho de 2016 ficou marcado como mais um dia negro da história francesa, após uma carrinha, dirigida por um tunisino, ter invadido a Promenade des Anglais, em Nice, resultando em 86 mortos e 450 feridos. Mais uma vez, é o EI que reivindica o ataque (DN, 2019).

Mais uma vez, França enfrente a ameaça terrorista a 26 de julho de 2016. Nesse dia, um padre foi degolado na sua igreja em Sant-Ettiene-du-Rouvray. Os agressores eram dois terroristas que se identificaram como membros do EI (JN, 2017).

Era época natalícia quando, a 19 de dezembro de 2016, um tunisino entra com uma carrinha num mercado de Natal em Berlim, ferindo 48 pessoas e tirando a vida a 12 (DN, 2019).

O tempo foi passando e o EI foi continuado a deixar a sua marca de terror por toda a Europa. Em 2017, no dia 22 de março, Londres foi apanhado de surpresa quando um britânico convertido ao islamismo e sob influencia do EI sobe o passeio da ponde de Westminster e esfaqueia um polícia que o abordara. Deste ataque resultaram cinco mortes (DN, 2019).

No dia 3 de fevereiro de 2017, um *lone wolf* atacou um grupo de soldados à porta de um dos museus mais conhecidos e movimentados de França, o Museu do Louvre (JN, 2017).

Em abril de 2017, mais precisamente do dia sete, um homem do Uzbequistão, avançou com a sua carrinha sobre uma rua no centro de Estocolmo, causando cinco vítimas mortais (DN, 2019).

No dia 22 de Maio de 2017, no final de um concerto da Ariana Grande em Manchester (cujo publico era sobretudo crianças e jovens), um atentado suicida tira a vida a 22 pessoas e fere 100. Mais uma vez, é o EI que assume a responsabilidade do ataque (JN, 2017).

Mais uma vez sob reivindicação do EI, três terroristas conduziram uma carrinha sobre a multidão na London Bridge e, de seguida, esfaquearam vários pedestres. Neste dia, a três de junho de 2017, oito pessoas perderam a vida em resultado deste ataque. (DN, 2019).

Desta vez em Barcelona, Espanha, no dia dezassete de agosto de 2017, uma carrinha avança sobre a multidão de pessoas que circulava nas Ramblas. A avenida mais turística de Barcelona passa a ser um cenário de terror, após a morte de quinze pessoas, entre as quais o motorista da carrinha. Umas horas mais tarde, cinco cúmplices deste primeiro ofensor, acionam um carro-bomba em Cambrils, no sul de Barcelona. É o EI que reivindica os ataques que causam 16 mortos e 125 feridos (DN, 2019).

A 18 de Agosto de 2017, em Turku, Finlândia, um homem com afiliação ao EI mata duas pessoas e fere oito (DN, 2019).

2018 volta a trazer o terror a França, quando a 23 de março, um homem pertencente ao EI mata quatro pessoas e fere quinze em ataques em Carcassonne e Trebes (DN, 2019).

No mesmo ano, a Bélgica é também mais uma vez alvo do autoproclamado Estado Isâmico. A 28 de maio, um homem matou dois policias e um estudante em Liège (DN, 2019).

11 de dezembro de 2018, é mais um dia trágico. Neste dia, um homem fiel ao EI, matou cinco pessoas e feriu outras doze num mercado natalício em Estrasburgo, França (DN, 2019).

Já em 2020, O EI continuou a deixar a sua marca de terror pela Europa. França continuou a ser alvo do crime do terror. A 16 de outubro, um professor de História foi decapitado por um jovem de 18 anos. O motivo do crime terá sido umas caricaturas de Maomé numa aula sobre liberdade de expressão. Poucas semanas mais tarde, é na basílica de Notre-Dame que um ataque de motivação islamista tira a vida a três pessoas e feriu muitas outras (Público, 2020).

No dia 3 de novembro de 2020, dá-se um ataque terrorista em Viena. Um "jihadista libertado" vitimiza vinte e seis pessoas, das quais quatro perderam a vida (Público, 2020).

Para dar resposta a esta ameaça que não conhece fronteiras, a União Europeia definiu algumas diretrizes neste domínio. Foi definido que deveria existir um melhor intercâmbio de informações, o reforço dos controlos fronteiriços, a prevenção da radicalização em linha, um

maior controlo no que respeita às armas de fogo, a dinamização da cooperação judiciaria (nomeadamente através da digitalização e partilha de dados), a criminalização do terrorismo, o corte do financiamento dos grupos e organizações terroristas, maior controlo do dados dos passageiros de transportes aéreos e o reforço da cooperação entre os estamos-membros (Conselho Europeu, 2021).

Atualmente, a União Europeia está a estudar novas formas de recolher, partilhar e utilizar informações entre as diferentes forças de segurança. Em 2019 o Conselho Europeu aprovou dois novos regulamentos, criando assim um quadro para a interoperabilidade entre os sistemas de informação da UE. Esta nova realidade deverá estar pronta em 2023 e vai permitir que exista um único serviço com informações biométricas que permitem identificar indivíduos (Conselho Europeu, 2021).

Uma vez que o terrorismo é uma ameaça poderosa, imprevisível e transfronteiriça a Europol criou, em Janeiro de 2016, o Centro Europeu de Luta contra o Terrorismo (CELT). O CELT providencia suporte operacional quando a UE assim o requer para questões de investigação, auxilia o combate a combatentes estrangeiros, partilha informações e conhecimentos no que diz respeito ao financiamento do terrorismo, estuda a propaganda terrorista e extremista online, debruça-se sobre o trafico de armas ilegais e atua na cooperação internacional entre agências de combate ao terrorismo (Europol, 2021).

Em 2019, houve cento e dezanove ataques terroristas falhados, abortados ou perpetrados na Europa e mil e quatro pessoas foram detidas por infrações terroristas (Conselho Europeu, 2021).

O contexto prisional tem preocupado os Estados Membros da UE no que diz respeito à radicalização dentro dos estabelecimentos prisionais. Tem havido a denuncia de vários países de reclusos que se radicalizem durante o cumprimento da sua pena por outros crimes e, muitos destes, estão prestes a ser libertados constituindo assim uma ameaça grave para a segurança interna dos Estados. A Holanda está especialmente preocupada com a radicalização jihadista, tal como Espanha. Por sua vez, a Dinamarca tem uma outra preocupação relacionada com as relações estabelecidas dentro das prisões entre jihadistas e membros de organizações criminosas, pelo risco agravado de um maior acesso a armas e a financiamento (Europol, 2020).

O fenómeno do terrorismo em Portugal

Tal como foi anteriormente referido, os conceitos segurança e liberdade têm uma relação de interdependência, já que teremos de abdicar de parte da nossa liberdade para viver em segurança e vice-versa.

Apesar de, na era moderna, a ameaça terrorista não se manifestar no nosso território nacional, a verdade é que nem sempre foi assim. Durante a III república, Portugal foi palco de vários atos terroristas que puseram em causa a paz e a tranquilidade publicas. O primeiro evento refere-se a agentes internos que, durante o período revolucionário cometeram vários crimes por motivações politico-ideológicas; segue-se o período jurídico-constitucional, pautado pelos crimes cometidos por agentes internos, mais uma vez por razoes politico-ideológicas; em 1979, o embaixador de Israel em Portugal, foi vitima de uma tentativa de homicídio levada a cabo pela Organização Nasserista para a Libertação dos Presos no Egipto; mais tarde, no ano de 1983, dá-se o assassinato do representante da Palestina ao congresso internacional em Montechoro, levado a cabo por um comando extremista palestiniano da Abu Nidal; em julho do mesmo ano, um atentado levado a cabo por uma fação do Exército Revolucionário Arménio contra a Embaixada da Turquia em Portugal, tira sete vidas, incluindo a mulher de um diplomata (Gouveia, 2018).

Estes acontecimentos, tiveram um impacto na própria Constituição da República Portuguesa (CRP), introduzindo a possibilidade de extradição de nacionais no âmbito de crimes de terrorismo e criando a possibilidade de entrar em residências durante a noite, sem consentimento, em situação de flagrante delito ou autorização judiciaria em caso de crimes graves, nomeadamente, de terrorismo. Resultou ainda na exclusão da possibilidade de julgamento com recurso a júri nos crimes de terrorismo, uma vez que este tipo de criminalidade tem um grande impacto emocional no público, podendo afetar a imparcialidade e a independência do mesmo (Gouveia, 2018).

Apesar dos acontecimentos supramencionados terem acontecido num passado distante, isto não significa que não se poderão repetir, até porque, tal como já foi mencionado, as características do terrorismo moderno tornam-no uma ameaça imprevisível e suscetível a qualquer espaço e tempo. Desta forma, passaremos a analisar o regime jurídico relativo ao Terrorismo em Portugal.

Tal como supramencionado, a segurança interna é definida na Lei nº 53/2008 de 28 de agosto e refere-se a uma atividade da tutela do Estado na procura pela segurança e tranquilidade publicas e pela prevenção e repressão da criminalidade.

Assim como os restantes Estados Membros, Portugal teve de seguir os princípios definidos pela Decisão Quadro nº 2002/475/JAI do Conselho, de 13 de junho da União Europeia no âmbito do combate ao terrorismo.

Esta Decisão Quadro oferece alguma liberdade aos Estados Membros para definirem as sanções penais relativas ao terrorismo e a crimes a ele relacionados, de acordo com o próprio ordenamento jurídico. No entanto, define as motivações que tornam algumas ações atos terroristas, desde que "pela sua natureza ou pelo contexto em que foram cometidos, sejam suscetíveis de afetar gravemente um país ou uma organização internacional" (Decisão-Quadro nº 2002/475/JAI do Conselho, de 13 de junho).

Segundo a Decisão Quadro de 13 de junho de 2002 do Conselho da União Europeia, um grupo terrorista é qualquer organização composta por duas ou mais pessoas, prolongada no tempo, que atua com o intuito de cometer atos terroristas (Portela, 2009).

Podemos verificar que esta norma legal não oferece uma definição clara e sucinta de terrorismo, o que acaba por resultar numa ambiguidade que se reflete no direito penal de cada país.

É a partir deste texto legal que Portugal cria, em 2003, a Lei nº 52/2003 de 22 de agosto, também conhecido por Lei de Combate ao Terrorismo. O objeto desta lei é a previsão de punição de atos e organizações terroristas.

À semelhança da definição dada pela Decisão Quadro de 13 de Junho de 2002 do Conselho da União Europeia, também na lei nº 52/2003 de 22 de agosto do nosso ordenamento jurídico, é considerado "*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, forcar a autoridade pública a praticar um ato, a abster-se de o praticar ou a tolerar que se pratique, ou ainda a intimidar pessoas, grupos de pessoas ou a população em geral"* (Lei nº 52/2003 de 22 de agosto, 2003).

É também definido terrorismo como a prática dos atos enumerados no artigo 2º da mesma lei (relativo às organizações terroristas) e é definida a moldura penal correspondente (Lei nº 52/2003 de 22 de agosto, 2003).

Por fim, é importante mencionar que também é retratada a aplicação desta lei no espaço. Assim, salvo tratado ou convenção em contrário, esta lei é aplicável a factos cometidos no estrangeiro quando se referir aos crimes previstos nos artigos 2º e 4º (Organizações terroristas e Terrorismo), e, quando constituírem os crimes previstos nos artigos 3º e 5º (Outras organizações terroristas e Terrorismo Internacional), desde que o agente do crime seja encontrado em território nacional e não haja a possibilidade extradição ou exista um mandado de detenção europeu (Decisão-Quadro nº 2002/475/JAI do Conselho, de 13 de junho).

Contudo, esta lei foi alvo de enumeras alterações ao longo dos anos, o que é comum já que o Direito Penal acompanha o desenvolvimento social e as necessidades sociais.

A primeira alteração acontece em Outubro do mesmo ano, no entanto, não altera o conteúdo legal, mas antes a sua estrutura. Mais tarde, em 2007 dá-se uma alteração importante no texto legal, acrescenta-se, no artigo 8º, o número 2 que acrescenta que aos crimes previstos na alínea a) (Organizações terroristas e Terrorismo) do número anterior não é aplicável o nº2 do artigo 6º (referente às restrições à aplicação da lei portuguesa) do código penal.

No entanto, a primeira grande alteração é feita em 2008, quando é acrescentado o artigo 5º. -A, relativo ao financiamento do terrorismo. Assim, quem, direta ou indiretamente, fornecer, recolher ou detiver fundos, produtos ou direitos com a intenção de financiar a preparação ou a prática de atos terroristas, passa a incorrer num crime cuja moldura penal é 8 a 15 anos de pena de prisão.

Em 2011, entram para o artigo 4º desta lei (relativo ao terrorismo), três novos factos. Passa a ser crime a difusão de mensagem incitante à prática de atos terroristas ou associação a organização ou grupos terroristas, o recrutamento para a prática dos mesmos factos passa também a estar consagrado neste artigo. Por último, o treino e a instrução de pessoas para o fabrico ou utilização de explosivos, armas de fogo ou armas e substâncias nocivas e perigosas ou outras técnicas para a prática do terrorismo passam também a integrar o artigo 4º.

Quatro anos mais tarde, fruto das novas necessidades sociais e penais, o artigo 4º volta a sofrer acréscimos. Desta vez, dá-se enfoque aos meios de comunicação eletrónica e online na difusão de mensagens que incitam à violência; passa-se a penalizar também o acesso às

mensagens anteriormente referidas com o objetivo de ser recrutado para uma organização terrorista, e delas fazer uso na pratica de atos preparatórios; é também reconhecido como crime relacionado com terrorismo a utilização dos meios de comunicação, entre eles a comunicação social, para a recompensa e o louvar de grupos ou organizações terroristas; passa-se a penalizar também as viagens ou a tentativa de viajar para outro território com o intuito de usufruir de treino, apoio ou instrução para a pratica dos factos previstos nesta lei, bem como, a viagem ou tentativa de viagem para oferecer treino, suporte ou instrução para a prática dos mesmos factos; a adesão ou tentativa de adesão a uma organização terrorista através de viagem para fora do território nacional e a organização, financiamento ou facilitação das viagens anteriormente referidas englobam também este artigo 4º.

Ainda na mesma alteração supramencionada, é acrescentado o artigo 6.º -A, intitulado de "Comunicação de decisão final condenatória". Neste artigo, passa a estar definido que os tribunais devem enviar à Unidade de Coordenação Antiterrorismo as certidões das decisões finais condenatórias proferidas pelos factos de terrorismo, organizações terroristas, terrorismo internacional e financiamento do terrorismo.

Neste momento, a lei de combate ao terrorismo mantém-se, no entanto, o seu objeto mudou. Atualmente, esta lei pretende prever e punir os atos e organizações terroristas, fazendo cumprir a Diretiva da EU 2017/541 do Parlamento Europeu e do Conselho de 15 de março de 2017, que vem substituir a anterior Decisão-Quadro 2002/474/JAI do Conselho e alterar a Decisão 2005/671/JAI do Conselho. Para além disto, no artigo 5.º -A, nº 2 acrescenta-se que a recolha, fornecimento ou detenção de fundos para apoio na preparação ou prática dos factos punidos pela lei em questão, é punível bastando que o agente tenha consciência de que o seu destino são organizações terroristas ou terroristas que atuem individualmente.

É importante referir também que a Estrutura Nacional de Combate ao Terrorismo (ENCT), foi introduzida pela Resolução do Conselho de Ministros nº 7-A/2015, de 20 de fevereiro. Impulsionada pelas estratégias europeias de combate ao terrorismo, a ENCT tem por objetivos (Gouveia, 2018):

1. Detetar, isto é, identificar potenciais ameaças;
2. Prevenir, identificando e atuando nas causas da radicalização, do recrutamento e do terrorismo;
3. Proteger, fortalecendo a segurança de potenciais alvos;

4. Perseguir, através da neutralização e destruição de organizações terroristas, financiadores, redes de apoio, etc...;
5. Responder, através da utilização dos meios necessários para a resposta à ameaça terrorista.

Outro texto legal relevante, é a Resolução do Conselho de Ministros nº88/2015, de 8 de outubro. Esta Resolução cria a Comissão de Coordenação das Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo. O objetivo é prevenir e responder aos crimes de branqueamento de capitais e de financiamento do terrorismo (Resolução do Conselho de Ministros nº 88/2017, 2015).

A Lei nº 61/2015, de 24 de junho, traz também alterações importantes, já que vem permitir a realização de ações encobertas no contexto de crimes relacionados com o terrorismo. As ações encobertas são desenvolvidas por funcionários da investigação criminal ou por terceiros que atuem sob o controlo da Polícia Judiciária na prevenção ou na repressão de crimes; são chamadas de "encobertas" porque a sua identidade e qualidade são ocultadas. Estas ações podem acontecer no âmbito da investigação criminal, através de autorização prévia do Ministério Público (MP), ou para a prevenção criminal quando é o juiz de instrução criminal que as autoriza mediante proposta do MP (Gouveia, 2018).

Em 2017 surge mais um texto legal importante, a Lei de Combate ao Branqueamento de Capitais e Financiamento do Terrorismo. A Lei nº 83/2017, de 18 de agosto, estabelece medidas preventivas e repressivas para o combate ao branqueamento de capitais e ao financiamento do terrorismo *(Lei nº 83/2017, de 18 de agosto, 2017)*.

Outra alteração relevante, surge com a Lei de acesso a dados de comunicação eletrónicas para a repressão de crimes graves. Através desta lei, as empresas de comunicações eletrónicas ou de uma rede pública de comunicações vêm-se obrigada a preservar durante um ano os dados de comunicações a que têm acesso. Em caso de necessidade, estes dados devem ser fornecidos às autoridades judiciárias e/ou policiais, mediante decisão do juiz de instrução (Gouveia, 2018).

A evolução da lei criminal é especialmente evidente na análise da legislação portuguesa direcionada ao combate do terrorismo. Como podemos ver ao longo nesta análise, a lei penal foi-se desenvolvendo e transformando de modo a dar resposta aos novos contornos que se foram criando em torno desta ameaça. O direito penal acompanha as transformações sociais, resultando em movimentos de descriminalização e neocriminalização. Dias e Andrade (2013,

p. 398), assemelham o direito penal *"àquelas árvores que constantemente perdem folhas velhas e geram novas folhas".*

As transformações tecnológicas, sociais e económicas, bem como todas as outras que todos os dias alteram o mundo e a sociedade, obrigam a novos ajustes nos diferentes setores sociais, incluindo o da lei penal. O terrorismo, apesar de ser um fenómeno antigo, surge também de um movimento de neocriminalização, pelo menos no contexto ocidental, e enquanto uma ameaça que transcende fronteiras e ameaça os valores da comunidade internacional (Dias e Andrade, 2013).

Capítulo IV

Radicalização

A criminologia vê o homem como um ser biopsicossocial, o que significa que as suas características individuais (biológicas e psicológicas), aliadas ao contexto social e económico em que está inserido podem facilitar a adoção de comportamentos criminais, nomeadamente terroristas. Assim, é esta preocupação pelo entendimento do comportamento criminoso que leva à procura do entendimento da radicalização, tentando responder a perguntas como: Quem? Como? Porquê?

O termo "radical" era utilizado no sec. XVIII, relacionado com a revolução francesa e americana. Radical representava também os representantes ou apoiantes de um setor extremo da sociedade (Schmid, 2013).

Segundo Schmid, o conceito "radicalismo" pode ser descrito através de dois elementos principais: pensamento/atitude e ação/comportamento, respetivamente:

- Baseado na convicção de que o estado das coisas é inaceitável, e ao mesmo tempo parece não existir uma alternativa suficientemente satisfatória;
- Os meios utilizados para alcançar a mudança pretendida no sistema e na sociedade podem não ser violentos (persuasão e reforma política) ou ser violentos (coerção e revolução). Isto significa que um radical não tem, necessariamente, de ser violento, apesar de partilhar características em comum com extremistas que o são.

Apesar de vermos comumente a palavra "radicalização" na literatura relativa à problemática do terrorismo ou nos media, a verdade é que não existe ainda uma definição clara da mesma, o que torna este termo complexo e controverso. Desde 2004 que este é um termo central em estudos e legislações relativas ao terrorismo e ao contraterrorismo, no entanto, a ausência de uma definição clara e universal resulta numa panóplia de significados atribuídos a este termo, tal como já foi mencionado (Schmid, 2013).

A radicalização pode ser definida como um processo individual ou coletivo através do qual, normalmente numa situação de polarização política, o diálogo e a tolerância entre atores políticos são abandonados, para dar lugar a um conflito com recurso a técnicas de pressão e coerção, várias formas de violência, tais como o terrorismo e os crimes de guerra. Este processo acontece do lado das fações rebeldes, geralmente acompanhado por uma socialização ideológica afastada das posições comuns da sociedade, ou seja, direcionadas para posições radicais e extremistas opostas à ordem política dominante, já que esta mesma ordem não é considerada apropriada ou legítima (Schmid, 2013).

Já o *US Department of Homeland Security* (DHS), define radicalização enquanto um "processo de adoção de um sistema de crenças extremista, incluindo disponibilidade para usar, apoiar ou facilitar atos de violência, como um método para alcançar mudança social" (Schmid, 2013).

A Comissão Europeia entende radicalização enquanto "o fenómeno de pessoas que embarcam em opiniões, pontos de vistas e ideias que podem levar a atos de terrorismo" (Schmid, 2013).

A radicalização pode também ser descrita como um processo de socialização através do qual o individuo desenvolve ideias, crenças e atitudes políticas, religiosas, ambientais, económicas e outras, que o levam a criar uma visão do mundo e da sociedade, comum apenas a um pequeno grupo de pessoas e não à sociedade em geral (Carter & Carter, 2011).

Peter Neumann descreve este fenómeno como: *"what goes on before the bomb goes off"* (Schmid, 2013, p. 6). Ou seja, todos os acontecimentos que decorrem na vida do individuo e que culminam no ataque terrorista.

Quando falamos daquilo que leva um individuo a ser radicalizado, podemos estar a falar de fatores de diferentes níveis: micro, meso e macro (Schmid, 2013).

Os fatores micro dizem respeito a questões individuais, como por exemplo, problemas de identidade, desintegração social, sentimentos de alienação, vingança e raiva, rejeição, entre outros (Schmid, 2013).

No nível meso, falamos do meio que envolve o individuo, que pode ser mais ou menos conivente com as intenções violentas, por exemplo estar inserido num grupo que se sente injustiçado e desenvolve sentimento de vingança e com ligações a grupos terroristas (Schmid, 2013).

E, no nível macro, destaca-se o papel do governo e da sociedade em geral: problemáticas como a discriminação de minorias étnicas e religiosas, falta de oportunidades socioeconómicas, entre outros fatores, levam alguns setores da sociedade a serem radicalizados como consequência do descontentamento e da frustração que sentem (Schmid, 2013).

Estes níveis de fatores que propiciam a radicalização deixam-nos mais próximos de compreender as causas sociopsicológicas deste fenómeno. Contudo, a investigação diz-nos que não há uma causa única para o processo de envolvimento em atividades terroristas, mas antes um conjunto de fatores de risco que podem levar alguns indivíduos à radicalização e a comportamentos extremistas (Schmid, 2013).

A radicalização pode ser dividida em dois tipos: a radicalização cognitiva e a radicalização violenta. No que diz respeito à radicalização cognitiva, esta trata-se de um processo durante o qual o individuo se distancia dos ideais sociais e passa a adotar ideias que contrapõem os primeiros. Já a radicalização violenta, acontece quando existe uma alteração de crenças e sentimentos que levam a adoção de comportamentos violentos (Prates, 2018).

Podemos também falar em "radicalização de opinião" e "radicalização de ação" tal como referem McCauley & Moskalenko, 2017. Assim temos duas pirâmides: na pirâmide da radicalização de opinião temos os indivíduos que se encontram na base, denominados de *neutral*, seguindo-se os *sympathizers*, que simpatizam com a causa, mas não justificam a violência; depois, os *justifiers*, que acreditam que a violência é justificada em nome da causa; e, por fim, aqueles que se sentem na obrigação de lutar, usando a violência, para defender a causa.

Já na pirâmide da radicalização de ação, começamos por encontrar na base aqueles que nada fazem pela causa *(inerts)*; depois, os indivíduos que aderem à causa *(activists)*, de seguida

encontramos aqueles que agem ilegalmente em prol da causa *(radicals)*; e, finalmente, os *terrorists*, que agem através de ataques violentos a civis (McCauley & Moskalenko, 2017).

Neste modelo, os indivíduos podem mover-se entre os diferentes níveis, ascendente ou descendentemente.

Fig. 1 - Modelo das 2 Pirâmides de McCauley & Moskalenko

(Fonte: Prates, 2018)

Segundo a abordagem *"The staircase to terrorism*" de Moghaddam, a radicalização assemelha-se a uma escada de seis pisos, que se vai estreitando; as ações terroristas encontram-se no último piso. O individuo sobe ou não de piso, dependendo das recompensas que acredita que lhe esperam no piso seguinte. Quanto mais sobe, menos opções de escolha lhe restam, até chegar à sua destruição e à do próximo (Prates, 2018).

No piso Térreo encontram-se os indivíduos que se limitam a uma sensação de injustiça e desigualdade; segue-se o primeiro piso, com indivíduos que começam a procurar soluções para a injustiça percecionada; no *Piso 2* há uma projeção da raiva para aqueles que culpa pela sua insatisfação; no *Piso 3*, estão aqueles que aderiram moralmente ao Terrorismo, vendo-o como justificável; seguidamente, no *Piso 4*, os que se juntam a um grupo ou organização terrorista; no *Piso 5*, aqueles que desumanizam os seus alvos e lhe direcionam atos de violência (Prates, 2018).

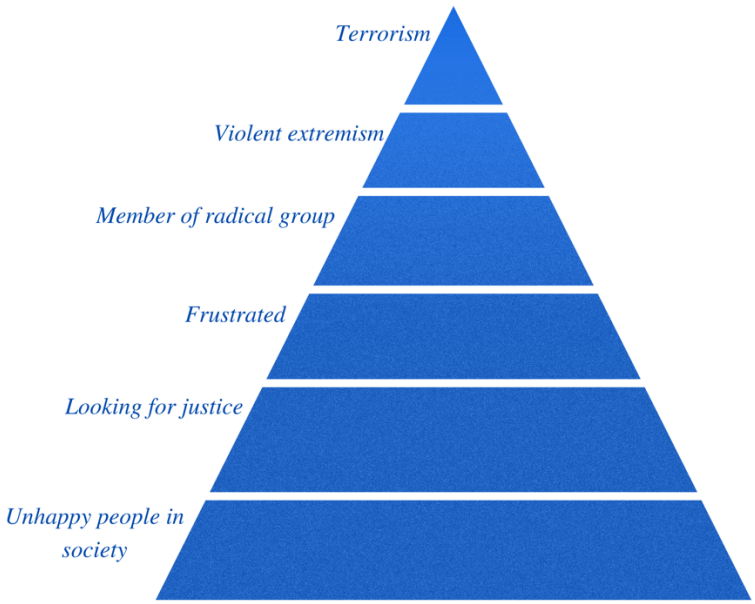


Fig. 2 Modelo "escada" de Moghaddam

A "Teoria da Gestão do Terror", afirma que "*todos os que se identificam com um grupo vão responder à violência dirigida a esse grupo com um maior empenho para o grupo e maior apoio à violência contra aqueles que ameaçam o grupo".* Ou seja, existe uma dinâmica de ação-reação entre aqueles que perpetuam a violência e aqueles que a vivenciam (Prates, 2018).

Os *"lone wolves"* são uma das maiores preocupações dos países e das agências de segurança, já que se tratam de indivíduos muitas vezes naturais do país alvo, que se radicalizam de forma independente e sem afiliações a grupos ou organizações terroristas, o que levanta vários obstáculos à sua identificação.

Só no período de um ano, entre 2009 e 2010, o ritmo de aparecimento de *"lone wolves"* cresceu significativamente com vários ataques e tentativas de ataque (Carter & Carter, 2011).

No fundo, estes indivíduos passam por um processo de ressocialização, já que estas novas crenças, atitudes e ideias são incompatíveis com a sua vida prévia (Carter & Carter, 2011).

Alguns especialistas acreditam que o processo de radicalização nestes indivíduos se divide em quatro etapas:

A primeira relativa à pré-radicalização, ou seja, ao estilo de vida do individuo antes da radicalização (as suas relações, o ambiente onde vive, trabalho, vida social…);

Depois, a autoidentificação, quando o individuo é influenciado por fatores internos e externos que o fazem explorar as filosofias, ideologias e valores extremistas.

Em terceiro lugar, a doutrina, quando as crenças se intensificam e é adotada uma filosofia, ideologia e valores extremistas.

Por último, a fase do soldado, isto é, quando o individuo aceita o seu dever de participar, enquanto soldado, na luta contra aqueles que vão contra a sua ideologia, numa tentativa de alcançar a realização (Carter & Carter, 2011).

O *Radicalisation Awareness Network* (RAN), alerta para a necessidade de mais estudos relativos às causas, processos, mecanismos de radicalização e medidas preventivas, bem como a urgência de se conhecer melhor a dinâmica da radicalização, do extremismo e do terrorismo. Outras preocupações passam por perceber o impacto dos conteúdos audiovisuais disseminados pelos grupos terroristas e pelos seus simpatizantes. O RAN preocupa-se também com a discordância ainda existente no que diz respeito a conceitos chave como terrorismo e radicalização e a falta de relevância dada a áreas do conhecimento como a criminologia, a sociologia e outras. Ressalta ainda a necessidade de haver uma avaliação continua de programas de prevenção ou desradicalização que devem ser implementados. Para além disto, a comparação entre os diferentes tipos de terrorismo e a falta de cooperação entre as diferentes agências com competências para este tipo de criminalidade põem também em risco o sucesso do contraterrorismo.

Em Portugal, a Estratégia Nacional de Combate ao Terrorismo (ENCT), estabelece os objetivos de detetar, prevenir, proteger, perseguir e responder à radicalização e engloba o Plano de Ação de Prevenção da Radicalização e do Recrutamento para o Terrorismo. Esta estratégia pretende ainda um melhor diálogo inter-religioso e intercultural (Gouveia, 2020).

A Deteção Comportamental

O tema abordado por este estudo, implica várias questões do foro da segurança interna e da investigação criminal e, está, por isso, protegido por bastante confidencialidade. Assim, a literatura disponível sobre Deteção Comportamental é escassa e revelou-se um obstáculo na realização desta fase do estudo. Contudo, os poucos documentos disponíveis destacam-se pela

riqueza de informação que dispõem, nomeadamente, o guia de boas práticas do governo Britânico. E, será esse o principal documento a ser analisado nesta secção.

O governo britânico entende deteção comportamental como um método de deteção de pessoas com intenções hostis a partir da observação dos seus comportamentos e atitudes. De modo a alertarem para a relevância deste método elaboraram um guia realizado por especialistas com o auxílio de consultores, especialistas externos, pesquisa, literatura e outras partes interessadas. O objetivo é dar indicações de como utilizar a deteção comportamental no contexto da prevenção do terrorismo.

Para os especialistas da deteção comportamental, algumas pessoas com intenções hostis[1] irão transparecê-lo através de comportamento e atitudes; membros de equipas de segurança, sejam elas de natureza pública ou privada, podem ser treinados para as detetar; e, a deteção comportamental pode ser utilizada para prevenir hostilidades e para dar uma sensação de segurança à comunidade. Para além disto, realçam também o potencial deste método na deteção de pessoas em sofrimento ou a necessitar de auxílio, nomeadamente, quando se encontram perdidas, a sofrer algum surto psicológico ou pensamento desorganizado, quando estão a ter pensamentos suicidas, entre outras (HM, Government, 2020).

Quem defende este método afirma que, quando integrado com outros métodos e/ou técnicas de segurança, a deteção comportamental tem um grande potencial e revela-se uma ferramenta poderosa que pode ser utilizada num leque variado de contextos como parte de uma abordagem sistémica para neutralizar criminosos e terroristas. Esta disrupção pode acontecer através da deteção de indivíduos com reconhecimento hostil, impedindo os atores de alcançarem o seu alvo e impedindo que os criminosos tenham acesso a informações necessárias para o planeamento de ataques (HM, Government, 2020).

Os ataques de 11 de setembro de 2001 surpreenderam todos os Estados no que diz respeito à evolução nas táticas utilizadas por extremistas violentos para matar, causar danos e instalar o medo. Estas alterações nas táticas de ataque utilizadas pelos grupos, organizações ou indivíduos terroristas, obrigou a uma revisão das políticas e das medidas de prevenção de modo

[1] Entende-se por hostil, alguém que tenciona realizar um ataque ou interferir com uma organização e a tranquilidade pública para benefício próprio ou para expressar uma ideologia. Já o reconhecimento hostil, passa pela observação com o intuito de fornecer informações que contribuem para o planeamento de um ato contra um alvo específico. Outro termo relevante é a intenção hostil, isto é, quando a pessoa hostil tem a intenção de concretizar a sua vontade HM Government, 2020)

a darem uma resposta adaptada à ameaça atual. O NSI *(National Suspicious Activity Reporting Initiative)* enfatiza a necessidade de se reportar, analisar e reter informações relativas a comportamentos suspeitos observados, de modo a serem utilizadas pelas forças de segurança nos seus esforços para travar o terrorismo. Esta informação é, nos Estados Unidos, conhecida por *"Suspicious Activity Reports"* (SARs), um programa que funciona muito por conta da parceria que existe entre a comunidade e as forças de segurança. Ou seja, muitas das informações adquiridas são reportadas por membros da própria comunidade (Carter & Carter, 2011).

No caso do SARs, a comunidade é informada de comportamentos que podem indicar suspeitas através de indicadores de probabilidade, contudo, para que estes indicadores existam tem de haver um padrão de comportamentos (Carter & Carter, 2011).

Os *Suspicious Activity Reports* tratam-se da simples documentação de comportamentos observados que tenham levantado suspeitas do cometimento de qualquer crime. Contudo, existe um tipo SAR específico para os comportamentos relativos ao terrorismo ou crimes que sustentem ou facilitem o cometimento de ataques terroristas. Este SAR chama-se *Information Sharing Environment – Suspicious Activity Report* (ISE-SAR) (Carter & Carter, 2011).

É este tipo de SAR que contém tem mais potencial para a identificação de terroristas que se radicalizaram sozinhos, os *lone wolves* (Carter & Carter, 2011).

Uma característica fundamental da implementação de este tipo de documentação (SAR) é o compromisso com a proteção da privacidade dos cidadãos, bem como o respeito pelos seus direitos e liberdades civis. Por este método se focar em comportamento observado, mitiga o risco de traçar um perfil com base nas características raciais, étnicas ou religiosas dos indivíduos (Carter & Carter, 2011).

A Austrália adotou uma estratégia semelhante, criando parcerias com as entidades privadas que fazem a segurança nos aeroportos. Também a polícia de Israel e a polícia turca desenvolveram uma parceria comunitária para recolherem informações a partir da comunidade relativamente a atividade suspeita relacionada com terrorismo (Carter & Carter, 2011).

Ainda relativamente ao comportamento observado pelos membros da comunidade existe o programa americano *"See something, Say something"*, lançado em julho de 2010. Este programa utiliza materiais educativos públicos, publicidade e outras ferramentas para informar

e envolver turistas, negócios, organizações comunitárias e os funcionários dos setores públicos e privados a identificarem comportamentos suspeitos (Carter & Carter, 2011).

Contudo, os especialistas também reconhecem que a Deteção Comportamental não é a única abordagem disponível para neutralizar aqueles que pretendem proliferar o terror. Antes, vêm-na como parte integrante do Modelo de Rutura dos 3DS *(The 3Ds disruption model)*. Este modelo é composto por três dimensões: a negação *(deny)*, nesta fase as organizações adotam medidas preventivas, de modo a impedirem o acesso a informações vitais que possam ser utilizadas no planeamento de um ataque terrorista, para isto podem, por exemplo, ser mais seletivas na informação que dispõem online ou preparar o seu staff para intervir em situações de suspeita. Segue-se a deteção *(detect)*, que passa pela implementação de medidas de segurança e pelo desenvolvimento de estratégias que facilitem a deteção de pessoas ou atividades suspeitas, é neste momento que a Deteção Comportamental entra; por último, a dissuasão *(deter),* que é alcançada através de comunicação corporativa, a comunicação é essencial, uma vez que pode ser utilizada para dissuadir os potenciais ofensores, bem como para assegurar e informar a população (HM Government, 2020).

Para a aplicação da Deteção Comportamental, é necessário a formação de especialistas nesta abordagem, contudo, um público vigilante pode ser um fator multiplicador de forças na identificação de comportamentos suspeitos. Este público pode incluir a população em geral, em especial agentes das forças de segurança e funcionários da segurança privada. No Reino Unido, o *Centre for the Protection of National Infrastucture (CPNI)* criou o modelo de efeito e alcance *(effect and reach)*, que demonstra a utilização do público como recurso para a deteção de ameaças. No topo da pirâmide estão aqueles que são mais treinados e com formação mais especializada no âmbito da deteção comportamental, e quanto mais nos aproximamos da base da pirâmide encontrados aqueles que menos formação/treino têm, sendo que no último degrau se encontra a comunidade civil (HM Government, 2020).

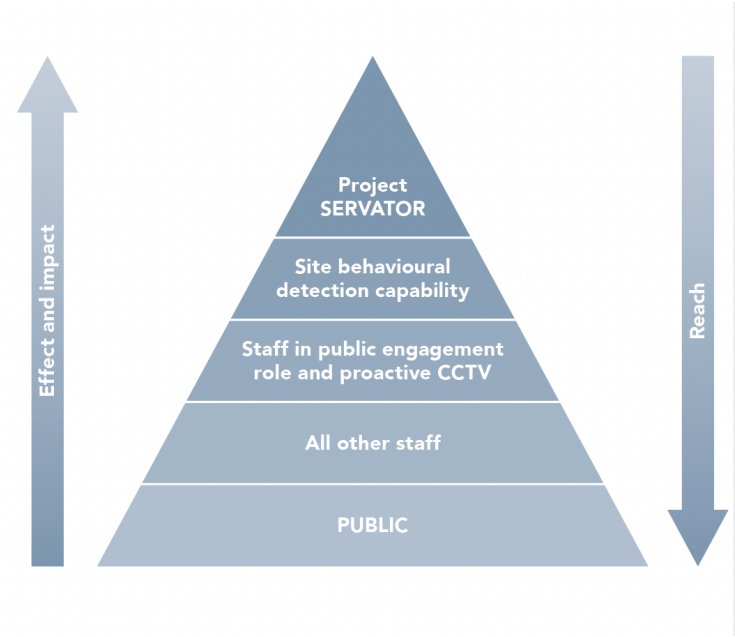


Fig. 3 Modelo "effect and reach" de CPNI

(Fonte: HM government, 2020)

Dentro do conceito amplo de Deteção Comportamental podemos dividi-lo eu dois tipos: a deteção passiva, isto é, identificar comportamentos e atividades suspeitas, como por exemplo alguém que se está a comportar de forma inadequada ou que foge à norma num determinado contexto; e, a deteção ativa, ou seja, a utilização do próprio contexto para evocar receio em indivíduos com intenções hostis de serem detetado e identificados, por exemplo, através da colocação de seguranças na entrada e na saída dos recintos (HM Government, 2020).

Passemos a analisar diferentes programas e situações em que a deteção comportamental é utilizada e a descrição dos seus atores.

Comecemos pelo projeto SERVATOR. Este projeto, implementado por várias forças de segurança no Reino Unido e na Nova Gales do Sul, na Austrália, tem como objetivo neutralizar um leque variado de atividades criminais, incluindo o terrorismo. Esta iniciativa tem por base um estreitamento da relação entre a polícia e a comunidade, de modo a que exista uma rede integrada de vigilância e de reporte de informações. Este projeto é implementado em vários contextos, tais como: centros comerciais, aeroportos, locais turísticos, etc. Pode incluir também medidas visíveis, como policias uniformizados, cães e cavalos, ou medidas não visíveis, por exemplo, agentes não identificados (Counter Terrorism Policing, 2021).

Os agentes de deteção comportamental são treinados com alto nível de rigor para identificar comportamentos ou atitudes suspeitas. Durante o seu treino, aprendem uma lista de

sinais que podem ser comportamentos ou indicadores de preocupação que podem ser verbais, ou seja, o que alguém diz ou não diz, e, não verbais, entre eles as expressões faciais e movimentos corporais (HM Government, 2020).

Segue-se o projeto SCaN, do Reino Unido, que foi desenvolvido para auxiliar as organizações e empresas assegurarem a sua segurança, partindo do princípio de que as pessoas representam a melhor vantagem na prevenção de ameaças, nomeadamente, do terrorismo. O treino proporcionado por este projeto, torna as pessoas capazes de identificarem ameaças e de como agir perante as mesmas. Para além disso, dota os indivíduos de conhecimentos de como proteger as suas informações (Centre for the Protection of National Infrastructures, 2021).

A história da segurança dos aeroportos americanos, permaneceu inalterada durante várias décadas. As medidas de segurança implementados nos aeroportos dos Estados Unidos passavam pela procura por objetos perigosos através das máquinas de raio-x, detetores de metais, revistas, e, mais recentemente, surgiram novas técnicas como detetores de explosivos e as imagens de corpo inteiro. Contudo, a grande inovação surge em 2003, quando a *Transportation Security Administration (TSA)* decidiu que seria importante mudar o foco para os indivíduos, ao invés dos objetos. Esta ideia surge após o 11 de setembro, com Rafi Ron, um antigo chefe de segurança do aeroporto principal de Israel, em conjunto com Paul Ekman, um especialista em deteção comportamental, que afirmou que os membros do staff dos aeroportos não estavam preparados para identificar indivíduos com intenções hostis (Kuperberg, 2010).

Para isso, a *TSA* desenvolveu o programa *Screening of Passengers by Observation Techniques* (SPOT) em 2006, com o intuito de ser possível identificar comportamentos indicativos de uma ameaça à segurança nos aeroportos do país (Kuperberg, 2010). O programa SPOT compreende a observação e análise de comportamentos pelos *Behavior Detection Officers* (BDOs). Os BDOs são agentes de segurança dos aeroportos, altamente treinados e qualificados especificamente para a deteção de comportamentos indicativos de uma potencial ameaça. Indivíduos que apresentem, por exemplo, comportamentos que indiquem altos níveis de stress, medo ou tentativa de engano são investigados por estes agentes (U.S Department of Homeland Security, 2011).

A informação que os BDOs da TSA recolhem dividem-se em duas categorias: a primeira refere-se a comportamentos observados pelos agentes e que são introduzidos na base de dados do programa SPOT para que, mais tarde, seja possível compreender os padrões de comportamento dos aeroportos nacionais e, de um aeroporto em particular. A segunda

categoria, refere-se aos comportamentos que ultrapassam o padrão de comportamentos observado e, portanto, os indivíduos com estes comportamentos são submetidos a um rastreio mais profundo, no qual se recolhem informações pessoais, de forma a que seja possível confirmar ou não a sua identidade e perceber se o individuo está referenciado em alguma base de dados policial (U.S Department of Homeland Security, 2011).

Esta nova abordagem de segurança aeroportuária, surge depois do 11 de setembro ter levantado questões sobre as técnicas comumente utilizadas nestes espaços. Os ataques às Torres Gémeas provaram que o terrorismo não está dependente de uma arma, mas antes da vontade humana em provocar o terror. Assim, os apoiantes da deteção comportamental argumentam que o terrorismo irá sempre encontrar estratégias criativas para contornar as ferramentas de segurança orientadas para o objeto, mas, dificilmente, será capaz de suprimir o comportamento humano que atraiçoa quem pretende implementar um ataque. No entanto, há quem questione a eficácia do programa *SPOT* e da Deteção Comportamental em geral neste contexto (Kuperberg, 2010).

O programa implementado nos aeroportos americanos é inspirado pela abordagem presente nos aeroportos de Israel. A segurança aeroportuária israelita é tida como referência pela sua capacidade histórica de prevenir ameaças à segurança interna, apesar do clima de tensão em que o país está envolto. Nos aeroportos de Israel, a Deteção Comportamental é a principal estratégia de segurança, e, vem recomendada num mesmo relatório que questiona o programa SPOT (Kuperberg, 2010). Esta situação levanta a questão de se as dúvidas existentes sobre o programa americano se devem à utilização da Deteção Comportamental ou das condições em que esta é aplicada.

A *American Civil Liberties Union* (ACLU), têm uma postura extremamente critica da Deteção Comportamental e da utilização desta abordagem pela TSA. Algumas das críticas feitas pela ACLU à administração americana são a alegada falta de suporte científico relativo aos indicadores comportamentais utilizados pelos BDOs na identificação de indivíduos com comportamentos suspeitos; existe também a preocupação com vários tipos de discriminação, nomeadamente, racial e religiosa, fazendo até acusações de ações discriminatórios. Realçam também o facto de os indicadores comportamentais serem vagos e tornarem impossível qualquer pessoa não os demonstrar num determinado momento, e, por fim, surgem preocupações com o custo da Deteção Comportamental e dos BDOs, uma vez que na perspetiva

da ACLU o programa não responde às questões para que foi desenhado (American Civil Liberties Union, 2017).

E, por último, existem vários programas que envolvem a população e a torna um agente ativo na Deteção Comportamental. Por exemplo, o *Action Counters Terrorism* (ACT), um programa de formação online sobre comportamentos e atitudes suspeitas no âmbito do terrorismo, grátis e direcionada ao individuo comum, ou o *"See it, Say it, Sorted"*, direcionado a quem utiliza os comboios e frequenta as estações ferroviárias e que pede para que a população esteja atenta a objetos ou atividades suspeitas e que as reportem (HM Government, 2020).

A Deteção Comportamental passa pela observação do comportamento humano e atua quando este comportamento foge da norma. Os especialistas nesta abordagem acreditam que as pessoas com intenções hostis experienciam um leque de emoções que pode passar por ansiedade, medo, culpa, nervosismo, entre outras, por saberem que estão a praticar atos ilegais ou socialmente inaceitáveis, que estas emoções irão, em alguns casos, afetar os comportamentos e as atitudes destes indivíduos, que estes comportamentos e atitudes podem ser observados e detetados, que staff de equipas de segurança e/ou vigilância podem ser treinados para identificar estes comportamentos e atitudes (HM Government, 2020).

É imperioso atender ao facto de esta abordagem ser baseada em evidências científicas, retiradas de estudos sobre as alterações comportamentais em indivíduos que estão a mentir ou a ter atitudes socialmente inaceitáveis. No entanto, esta visão parte do pressuposto de que o comportamento humano reflete as emoções sentidas, mas alguns estudos demonstram que isto nem sempre é verdade. As expressões faciais podem não representar necessariamente as emoções que a pessoa está a experienciar, as respostas emocionais e comportamentais a uma determinada circunstância variam de pessoa para pessoa devido a diferentes personalidades, a experiências anteriormente vivenciadas e a preferências pessoais. Estas variações podem levar a falsos positivos, quando o staff identifica um individuo por estar a ter comportamentos para os quais estes foram treinados para detetarem, mas que podem estar relacionados com outras situações, bem como falsos negativos, no caso de pessoas que não transparecem as suas intenções hostis através dos seus comportamentos (HM Government, 2020).

Para se assegurar o bom funcionamento desta abordagem é imperativo que haja um treino especializado dos membros das equipas que implementem a mesma, sejam eles do setor público ou privado, e uma sensibilização para a adoção de uma abordagem pacífica e cordial, uma vez que pode-se estar perante um falso positivo.

No que diz respeito à comunidade civil, é importante dotá-la de conhecimento sobre aquilo a que deve estar atenta e ao que fazer com essa informação, por exemplo, identificar aquilo que é normativo no seu ambiente e de como a norma varia de acordo com o contexto. Neste caso, não se pretende que a população seja treinada para identificar comportamentos específicos, mas antes, incentivarem para que reportem qualquer comportamento ou atitude invulgar dentro do seu contexto, como por exemplo, um veículo estacionado num local inadequado ou por exemplo a utilização de indumentária que não se adequa à estação do ano (e.g. utilizar um quispo preto no verão). Após a observação destes comportamentos, é necessário que exista uma linha de comunicação entre a comunidade e a entidade competente pela investigação dos mesmos. Por exemplo, uma linha telefónica ou o reporte direto a instituições privadas ou públicas de segurança. Para encorajar a população a tomar esta iniciativa podem ser implementadas medidas como tratar esta atitude como um dever cívico, é crucial que existam as condições necessárias para que a população possa reportar aquilo que observou e que quem recebe as informações tenha uma atitude adequada, assegurando a população de que as suas preocupações irão ser investigadas apropriadamente (HM Government, 2020).

Tal como já foi referido, a Deteção Comportamental é uma abordagem que deve fazer parte de um sistema de segurança complexo e completo e tem potencialidades e limitações. Para que seja implementada eficazmente, os funcionários das forças de segurança ou de empresas de segurança privadas devem ser dotados de conhecimentos especializados sobre a mesma e atuar sem que o seu julgamento seja afetado por preconceitos ou crenças pessoais.

A polícia enquanto screener de comportamentos

As forças policias têm uma natureza reativa, atuando, comumente, após o ato criminoso ter sido consumado. Contudo, no século XIX, em Inglaterra, surgiu um novo tipo de policiamento que hoje conhecemos por Policiamento de Proximidade. Foi com Sir Robert Peel e com a fundação da *Metropolitan Police Force* e da *Scotland Yard,* que uma nova vanguarda nasce no meio policial. Este policiamento surge da necessidade de dar resposta à sociedade moderna, que procurava na polícia um elemento preventivo. O objetivo do Policiamento de Proximidade é diminuir a criminalidade e aumentar o sentimento de segurança da sociedade, bem como a confiança dos cidadãos nos órgãos policias. Segundo Dias & Lisboa (2008), o Policiamento de Proximidade assenta dois princípios: “a polícia é o publico e o publico é a

polícia" e "a eficácia não é medida pelo número de detenções, mas antes pela ausência de crimes" (Lisboa & Dias, 2008, pp. 3-5).

Ou seja, entende-se que a polícia e a comunidade devem trabalhar em conjunto numa relação de troca de informação e confiança para reduzir a criminalidade e o sentimento de insegurança dela consequente. Também em Portugal o policiamento de proximidade é uma realidade e é exercido em programas criados para dar resposta a problemáticas especificas. Para exemplificar, podemos mencionar os programas "Violência Doméstica" e "Comércio Seguro" da Polícia de Segurança Pública (Polícia de Segurança Pública, 2021). Ou, os programas "Escola Segura" e "Residência Segura" da Guarda Nacional Republicana (Guarda Nacional Republicana, 2021). Entende-se, portanto, a relevância da cooperação entre as forças de segurança e os cidadãos na prevenção criminal e o potencial que teria a criação de um programa de Policiamento de Proximidade dedicado à prevenção do terrorismo através da observação do meio e do comportamento humano.

Havendo uma relação próxima entre a comunidade a polícia de proximidade, esta pode funcionar como um autêntico *screener* de comportamentos.

Uma das novas *nuances*, reconhecida pelos Estados Unidos como um dos maiores desafios atuais neste contexto, é a cada vez maior prevalência de *"lone wolves"*, isto é, nacionais que se radicalizaram a si próprios. O *National Strategy for Information Sharing* também reconhece o crescimento de cidadãos nacionais que se têm envolvido no terrorismo. Apesar de não terem uma ligação com o al-Qaeda ou a outros grupos extremistas, estes cidadãos são radicalizados e violentos, e retiram inspiração desses mesmos grupos. (Carter & Carter, 2011).

A emergência de uma filosofia de prevenir e mitigar o terrorismo dentro das forças de segurança é chamado nos EUA de *"intelligence-led policing*" (ILP). Trata-se de um processo de recolha e análise de informação desenhada para identificar ameaças criminosas e desenvolver respostas operacionais para eliminar as mesmas (Carter & Carter, 2011).

O processo de como a ILP é aplicada varia de acordo com a área geográfica, população, força de segurança, entre outras variáveis. Contudo, este processo respeita sempre um ciclo composto por 6 fases: planeamento e direção, recolha, processamento e agrupamento, análise, disseminação e reavaliação (Carter & Carter, 2011).

Estas seis fases delineiam o acesso pelas forças de segurança a estas informações, bem como a análise que fazem das mesmas depois de transformadas em produtos analíticos. Estes

produtos analíticos informam os membros das forças de segurança que têm funções de chefia relativamente às variáveis encontradas nas ameaças reportadas, para que estes desenvolvam estratégias de prevenção. Em simultâneo com este processo, decorrem também uma variedade de parcerias formais e informais entre as forças policiais e a comunidade. Existem ainda políticas éticas que guiam o comportamento policial e a garantias das liberdades dos cidadãos, canais de informação direcionadas ao processo de ILP e métodos de pensamento critico na análise da informação suspeita que vai sendo recolhida (Carter & Carter, 2011).

Muitas forças de segurança utilizam métodos não tradicionais de obtenção de informação no terrorismo. Um desses métodos é a utilização de informações observadas por atores internos ou externos. O observador pode então ser a própria força de segurança, membros da comunidade ou empresas do setor privado. Esta informação é redigida e processada pela força de segurança em questão, através da verificação dos factos e confirmação do *nexus* criminal do comportamento observado. Por fim, é realizado um relatório de atividade suspeita *(SAR)*, que consiste na formalização da documentação e partilha de comportamentos observados que levantaram suspeitas ao observador. (Carter & Carter, 2011).

Em seguimento dos parágrafos anteriores, é importante referir o *Predictive Policing,* que em português podemos traduzir para policiamento preditivo. Trata-se de um tipo de policiamento que se foca na prevenção criminal através da recolha de informações que resultam na antecipação de um futuro crime, permitindo uma resposta mais eficaz. Para isto são utilizados meios de recolha de informações como a análise de *hot spots,* a mapiação criminal, *profiling* geográfico e a análise das relações sociais dentro de uma comunidade. Também aqui a cooperação da comunidade é fundamental. Os cidadãos devem ter uma relação de confiança com as forças policiais que privilegie a transparência e que faça com que a comunidade acredite que a polícia irá processar as informações que fornecer na forma mais correta possível (Pearsall, 2010).

A missão das informações (*intelligence*) das forças de segurança é prevenir e mitigar os crimes e as suas consequências. Esta missão pressupõe um conjunto de conhecimentos que devem estar disponíveis para as forças de segurança, como conhecimentos relativos aos atores criminais, às suas motivações, MOs e alvos. Algumas informações que parecem irrelevantes no momento da denuncia acabam por se mostrar vitais para completar o "puzzle" e desvendar o plano de ataque (Carter & Carter, 2011).

Apesar de, tal como referido anteriormente, a natureza das forças de segurança passar pela reação ao fenómeno criminal, estas podem e devem ter um papel crucial na prevenção criminal. Em suma, para a prevenção do terrorismo, as forças de segurança devem ser proactivas, através de investimento na sua formação, em ações de sensibilização e de treino junto da comunidade para que esta seja também capaz de identificar comportamentos indicadores de terrorismo ou de crimes anexos (Carter & Carter, 2011).

A criminalidade complexa, como o terrorismo e os crimes de colarinho branco, exigem uma planificação detalhada antes do facto. Apesar de sabermos que cada vez são mais utilizados métodos de ataque simples e acessíveis, existe sempre um longo processo de seleção dos alvos, do momento de ataque e da estratégia de ataque. Este planeamento é mais evidente em ataques mais arrojados como foi o caso do 11 de Setembro, que explorou as fragilidades da aviação civil. Esta janela temporal de planeamento do ataque dá às forças de segurança uma maior oportunidade de conseguir neutralizar a ameaça antes do ataque (Carter & Carter, 2011).

É necessário salientar que é impossível que as forças de segurança sejam capazes de identificar e neutralizar todas as ameaças. Assim como referido anteriormente, o terrorismo implica um período longo de planeamento e preparação, o que pode facilitar a identificação dos comportamentos suspeitos. Contudo, as oportunidades são também limitadas. Assim, quando não houver a possibilidade de prevenir o facto, é importante que as forças de segurança utilizem as informações que forem capazes de recolher dos incidentes que se concretizarem e aproveitá-las para a prevenção de ameaças futuras (Carter & Carter, 2011).

Desta forma, a capacidade de as forças de segurança prevenirem ataques terroristas depende, em parte, da informação que têm ao seu dispor, informação esta que muitas vezes surge fora da sua alçada. Por vezes, mais importante do que a tecnologia sofisticada disponível, é a partilha informal de informação relativa a comportamentos observados que chamam a atenção da comunidade. Por conseguinte, deve haver um investimento cada vez maior na relação entre as forças policias e a comunidade (Carter & Carter, 2011).

Apesar de todas as potencialidades anteriormente referidas, é importante notar que a deteção comportamental, para ser eficiente, deve estar integrada numa abordagem sistémica. Outro obstáculo é o facto de poder ser dispendiosa e requerer formação contínua das forças de segurança. Requer ainda a utilização regular das competências adquiridas na formação para que que se mantenha a sua eficiência. Implica ainda um protocolo de procedimentos para que os agentes estejam aptos a investigar as suspeitas de forma rápida e eficiente, requer monitorização

contínua de modo que se verifique que as suspeitas são fundamentadas e não são influenciadas por nenhum tipo de preconceito, e, deve ser considerada como complemento de uma avaliação completa e complexa (HM Government, 2020).

Outra preocupação levantada pelos especialistas passa pela sobrecarga dos agentes de segurança, que, estando incumbidos de desempenhar outras funções e, simultaneamente, implementar deteção comportamental podem pôr em causa a sua eficácia (HM, Government, 2020).

Conclusões

Após a analise da literatura encontrada, concluiu-se que o processo de radicalização envolve uma dinâmica complexa entre *push and pull factors*[2]. Durante este processo, o individuo desenvolve um conjunto de crenças e ideais que se refletem na sua conduta. É nesta fase que se encontra a primeira oportunidade para a Deteção Comportamental enquanto ferramenta preventiva ser implementada, pela comunidade. Isto é, os pares do individuo têm acesso privilegiado a estas alterações cognitivas e, potencialmente, comportamentais, podendo ter um papel fulcral na prevenção da escalada de comportamentos violentos. Para além disso, é a comunidade que melhor conhece o meio onde vive, as suas pessoas e os seus hábitos. Isto significa que também será a comunidade o elemento mais preparado para identificar condutas que vão contra as normas comportamentais e sociais característicos do meio onde vive. Para isto, é essencial encorajar a comunidade a estar vigilante, identificar comportamentos e a reportá-los às autoridades.

Os órgãos de polícia criminal podem também ter um papel crucial nesta matéria, já que a natureza da profissão policial tem uma componente extremamente sensorial e que é utilizada nos diferentes contextos em que operam. Por um lado, estão tecnicamente capacitadas para agir no pós-denuncia. Por outro lado, podem ser treinadas para elas próprias detetarem comportamentos suspeitos no âmbito do seu trabalho no terreno. Isto é, aquando da implementação de estratégias de segurança em contextos vulneráveis como por exemplo, em *soft targets* (eventos culturais, religiosos, desportivos, policiamento de proximidade, entre

[2] *Push and pull factors* são fatores que influenciam o meio, sendo que uns causam atração e outros pressão relativamente a uma determinada realidade.

outros.), mas também em *hard targets* (Instituições Governamentais, Atos Oficiais, entre outros).

Um terceiro elemento importante é a segurança privada. A segurança privada tem assumido um papel de relevo em Portugal e as suas funções e competências têm vindo a ser alargadas (Marques, 2013).

Segundo a lei nº 34/2013, a segurança privada compreende um conjunto de procedimentos, entre os quais a vigilância de bem móveis e imoveis, públicos ou privados, e a respetiva saída e entrada de pessoas, bem como a entrada de objetos perigosos como armas e substâncias. A segurança privada pode ainda ser a título pessoal ou desempenhada por empresas. Outras funções possíveis de desempenhar neste contexto são o transporte e guarda de valores, sinais de alarme e videovigilância, a inspeção de bagagens e títulos de transporte e a elaboração de planos e estratégias de segurança.

Dentro da sua função preventiva, destaca-se a prevenção situacional como uma área em que a segurança privada pode alcançar melhores resultados utilizando esta técnica. É comum vermos empresas de segurança privada a cargo da segurança de *soft targets* como centros e espaços comerciais, eventos desportivos e culturais, etc. É neste sentido que seria importante que estes trabalhadores estivessem treinados e informados sobre a que tipo de comportamentos devem estar atentos, como os identificar e como intervir na presença de uma possível ameaça.

Outra conclusão extremamente importante prende-se com o facto da Deteção Comportamental por si só não constituir uma ferramenta preventiva eficaz. Para que alcance o seu potencial máximo deve ser integrada num plano de segurança que envolva várias técnicas preventivas, sendo parte integrante da estratégia e não uma estratégia por si só.

Uma das grandes vulnerabilidades da Deteção Comportamental é garantir que as decisões tomadas são livres de preconceito e viés. Assim, todos aqueles que podem vir a utilizar esta técnica, desde o cidadão comum a um agente de polícia devem receber formação sobre Direitos Humanos, como contrariar os nossos preconceitos e sobre tomada de decisão isenta.

Em suma, verificou-se que apesar de algumas fragilidades a Deteção Comportamental pode ser implementada como estratégia de prevenção do Terrorismo quando integrada numa abordagem mais complexa e composta por outras técnicas que se auxiliam mutuamente. Os possíveis atores desta técnica podem ser de três naturezas diferentes e agir em diferentes momentos e contextos, falamos da Comunidade, dos Órgãos de Polícia Criminal e das

Empresas de Segurança Privada. Para que a sua implementação seja eficiente, os atores mencionados devem tomar decisões livres de preconceitos e viés, orientadas pelo conhecimento científico e pela experiência. A abordagem a potenciais ameaças deve ser cautelosa, contabilizando sempre a possibilidade de se estar perante um falso positivo ou um falso negativo.

Uma vez que não só a literatura sobre esta temática no contexto português, como também as orientações para que os atores supramencionados a ponham em prática é praticamente inexistente, decidiu-se que seria emergente e útil para a comunidade a criação de um guia para a utilização da Deteção Comportamental tendo por base a revisão de literatura feita e os guias já existentes noutros países dentro e fora da União Europeia. Assim, passaremos a apresentar o Guia para a Utilização da Deteção Comportamental em Portugal, que poderá ser consultado e utilizado por qualquer cidadão que procure informação sobre esta técnica e a sua implementação.

Capítulo V

Guia de Boas Práticas para a Implementação da Deteção Comportamental na Prevenção do Terrorismo

1. Propósito e Destinatários

Este Guia é baseado nas informações recolhidas durante uma revisão bibliográfica extensiva que incluiu textos em português e inglês e que explorou a Deteção Comportamental e a sua implementação em diferentes países. O seu propósito é oferecer informações sobre o que é a Deteção Comportamental; quando, onde, como e por quem pode ser implementada; e, os seus benefícios e malefícios. Durante a apresentação deste guia serão mencionados cuidados importantes a serem considerandos na implementação da Deteção Comportamental.

O público-alvo deste guia são todos os que procuram mais informações no âmbito da Deteção Comportamental, com ênfase nas forças policiais e de segurança, mas também, a população em geral.

2. O que é a Deteção Comportamental?

Este Guia entende a deteção comportamental enquanto uma técnica de observação de comportamentos, que, com base na investigação científica dos padrões comportamentais e na experiência, identifica indivíduos com comportamentos ou atitudes atípicas e inapropriados que indicam a presença de uma potencial ameaça para a segurança pública. Para a utilização deste método deve-se ter em conta diversos fatores como o contexto, a cultura e o comportamento esperado para o ambiente em que o individuo está inserido.

3. Formação

Os agentes das forças policiais, bem como os funcionários de empresas de segurança privada devem ser submetidos a uma formação inicial, antes de iniciarem o desempenho das suas funções. Esta formação deve abordar a Deteção Comportamental (O que é? Que comportamentos indicam uma conduta suspeita? Como se implementa? Em que contextos pode ser utilizada? Como agir na presença de uma potencial ameaça? Como neutralizar a ameaça?) e Direitos Fundamentais (O que são preconceitos? Como podemos contrariar os nossos preconceitos? Como abordar o suspeito? Como agir na presença de um potencial falso positivo?).

À *posteriori*, deve também existir formação continua, que aborde as mesmas questões acima referidas e que se vá adaptando às mudanças sociais e às necessidades da segurança interna do país.

Algumas ideias chave que orientam a Deteção Comportamental:

- Indivíduos com intenções hostis experienciam uma série de emoções negativas (medo, ansiedade, nervosismo, stress...) que se irão refletir na sua conduta, já que entendem como culpados e receiam ser detetados;
- Esta conduta pode incluir expressões faciais suspeitas, a verbalização da sua intenção ou de outras pistas, movimentos corporais que indicam nervosismo, comportamentos inadequados ao contexto onde está inserido;
- Agentes policiais ou de segurança podem ser treinados para identificarem e detetarem estes comportamentos.

Contudo, nem sempre os nossos comportamentos refletem adequadamente as nossas emoções, podendo levar a falsos positivos ou falsos negativos. Isto é, indivíduos detetados pelos seus comportamentos, mas que não representam uma ameaça e indivíduos que não aparentam

ser uma ameaça, mas que na realidade o são, respetivamente. Isto obriga a que os agentes policiais e de segurança estejam preparados para atuarem perante estas duas possibilidades. Assim, a abordagem deve ser sempre cordial e cuidadosa, movida pelo conhecimento cientifico e pela experiencia, evitando adotar uma atitude que possa ser entendido como preconceituosa ou agressiva.

O primeiro passe é conhecer e compreender o comportamento normativo num determinado contexto. Aqui a comunidade tem um papel fundamental já que é quem melhor conhece o contexto onde vive e quem o frequenta. E, seguidamente, devem-se seguir qualquer preocupação ou alertas relativos a comportamentos suspeitos que tenham sido observados.

4. A Deteção Comportamental e a Comunidade

A comunidade pode ser um agente determinante no sucesso da Deteção Comportamental. Tal como foi referido anteriormente, são os cidadãos que melhor conhecem o ambiente onde residem, os locais que frequentam, as pessoas que se movem nesse meio e os comportamentos habituais/normativos nesse contexto. Assim, a comunidade deve ser capacitada para identificar e denunciar comportamentos que não se enquadram nos diferentes contextos que a envolvem.

Um primeiro método para instruir a comunidade pode ser a implementação de campanhas informativas que não só apelem à denuncia de atividades suspeitas como também forneçam informação relativamente a que atividades podem/devem ser reportadas. No entanto, deve ressalvar-se que não se pretende fornecer uma lista de comportamentos suspeitos, mas antes apelar a que sejam os próprios cidadãos a identificarem esses comportamentos, já que o conceito de "normal" varia em determinados contextos.

Como exemplo, podemos referir o programa britânico *"Action Counters Terrorism" (*ACT), liderado pela *Counter Terrorism Policing*. Trata-se de uma plataforma online, que fornece um curto e simples curso informativo e instrutivo sobre terrorismo e os comportamentos a que devemos estar atentos. Esta plataforma oferece ainda a possibilidade de reportar online qualquer atividade suspeita que tenha sido observada e que o observador acredite poder estar relacionada com terrorismo. Para além disso, os cidadãos têm também acesso a um leque variado de informações o que devem reportar, ao que devem estar atentos, o que fazer se houver suspeita de quem familiar ou amigo está a viver um processo de radicalização, dicas para se manter seguro, entre outras informações extremamente importantes.

Outro passo importante é a criação de programas que apelem ao estreitamento da relação entre a comunidade e a polícia de proximidade. Programas como o *"See something, say something*" dos Estados Unidos da América que incentivam a que os cidadãos estejam atentos ao que acontece à sua volta e que reportem qualquer comportamento ou atividade duvidosa às forças de segurança, podem ser iniciativas extremamente eficientes para a prevenção criminal. Se, dentro destes programas, existir uma linha de contacto ou uma estratégia de reporte de atividades especificamente dedicadas ao terrorismo e ao crime organizado, isto permitirá uma triagem e uma posterior atuação mais eficazes por parte dos órgãos de polícia criminal.

5. Pontos chave para uma Deteção Comportamental eficaz

A Deteção Comportamental deve estar integrada numa abordagem preventiva ampla e complexa. Isto é, não deve ser encarada como uma ferramenta independente, já que a sua eficácia depende da inclusão numa estratégia complexa. Técnicas como o policiamento de proximidade, a monitorização de câmaras de vigilância, ações encobertas, entre outras, devem completar a Deteção Comportamental.

Outra consideração importante é adaptar a Deteção Comportamental ao ambiente em que está a ser implementado. Isto é, um evento de grande dimensão (e.g. festival de música) tem, necessariamente, necessidades de segurança distintas de um aeroporto. Desta forma, não só a implementação deste método deve ser adaptada às necessidades individuais do contexto, como também, as outras estratégias de segurança que o complementem podem variar (e.g. utilização de comunicação, segurança visível através de uniformes, agentes encobertos, equipas cinotécnicas, câmaras de vigilância, etc.).

A cooperação entre todos os agentes de Deteção Comportamental, forças policiais, de segurança privada e o cidadão comum, deve ser privilegiada. A troca de informações é crucial, já que permite que exista um conhecimento comum não só dos comportamentos padrão como também dos potenciais suspeitos já identificados.

Finalmente, só com uma avaliação regular será possível compreender a eficácia deste método. O primeiro passo será definir aquilo que se pretende avaliar e o método de avaliação. Alguns pontos que devem ser avaliados são os custos monetários e humanos a que este método obriga, a formação existente e os resultados na prevenção criminal. Uma vez que este é um método pouco comum em Portugal, a adaptação de programas de Deteção Comportamental estrangeiros ao nosso território pode ser o caminho mais seguro. A utilização de treino,

equipamento e tecnologias previamente implementadas em outros programas, ainda que para fins distintos, é uma boa estratégia para garantir um resultado positivo.

Contudo, é importante referir que ainda que a Deteção Comportamental já seja implementada em outros países, é ainda um método novo e que requer estudos mais aprofundados. Havendo um reduzido número de ameaças terroristas, torna-se difícil haver dados suficientemente robustos para que a avaliação seja verosímil. Ainda assim, este é um método em crescimento e que é cada vez mais implementado, o que poderá significar um aumento de dados sobre a sua eficácia num futuro próximo. Para além disso, a literatura tem vindo a estudar o comportamento criminal e como este pode ser utilizado para detetar potenciais ameaças terroristas.

Conclusão

O terrorismo, nomeadamente o de origem islâmica, tem fortemente ameaçado o continente europeu na última década. Apesar de Portugal ter vindo a escapar a esta ameaça de uma forma direta, no mundo globalizado em que vivemos, qualquer ataque a um Estado, tem, necessariamente implicações para os restantes. Para além disso, é importante destacar a imprevisibilidade deste tipo de crime, pelo que, a qualquer momento também o nosso país poderá vir a ser vítima de um ataque terrorista.

Nesta linha de pensamento, decidiu-se que seria imperioso realizar um estudo do qual resultasse um instrumento que pudesse ser utilizado na prevenção do terrorismo em Portugal. Estudou-se a realidade de outros países, e, a Deteção Comportamental suscitou interesse, pela sua inovação e controvérsia, criando curiosidade e interesse em conhecer mais sobre esta técnica e a sua implementação.

O cerne deste trabalho, prende-se pelo estudo e validação da Deteção Comportamental enquanto uma ferramenta preventiva do terrorismo e neutralizadora de atos terroristas. Para além disso, houve uma preocupação contínua em alertar o público não só sobre esta técnica, mas também sobre o papel que, não só as forças de segurança, mas também o cidadão comum pode e deve ter no garante da sua segurança e da segurança nacional.

As grandes dificuldades encontradas durante o desenvolvimento deste trabalho foram essencialmente a escassez de literatura sobre Deteção Comportamental em português, que, por

outro lado, corroboraram a necessidade de um estudo sobre esta temática no panorama nacional; e, a ausência de dados numéricos e estudos empíricos realizados neste âmbito, que pudessem esclarecer sobre a eficácia deste método.

Desta forma, encoraja-se à realização de estudos futuros, nomeadamente empíricos, desenvolvidos em contexto nacional, perto das forças de segurança e da comunidade que possam avaliar a eficácia da Deteção Comportamental em diferentes contextos.

Bibliografia

Almeida, R. H. (2018). *Fatores Biopsicossociais da Conduta Criminosa e Sistema de Justiça Juvenil: Avaliação do Comportamento Antissocial, Através da Escala Hare PCL-YV, de Adolescentes Femininas em Conflito com a Lei* [Master's thesis, Pontifícia Universidade Católica do Rio Grande do Sul].

American Civil Liberties Union. (2017). *BAD TRIP Debunking the TSA's 'Behavior Detection' Program*. ACLU Foundation. https://www.aclu.org/report/bad-trip-debunking-tsas-behavior-detection-program

Amman, M., Bowlin, M., Buckles, L., Burton, K. C., Brunell, K. F., Gibson, K. A., Griffin, S. A., Kennedy, K., & Robins, C. J. (2015). *Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks*.

As diferenças entre sunitas e xiitas, que explicam boa parte dos conflitos no Oriente Médio. (2021, January 10). *BBC News Brasil*, 1-11. https://www.bbc.com/portuguese/internacional-51068470

Barata, M. J. (2007). *A Oposição Sunismo/Xiismo Enquanto Fonte de Tensão e Conflito no Médio Oriente Contemporâneo*.

Burton, F., & Stewart, S. (2008, January 30). *The 'Lone Wolf' Disconnect*. RANE. https://worldview.stratfor.com/article/lone-wolf-disconnect

Carter, J. G., & Carter, D. L. (2011). Law enforcement intelligence: implications for self-radicalized terrorism. *Police Practice and Research*, *13*, 138-154.

Centre for the Protection of National Infrastructure, & ACTION COUNTERS TERRORISM. (2020). *RECOGNISING TERRORIST THREATS For the security professionals*. https://www.cpni.gov.uk/blog/physical-security/recognising-terrorist-threats

Chaliand, G., & Blin, A. (Eds.). (2017). *História do Terrorismo Da Antiguidade à Alcaida*. ODETE

Columbian College of Arts & Sciences. (n.d.). What Is the Difference Between Sunni and Shiite Muslims? And Why Does It Matter? *History News Network*. https://historynewsnetwork.org/article/934

Conselho Europeu, & Conselho da União Europeia. (2021, August 19). *Resposta da UE à ameaça terrorista*. conssilium.europa.eu. https://www.consilium.europa.eu/pt/policies/fight-against-terrorism/

Costa, C. S. F. (2016). *O Impacto do Terrorismo na Administração Interna em Portugal, no Século XXI* [Master's thesis, Universidade de Lisboa - Instituto Superior de Ciências Sociais e Políticos].

Costa, S. L. O. (2016). *O Pensamento Islamista Contemporâneo: A Jihad Global na Europa* [Doctoral dissertation, Universidade do Minho].

Costa, S. L., & Pinto, M. d. C. (2012). *A Problemática da Radicalização Islamista: Desafios Conceptuais e Dificuldades Práticas no Contexto Europeu*.

Coutinho, C. P. (2019). *Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática* (2nd ed.). Almedina.

Counterterrorism Policing. (2021). *Project SERVATOR Together We've Got It Covered*. counterterrorismpolicing.police.uk. Retrieved April 11, 2021, from https://www.counterterrorism.police.uk/servator/

CRONOLOGIA: Principais atentados terroristas na Europa, desde 2015. (2019, March 22). *Diário de Notícias*. https://www.dn.pt/lusa/cronologia-principais-atentados-terroristas-na-europa-desde-2015-10712346.html

Cuesta, A., Abreu, O., Balboa, A., & Alvear, D. (2019). *A new approach to protect soft-targets from terrorist attacks*.

Cuesta, A., Abreu, O., Balboa, A., & Alvear, D. (2019). A new approach to protect soft-targets from terrorist attacks. *Safety Science*, 877-885.

Europol. (2020). *European Union Terrorism Situation and Trend report 2020*. European Union Agency for Law Enforcement Cooperation 2020.

Europol. (n.d.). *European Counter Terrorism Centre - ECTC*. Retrieved February 25, 2021, from https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc

Dias, J. d. F., & Andrade, M. d. C. (2013). *Criminologia O Homem Delinquente e a Sociedade Criminógena* (1st ed.). Coimbra Editora.

Guarda Nacional Republicana. (2021). *Policiamento Comunitário e os Programas Especiais na GNR*. gnr.pt.

Gomez, G. R., Flores, J. G., & Jiménez, E. G. (1996). *Metodología de la investigación cualitativa*. Ediciones Aljibe, S. L. 1996.

Gouvia, J. B. (2018). *Direita da Segurança Cidadania, Soberania e Cosmopolitismo* (1st ed.). Almedina.

Henne, B. (2019). *Policy in Action Piece Hardening Soft Targets* (Artigo Científico). From University of Delawar: https://cpb-us-w2.wpmucdn.com/sites.udel.edu/dist/a/7158/files/2019/04/Henne_Hardening-2myw9o5.pdf?fbclid=IwAR1Fm4uod_sisx1-QDKGuVpcCrnt2_srG7Pu6SjJWF08LZhRKYR-Xs2kV2U

HM Government. (2020). *Behavioral detection Best practice, guidance and advice*. https://www.cpni.gov.uk/system/files/documents/03/73/CPNI0068_Behavioural_Detection_Brochure_DIGITAL_V8.pdf

Kuperberg, B. A., & Benjamin, M. (2010). *Behavior Detection a Commercial Aviation Security Measure: Prospects and Obstacles* [Master's thesis, Georgetown University].

Lei nº 52/2003 de 22 de agosto de 2003. Diário da República Série I-A, Nº 193/2003. https://dre.pt/web/guest/legislacao-consolidada/-/lc/67545383/201808091828/diplomaExpandido?p_p_state=maximized

Lei nº 53/2008 de 29 de Agosto de 2008. Diário da República Série I, Nº 167/2008. https://dre.pt/pesquisa/-/search/453479/details/maximized

Lisboa, M., & Dias, A. L. T. (2008). *Organizações e Meio Envolvente: o caso do ´Policiamento de Proximidade"* [Doctoral dissertation, Universidade Nova de Lisboa].

Lorena, S. (2018, November 3). Europa unida na condenação ao atentado reivindicado pelo Daesh em Viena. *Público*.

Martins, R. F. C. (2010). *À cerca de "Terrorismo" e de "Terrorismos"*. https://www.idn.gov.pt/publicacoes/cadernos/idncaderno_1.pdf?fbclid=IwAR3Q9-i88r2y8q5xzYHg6dIUDWoQEtsl4u1I6u2FVfoc7k7t9ONA8RbZLPk

Martins, A. R. R. (2018). *Terrorismo Jihadista na Europa - O regresso dos combatentes Jihadistas aos seus países de origem* [Master's thesis, Instituto Superior de Ciências Policiais e Segurança Interna].

McCauley, C., & Moskalenko, S. (2017). Understanding political radicalization: The two-pyramids model. *American Psychologist, 72*(3), 205 216. https://doi.org/10.1037/amp0000062

McMillan, J., & Shumacher, S. (2014). *Research in Education*. Pearson Education Limited 2014.

National Institute of Justice, B. P. (2010, May 1). Predictive Policing: The Future of Law Enforcement. *NIJ Journal*, 16-19.

Os atentados na Europa desde 2004. (2017, April 7). *Jornal de Notícias*. https://www.jn.pt/mundo/cronologia-atentados-na-europa-atribuidos-aos-movimentos-islamitas-5089588.html

Polícia de Segurança Pública. (2021). *O que é? MIPP*. psp.pt

Portela, I. (2009). A segurança interna e o combate ao terrorismo: o caso português. *Revista Enfoques*, *11*, 491-514.

Prates, D. D. M. (2018). *A Prevenção da radicalização Jihadista - O Papel da Polícia de Proximidade* [Master's thesis, Universidade Nova de Lisboa].

Rego, P. C. P. (2017). *Terrorismo lone wolf: Uma revisão da literature* [Master's thesis, Instituto Superior de Ciências Policiais e Segurança Interna].

Rezende, L. P. & Schwether, N. D. (2015). Terrorismo: A contínua busca por uma definição. *Revista Brasileira de Estudos e de Defesa,* V. 2, Nº1, 87-105. https://rbed.abedef.org/rbed/article/view/58349?fbclid=IwAR33XVFQexnEqzviZm1Rv7QWA9J0cgSnMrSsxq61A1ZAjOJmKHicV1eLdk0

Schmid, A. P. (2013, March). Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review. *International Centre for Counter-Terrorism - The Hague*.

Silva, A. M. L. (2017). *A CORRESPONSABILIZAÇÃO NO EXERCÍCIO DA SEGURANÇA PÚBLICA: A PROTEÇÃO DE SOFT TARGETS* [Master's thesis, INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA].

Silva, A. S. (2020, October 29). França está a ser atacada? Assume Macron após ataque terrorista em Nice. *Público*. https://www.publico.pt/2020/10/29/mundo/noticia/morto-varios-feridos-nice-apos-ataque-faca-1937158

U.S. Department of Homeland Security. (2011). *Privacy Impact Assessment Update for the Screening of Passengers by Observation Techniques (SPOT) Program*. https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-spot-update_0.pdf

What is jihadism?. (2014, December 11). *BBC*, 1-14. https://www.bbc.com/news/world-middle-east-30411519

Anexos

HM Government

Behavioural detection

Best practice, guidance and advice

CPNI
Centre for the Protection of National Infrastructure

Department for Transport

[dstl]
The Science Inside

NaCTSO

Executive Summary

The term 'behavioural detection' refers to a method of detecting individuals with hostile intentions by observing their behaviours and activities. This guidance is written by behavioural detection experts from across government, and has been informed by consultations with key stakeholders and other specialists as well as by research and other literature.

The purpose of this document is to inform those considering the use of behavioural detection and to provide specific advice for various stakeholders. It can help those needing to better understand (a) different behavioural detection approaches, (b) the strengths and weaknesses of these, and (c) how to choose and apply behavioural detection methods to specific environments to maximise the security of a location and its people.

As such, this guidance is designed to help both policy makers in government and industry who are responsible for advising and/or mandating security processes and measures, and those on the frontline responsible for ensuring security, such as security managers across a range of different sites.

This guidance provides information on:

- The role of behavioural detection within protective security, plus the pros and cons and other matters that should be considered before deciding to include the use of behavioural detection as a security measure.
- How behavioural detection works, and the need to set up and adapt the environment to help elicit behaviours of concern whenever possible.
- The vital importance of rapidly and effectively resolving suspicions that result from behavioural detection.
- Types of behavioural detection – from specifically trained personnel to public campaigns that encourage vigilance and reporting of suspicious activity.
- Matters to consider before procuring or instigating a behavioural detection capability.
- Measures of effectiveness and evaluation of training, technology and equipment.

Executive Summary

When incorporated with other security measures, behavioural detection can be a powerful tool that can be implemented in a range of environments, as part of a systematic approach to disrupt criminals and terrorists carrying out activities that aim to cause harm to others. This overall approach to disruption may include (i) detecting individuals (e.g. whilst conducting hostile reconnaissance), (ii) deterring thieves (e.g. from targeting a venue), and (iii) denying different types of criminals (e.g. access to information they need to plan an illegal activity)[1].

Behavioural detection can contribute to this disruption. However, it is vital to note that behavioural detection:

- Is not a panacea in protective security; it should be seen as part of a systematic approach to the security of a site – detection is just one aspect of this.
- Can be expensive to implement and difficult to retain as a capability, especially if staff turnover is generally high, unless there is a rolling training programme.
- Requires staff to use their skills regularly, to maintain competence.
- Requires a clear process in place for staff to rapidly, effectively and fairly resolve suspicions about any persons of concern.
- Requires on-going monitoring and evaluation to ensure it is effective and does not have or develop inherent biases that can skew outcomes (e.g. whereby individuals are prejudiced against because of their gender, race or mental health issues).

1. These are the '3Ds' of CPNI's disruption model. See https://www.cpni.gov.uk/disrupting-hostile-reconnaissance

Executive Summary

It is important to note that if trained personnel are expected to conduct behavioural detection but also other duties at the same time, this will limit the effectiveness of the capability. Moreover, the potential of behavioural detection to be effective is significantly impacted by the number of trained staff on duty, the area that they are covering, and other elements of the environment.

This guidance paper sets out key points to consider regarding the use of behavioural detection to contribute to the security of different environments. It outlines when, where, why and how behavioural detection may be effective or fail, and critically, what to consider when contemplating the use of behavioural detection. The guidance can be used to assist those responsible for the security of different environments, to ensure that any application of behavioural detection meets requirements and is successful. It should therefore be read and used by those responsible for security at strategic, operational and tactical levels. Doing so can lead to a shared understanding of behavioural detection in terms of both its strengths and its weaknesses, ensure that misunderstandings and myths are dispelled, and that the capability is implemented in an appropriate, proportionate and effective way.

Behavioural detection capability has the potential to detect, deter and deny hostiles from operating in a range of contexts and environments. However, it is important to note that:

Behavioural detection should only be deployed as part of an integrated system to ensure that it complements and is complemented by other security measures.

It is vital that the set-up of the environment is conducive to and organised in a way that can maximise the potential success of behavioural detection, and that training provides skills and techniques that are evidence-based and tailored for different audiences.

Those considering the procurement and deployment of behavioural detection capability should ensure that they do so in an appropriate and proportionate way and have the resources to do so.

Section 1: Introduction and background

1 Introduction and background

1.1 Purpose of this guidance

This guidance has been written by behavioural detection experts from across government, and has been informed by consultations with key stakeholders and other specialists as well as by research and other literature[2].

The purpose is to inform those considering the use of behavioural detection and to provide specific advice for government and businesses.

The guidance sets out key points to consider regarding the use of behavioural detection to contribute to the security of different environments. The aim is to demonstrate when, where, why and how behavioural detection may be effective or fail, and critically, what to consider when contemplating the use of behavioural detection.

1.2 Who this guidance is for

The guidance has been written for various stakeholders; primarily those needing to better understand different behavioural detection approaches, the strengths and weaknesses of these, and how to choose and apply behavioural detection methods to specific environments to maximise the security of a location and its people.

As such, this document is designed to help both policy makers in government and industry who are responsible for advising and/or mandating security processes and measures, and those on the frontline responsible for ensuring security, such as security managers across a range of different sites.

1.3 What is behavioural detection?

In the current guidance we use the term 'behavioural detection' to mean a method of detecting individuals with hostile intentions by observing their behaviours and activities[3]. Other terms are sometimes used interchangeably (e.g. 'behaviour awareness', 'behaviour analysis') but behavioural detection is our preferred term.

This guidance frequently refers to 'hostiles' or 'hostile individuals', meaning a range of individuals who are at a site for malicious reasons. This includes pickpockets and shoplifters, and others who are at a site to gather information and conduct other actions ('hostile reconnaissance') as part of plans to conduct a terrorist attack.

2. Senior security staff in major UK transport hubs and other specialists were consulted, and a systematic review of the literature and online resources, websites etc. was conducted.

3. It is important to note that behavioural detection can also provide a strong deterrent effect.

1 Introduction and background

Key definitions

HOSTILE

"A person who wants to attack or disrupt an organisation for profit or to make a political or ideological point"

HOSTILE RECONNAISSANCE

"The purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target"

HOSTILE INTENT

"What a hostile wants to achieve to meet their overall aims"

Advocates of behavioural detection suggest that in the right environment:

- Some people with hostile intentions can exhibit overt, observable 'cues';
- Security staff (and others, including the public) can be taught to identify these cues, and as such can detect individuals with hostile intentions;
- Behavioural detection can be used to deter hostiles and to reassure the public.

It is also important to note that behavioural detection may lead to staff noticing and being able to help members of the public who may be distressed and/or need help. For example, people may be behaving unusually compared to others around them, because they are lost, have mental health issues or are having suicidal thoughts, or because they need help for other reasons.

When incorporated with other security measures, behavioural detection can be a powerful tool that can be implemented in a range of environments, as part of a systematic approach to disrupt criminals and terrorists carrying out activities that aim to cause harm to others. This overall approach to disruption may include **detecting** individuals whilst they are conducting hostile reconnaissance, **deterring** thieves from targeting a venue and **denying** criminals access to information they need to plan an illegal activity.
These are the '3Ds' of CPNI's disruption model (see Figure 1 on Page 10). Behavioural detection can contribute to this disruption.

1 Introduction and background

However, it is vital to note that behavioural detection:

- Is not a panacea in protective security; it should be part of a systematic approach to the security of a site – detection is just one aspect of this.
- Can be expensive to implement and difficult to retain as a capability if staff turnover is generally high, unless there is a rolling training programme.
- Requires staff to use their skills regularly, to maintain competence.
- Requires a clear process in place for staff to rapidly, effectively and fairly resolve suspicions about any persons of concern.
- Requires on-going monitoring and evaluation to ensure it is effective and does not have or develop inherent biases that can skew outcomes (e.g. whereby individuals are prejudiced against because of their gender, race or mental health issues).
- Should only be considered as a mitigation on completion of a full security risk assessment

It is also important to note that if trained personnel are expected to conduct behavioural detection as well as other duties at the same time – this will limit the effectiveness of the capability. Moreover, the potential of behavioural detection to be effective is significantly impacted by the number of staff on duty who are trained, the area that they are covering, and other elements of the environment. For example, how busy or quiet it is or how the area is set up and whether there are measures in place that act as a stimulus to elicit behaviours from those with hostile intent or conducting hostile activities.

1.4 What this guidance contains

This guidance provides the policy maker and security professional with an understanding of:

- The role of behavioural detection within protective security, plus the pertinent considerations before deciding to include the use of behavioural detection as a security measure.
- How behavioural detection works, and the need to set up and adapt the environment to help elicit behaviours of concern whenever possible.
- The vital importance of rapidly and effectively resolving suspicions that result from behavioural detection.
- Types of behavioural detection – from specifically trained personnel to public campaigns that encourage vigilance and reporting of suspicious activity.
- A checklist of matters to consider before procuring or instigating a behavioural detection capability.

Section 2:
The role of behavioural detection in protective security

Often behavioural detection is seen by security managers as a desirable, additional layer to protective security. It is expected and perceived to enhance the detection capability of a site and potentially act as way of disrupting a wide range of criminality, for example through the deterrence or detection of hostile individuals.

Indeed, this can be the case for a well-trained behavioural detection capability, but, as this guidance will show, **behavioural detection is a specialist skill that requires training, frequent use and continuous evaluation, and should be used strategically in a proportionate and effective way**.

Most organisations tend to have a limited behavioural detection capability, depending on the size of the venue and available resources. It is rarely possible for a behavioural detection capability to cover all parts of a site at all times. Therefore, to be as effective as possible, it needs to be deployed across key areas of a site (e.g. where hostile activity is most likely), at specific times (e.g. when hostile activity is most likely).

It is imperative that a location or organisation is not wholly reliant on specialist behavioural detection capability to detect hostile individuals. Every site should use the entirety of its people and other resources (e.g. staff and the public, security officers and CCTV) to full effect, with or without a dedicated behavioural detection capability.

How to achieve this is covered in Section 2.2.

2 The role of behavioural detection in protective security

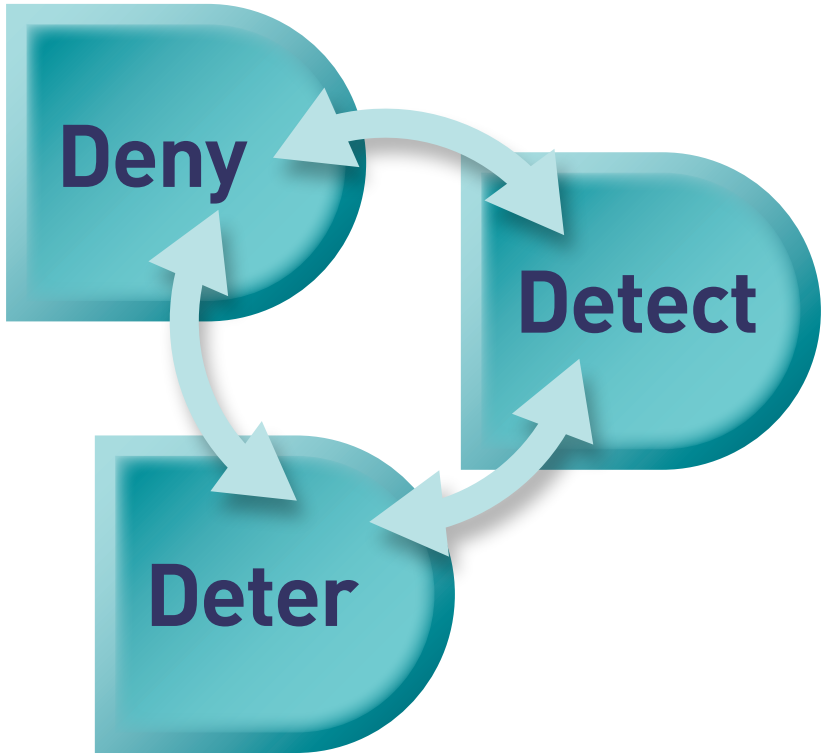
2.1 The 3Ds of disruption

Behavioural detection is not the only approach available to a site to disrupt those with malicious intent. There are other methods of disruption that are practical and relatively easy to implement and sustain, instead of or alongside a specialist behavioural detection capability.

For example, use of corporate communications to promote capabilities and using staff in customer engagement roles to have a stronger security function by attending to and engaging with suspicious individuals in a friendly, customer service oriented manner.

Organisations procure and train behavioural detection because ultimately, they want to disrupt terrorists and wider criminality by detecting them. However, the site or organisation considering behavioural detection should think beyond just detection, as there are two other key elements of disruption that can be readily achieved by a site or organisation: DENY and DETER. This is encapsulated in CPNI's 3Ds disruption model in Figure 1.

Figure 1:
The 3Ds disruption model



2 The role of behavioural detection in protective security

DENY:

Organisations should aim to deny a hostile's ability to gain useful, credible information that can help them plan effective attacks or other criminal activity. This includes information that can be found online, for example an architect's exact floor schematic of a venue, which reduces the need to go to the site to determine this information. This can be readily achieved by auditing and adapting an organisation/site's communications and digital footprint to ensure that this kind of information cannot be accessed. Sites should also aim to deny the hostile's ability to operate effectively at the site itself – where they can collect information needed to plan an attack. This can be achieved by proactive, friendly engagement by staff, which can maximise the hostile's fear of detection via the organisation's capabilities (such as staff, CCTV, police and other security measures). When the hostile is aware of and/or has sight of these, this can increase their levels of anxiety and cognitive workload as they need to look out for and counter these security measures, which can also help DETER them from continuing these activities. Communications can be used strategically to help with this, by highlighting capabilities in place that can lead to the detection of hostile activity.

DETECT:

Organisations should aim to set up security measures and develop capabilities that focus on facilitating and optimising the detection of suspicious people and activities. This is achieved by providing integrated, effective detection capabilities focussed in the right areas at the site (e.g. where hostiles will have to come to obtain information during reconnaissance, or where pickpocket observation points are). These capabilities include: trained specialist staff, well-positioned CCTV and control room (with operators proactively looking for suspicious activity in areas hostiles are more likely to be), staff who have a customer engagement role, and other staff and the public/venue visitors who are enabled to be vigilant, detect and report concerns via an effective reporting and review system.

DETER:

Deterrence is primarily achieved through corporate communications that regularly promote effective DENY and DETECT capabilities at a location, without including any detail that could enable hostiles to counter them. Simple messaging can deter hostiles, and inform, reassure and help recruit the public and staff to assist with detection efforts.

2 The role of behavioural detection in protective security

A venue may have an effective behavioural detection capability and/or staff who are vigilant and take appropriate action – by seeking to identify suspicious activity as well as dealing with any public reports relating to such activities. However, if this is not visible and/or promoted publicly, then a deterrent effect is unlikely – as the hostile must be in the right place at the right time to see this in action. By promoting security measures and capabilities at the location and online, the venue can create a strong message and digital footprint that tells the hostile that it is not just police or security that they need to be concerned about: Anyone, anywhere, could detect them – and this will be investigated and resolved by expert security staff or the police. This helps create fear and concern about detection, increasing workload (DENY) and anxiety (DETER and DETECT) in hostiles considering operating at a site, be they terrorists conducting hostile reconnaissance or petty criminals.

CPNI has specific guidance on the 3Ds disruption model and products available to assist sites, such as security-minded and deterrence communication guidance and training. For further information, see https://www.cpni.gov.uk/beyond-perimeter.

CPNI strongly recommends that sites and organisations first consider the 3Ds approach to disruption if they are contemplating developing a specialist behavioural detection capability.

If this is not considered, then sites run the risk of conducting activities that may counter the effectiveness of specialist behavioural detection capability. For example, poor staff behaviours that create a perception of an easy operating environment, and online communications that may give away details of behavioural detection tactics and capability.

Considering disruption as a whole (i.e. the 3Ds model) will help ensure that every aspect of your site and resources are used in a coherent and complementary manner to disrupt hostiles. For example, communications can help deter hostiles at the point of target selection – these can make them feel wary if they decide to operate on site because of the effective capabilities that are there to detect them. Communications should focus on security measures that are actually in place, otherwise a hostile may perceive that information being communicated is false (or fabricated) and will not be deterred.

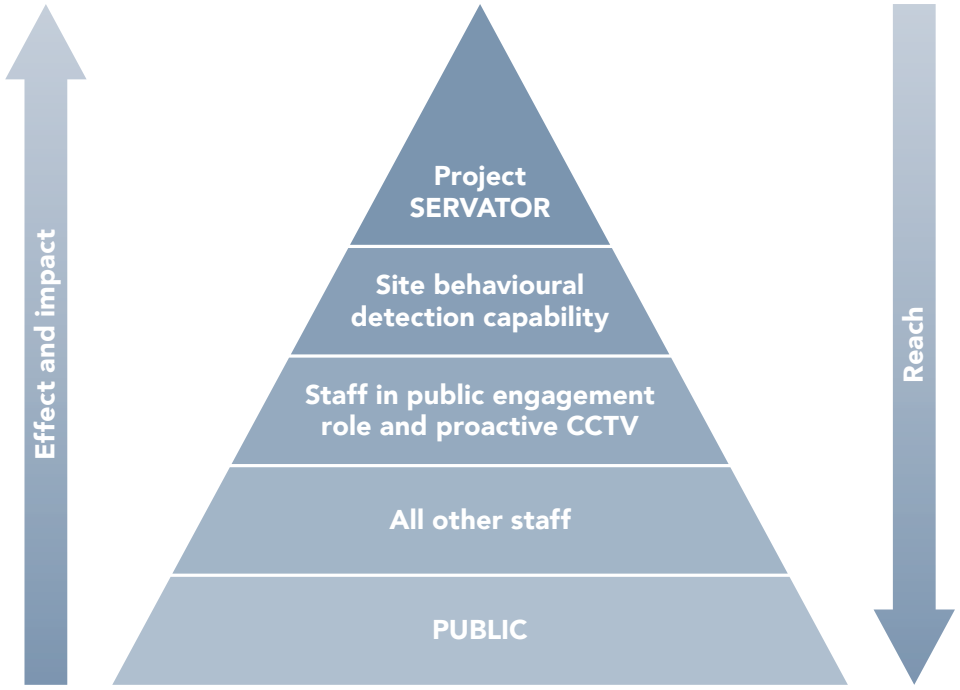
2 The role of behavioural detection in protective security

2.2 The effect and reach of behavioural detection

Staff and the public who are vigilant and report suspicious activity can be a huge 'force multiplier' to complement a limited specialist behavioural detection capability – both in terms of numbers and coverage across the site and times of day – and can help elicit behaviours of concern. For example, in 2015, during a routine security check, a security officer prevented an attacker wearing a suicide belt from entering the Stade de France stadium ground[7]. He was 'just doing his job', but undoubtedly saved lives and mitigated the impact of this co-ordinated terrorist attack.

Figure 2 illustrates CPNI's 'effect and reach' model, which demonstrates using people resource at a site to full effect in order to disrupt hostiles. The further towards the tip of the triangle, the more highly trained and effective the people resource is – but this tends to be very limited in numbers and operation across the site. Lower down the triangle there are greater numbers of people and reach across the site, but these groups are less well trained (e.g. general staff, the public).

Figure 2:
CPNI's 'effect and reach' model



7. https://www.dailymail.co.uk/news/article-3337928/Hero-guard-saved-France-baby-faced-bomber-football-stadium-stopping-sneaking-turnstile-detonating-vest-thousands-fans-President-Hollande.html

2 The role of behavioural detection in protective security

Specialist behavioural detection training typically covers:

- Passive detection – looking for behaviours that may indicate suspicious activities such as conducting hostile reconnaissance or someone behaving atypically from the norm in a particular environment.
- Active detection – using the 'natural' set up of the environment to evoke concern or fear of detection in individuals who have guilty knowledge and hostile intent, such that behaviours (as outlined below) are elicited and are more likely to be displayed in some form (i.e. 'leakage').

Careful consideration should be given to the environment and how the site can be set up. For example, engaging and overt security deployments can be in place at entrance and exit points at a theme park, to observe and potentially influence the responses from people passing through that area. These locations provide 'pinch points' that everyone has to pass through, and therefore provide an opportunity to see if certain individuals respond differently when faced with overt security measures (e.g. canine detection). If it is not possible to set up the environment to help elicit cues, then behavioural detection will be more limited to the passive type outlined above.

Active detection complements measures that aim to DENY and DETER, as this often requires a visible and engaging security presence. Passive behavioural detection is normally more covert and less visible, hence ability to DENY and DETER is more limited. Both approaches require understanding of what is normal for that environment both on that day/time of day, but also in response to the environment set-up.

Section 3:
How behavioural detection works – specialist training

3 How behavioural detection works – specialist training

Table 1 and the following sections of this document provide advice and guidance on what this training should entail and how to obtain it, with a significant focus on specialist behavioural detection training.

Table 1: Capability options that include a behavioural detection component

Capability	Description	Summary of behavioural detection component
PROJECT SERVATOR TOGETHER, WE'VE GOT IT COVERED	National, specialist police capability developed in partnership with CPNI to disrupt hostile reconnaissance and wider criminality via the 3Ds model. Includes specialist behavioural detection capability. For further information see https://www.counterterrorism.police.uk/servator/. Project Servator operates at a range of sites and crowded places across the UK, including events, shopping centres, airports, rail and iconic sites. As such, police may already be deploying Project Servator at a site that is considering the use of behavioural detection and other measures. The deployment of Project SERVATOR and the range of assets used across the UK is effectively managed under a planning and prioritisation process.	Unable to supply for operational security reasons.
Site specialist behavioural detection capability	Specialist behavioural detection officers trained to a high level (as defined in this guidance) to identify and resolve suspicious individuals at a site.	Staff are taught a list of cues, which include behaviours and indicators of concern (e.g. hostile reconnaissance activities and behaviours), and those assumed to indicate emotions such as anxiety and stress due to fear of detection. Cues include: • 'verbal' (e.g. what people do or do not say); and • 'non-verbal' (e.g. facial expressions, body movements, physiological indicators). Good behavioural detection programmes also train people to successfully resolve suspicions, for example, via a 'resolution conversation' or a more formal interview.

3 How behavioural detection works – specialist training

Table 1 and the following sections of this document provide advice and guidance on what this training should entail and how to obtain it, with a significant focus on specialist behavioural detection training.

Table 1: Capability options that include a behavioural detection component

Capability	Description	Summary of behavioural detection component
Staff with a public engagement role/ SCaN for Customer Facing	Staff who can engage with the public, such as roving security personnel and those who act as customer ambassadors. These can be trained to understand what suspicious behaviour may look like on their site, and how to have a polite, but probing, conversation to help resolve suspicions or escalate to a behavioural detection specialist / Project Servator officers (where operational) to resolve.	Staff are educated on the kinds of behaviours and activities associated with Hostile Reconnaissance. For example, people taking particular notice (maybe taking notes or photographs) of security equipment. Staff are also educated on the importance of understanding their own environment and what might be unusual or suspicious activity within this. Staff need to be aware of what is 'normal' and how this can vary according to, for example, the time of day/ week/ year, different locations within their site etc. – in order to detect when something is unusual or suspicious. People are taught to be situationally aware and to report when they detect something 'unusual'. Here the focus is more broadly on 'activities' and 'cues', rather than on specific behaviours. For example, a person loitering in a particular area for a prolonged time for no explicable reason when everyone around them is on the move. SCaN is a free training product available to industry which is delivered against NaCTSO priorities by Counter Terrorism Security Advisors. For further information on this type of training and awareness see: https://www.cpni.gov.uk/security-awareness-campaigns; https://www.gov.uk/government/organisations/national-counter-terrorism-security-office; https://www.cpni.gov.uk/system/files/documents/53/50/Running%20a%20staff%20vigilance%20campaign.pdf For further information on the six SCaN training modules available see: https://www.cpni.gov.uk/Scan
Proactive CCTV control room staff/ SCaN for CCTV Operators/ SCaN for Security Managers	CCTV operators trained to understand when, where and how to proactively look for suspicious activity on their site – that they can refer to roving security personnel and/or behavioural detection specialist / Project Servator officers (where operational) to resolve.	
All other staff/ SCaN for All Staff	Staff with a general awareness as to what suspicious activity and behaviour is at their site, the power of 'hello, can I help you?' in disrupting criminality, and the importance of being vigilant and reporting. The content of this module can also be found in the ACT e-learning https://ct.highfieldelearning.com	
Public and visitors	Public facing vigilance campaigns such as Action Counters Terrorism (ACT) and See it, Say it, Sorted' and other communications to help educate and encourage the public to be vigilant and report suspicious behaviour or activity – as part of their role in helping to keep themselves and the site safe.	

3 How behavioural detection works – specialist training

3.1 Training to spot behavioural cues: Assumptions and limitations

Many providers of behavioural detection training/ capability propose that:

- People with hostile intent will **experience emotions** such as fear, anxiety and stress, because they have 'guilty knowledge' that they are conducting actions which are, for example, illicit and/or illegal, and because they do not want to be caught.
- Hostiles will **exhibit behavioural cues** because of these emotions, for example via facial expressions, body movements, and/or verbal cues.
- These **cues can be reliably observed**.
- Staff **can be taught to detect hostile individuals by looking for these cues**.

This approach is based mainly on evidence from research on detecting deception – how people behave when they are lying and how their behaviour differs to that of people who are telling the truth.

Here there is an assumption that certain cues are a reliable reflection of a person's emotions. However, research has shown that this is not necessarily the case, for example:

Facial expressions may not necessarily reflect how a person is feeling. For example, research has shown that people use their own facial expressions to entice others to engage with them. Therefore, we may smile to invite another person to interact with us, not because we are happy. As such, observing a person's facial expression is unlikely to tell us if that person is experiencing emotions because they have hostile intentions.

Emotional and/or behavioural responses to particular situations will vary between individuals. This can be a result of, for example:

- **Personality differences** (e.g. extroverts seek exciting experiences and need more stimulation to feel excited, so some people may enjoy the thrill of doing something criminal, and be less likely to feel and/or look nervous, fearful)[10];
- **Previous experiences** (e.g. those who have committed crimes before may be more confident and therefore unlikely to feel and/or look nervous)[11]; and
- **Personal preferences** (e.g. people may look nervous in an airport because they are scared of flying, not because they are conducting hostile activities).

10. Ellis, L., Farrington, D., & Hoskin, A. (2019). Handbook of Crime Correlates. New York, NY: Academic Press.

11. Jacobs, B. A., & Cherbonneau, M. (2017). Nerve management and crime accomplishment. Journal of Research in Crime and Delinquency, 54(5), 617–638.

3 How behavioural detection works – specialist training

A number of assessments of this kind of approach have demonstrated that many of the cues people are trained to look for lack any empirical evidence in terms of them being an indicator of hostile intent. Moreover, this approach has the potential for both:

- **'false alarms'** – innocent individuals are identified as potential threats because they are exhibiting behaviours that staff have been trained to look for; and
- **'false negatives'** – individuals with hostile intent are missed because they do not exhibit the behavioural cues that staff have been trained to look for.

Therefore, whilst there is a huge body of research on behavioural cues associated with emotion and deception, when people are being observed in real world environments (e.g. in open, potentially crowded, places) this approach has a high risk of failure, for the following reasons:

3.1.1 Not all hostiles will be or will appear stressed

First, it is incorrect to assume that all hostiles will experience emotions such as fear and stress, and that they will exhibit behavioural cues to indicate that they are feeling this way. **Some criminals and terrorists may not feel nervous if they are confident that they will not be caught, or they may enjoy high stake situations and will therefore not look and/or feel stressed or fearful. This is why the set up and the perception of the environment are vital to consider in any behavioural detection capability.** If the site works comprehensively along the CPNI 3Ds model then it can help create a perception in the mind of the hostile that even a relatively benign environment (e.g. a shopping centre) is actually a high threat environment as there are measures in place to detect them.

In addition, **although hostiles may feel stressed, they can learn ways to manage and conceal their feelings in order to appear confident**. For example, some terrorists and criminals have been known to take drugs in an attempt to calm themselves and conceal signs of nervousness or fear[12].

12. Jacobs, B.A. & Cherbonneau, M. (2017). Nerve management and crime accomplishment. Journal of Research in Crime and Delinquency, 54, 5, 617-638.

3 How behavioural detection works – specialist training

3.1.2
Not all stressed people or people exhibiting particular behaviours are hostile

Some innocent individuals may be mistaken for being a hostile, because they are experiencing certain emotions and exhibiting behaviours that staff have been trained to spot. This issue is particularly relevant in crowded environments, which may be inherently stressful for some people. For example, at a music event, people may be worried when they see security processes in place and/or they may dislike crowded spaces. Moreover, if staff engage with innocent members of the public in a negative way that results in a poor customer experience, this can damage an organisation's reputation. **This is why it is essential to (a) understand the baseline of what is normal for an environment, and (b) follow up any concerns and suspicions with a 'resolution conversation'.**

A resolution conversation is a polite and friendly discussion that involves staff asking probing questions to understand why an individual is behaving in a certain way. Questioning can involve something as simple as asking if the person of concern is okay, or if they need help. The member of staff needs to actively listen to and observe how the individual then responds. If concerns are not resolved and there is no innocent, credible explanation for the behaviours that led to the detection, the member of staff should follow their organisation's process for responding to threats and raise an alarm.

3 How behavioural detection works – specialist training

3.1.3
Even if behaviours are evoked and observable, they may not be seen.

Even if people do feel certain emotions, and exhibit behavioural cues and associated indicators, these cues may not be observable/ seen by others, even when they are trained to do so. That is, behavioural detection is not an 'all seeing, all knowing' capability. It is limited by the attention of the trained observer and what is going on in the environment at the time. It should be noted that:

- **Some cues are hard/ impossible to spot especially from a distance and when it is busy or quiet.** For example, when there is a large crowd at an iconic site where a lot of people are taking photographs, this will make it difficult to spot a hostile taking pictures as part of their hostile reconnaissance activities.
- People may find it difficult to remember all of the cues that they have been taught to look for, therefore they may be more likely to resort to looking for cues they find easiest to remember and/or spot. **This can lead to critical biases such as a reliance on stereotypes of what they believe a hostile is likely to look like.**
- Some behavioural detection training includes 'micro expressions' on the list of cues to look for. However, these are by definition 'micro' (i.e. very subtle) – and therefore most cannot be detected at a distance, and are often said to be hard to detect even during a close-up conversation. Some micro expressions last only a fraction of a second, and as such, can only be observed when watching recorded video that has been slowed down. **Therefore, detecting hostile intent via micro expressions is not practical in real-world situations, especially in large, crowded places. There is also a lack of evidence that technologies can detect hostile individuals via micro expressions, even when they are designed to do so and advertise that they can.**
- The hostile actor may simply be out of sight (e.g. hiding from, or in an area where there is no behavioural detection capability).

3 How behavioural detection works – specialist training

3.2 Addressing the limitations of this approach

When seeking to detect hostile actors via their behaviours and activities we need to consider the following:

- **We need to understand how a particular individual of interest usually behaves in the context that you are observing them in:** This can vary dramatically depending on a range of contextual factors. If you do not have this 'baseline', you cannot detect when someone is acting out of the ordinary.

- **Rather than providing a list of behaviours to look for, training and guidance should provide 'hand holds'** – these are examples of the kinds of things that might be unusual in a specific environment and context – as this is more likely to be an effective behavioural detection approach. 'Hand holds' may include looking for people: with an unusual appearance/attire or belongings (e.g. different to the majority of people in the same context), expressing extremist views, or making threats; loitering near staff-only areas or outside normal dwell zones; seen in multiple areas, outside of a usual journey or work pattern or timeline; attempting to photograph or film security areas or taking measurements/notes of their surroundings; and/or acting in a furtive or secretive manner (avoiding security personnel, CCTV, eye contact or interaction with others), engaging with staff to ask probing or inappropriate questions (e.g. about security measures and staff routines).

- **It is vital that any behavioural detection training includes techniques for successfully resolving suspicions, rapidly and effectively in a short and friendly interaction** – because the majority of behavioural detections are likely to have an innocent explanation. **Without this, suspicions will not be resolved and an innocent member of the public may be made to feel they have been treated like a criminal.**

Section 4:
How behavioural detection works for wider staff and public

4 How behavioural detection works for wider staff and public

4.1 What to look for

An alternative (or complementary) method to detect hostiles is to enable people (staff and the public) **to learn, be aware of and look out for:** (a) What is 'usual' for their environment, and how this varies according to context; and (b) When something looks or feels 'unusual' for that context.

4.2 Looking for the unusual: Strengths of this approach

This approach does not assume that hostile individuals experience and exhibit signs of certain emotions, and has been developed and applied to different environments (e.g. on trains and at bus stops and stations) as a key part of a range of security measures (e.g. the 'See it, Say it, Sorted' DfT campaign).

Rather than training people to look for specific behavioural cues (as described in Section 3.1), facilitating the reporting of anything unusual may be a more effective approach to detect hostile acts, as it is more encompassing and does not focus on specific behaviours. Something 'unusual' might include unusual clothing (e.g. a padded jacket on a summer's day), or a vehicle parked in an unusual location. These examples demonstrate how the concept of looking for the unusual is likely to be more effective in detecting hostiles compared to relying on a list of behaviours:

Wearing a padded jacket could not be included on a generic list of 'behaviours' to look for, but when observed in context may help in detecting a hostile[14]. Otherwise there is a risk that people will rely on 'mental shortcuts' (e.g. stereotyping) to detect potential hostiles.

This approach overcomes the issue of behaviours being context-specific. Whereas looking for behavioural indicators of emotions can be affected by the context (e.g. how confident and experienced the hostile is, how nervous and stressed the non-hostile individuals in the same environment are likely to be), this approach relies on people (staff and the public) having intrinsic and 'expert' knowledge of their environment and knowing when things look or feel out-of-place within that context. For example, what passengers usually do at a train station may vary depending upon the station, time of day and day of week.

14. https://www.independent.co.uk/news/world/europe/istanbul-airport-attack-ataturk-suicide-bombers-images-video-latest-news-a7110536.html

4 How behavioural detection works for wider staff and public

4.3 Responding to suspicions

The public should be encouraged and enabled to report (e.g. directly to staff, via a telephone call or mobile text message to appropriate authorities) and where possible, thanked for making the report. People can be encouraged and enabled by **promoting reporting as a 'civic duty'** – that can benefit themselves and others, **enabling people to be capable of reporting** and ensuring **that they are confident to report and are assured that their concerns will be dealt with appropriately.** This relies also on the organisation taking appropriate and timely action to investigate and resolve these reports, and to give feedback where possible to demonstrate that reporting is acted upon proportionately and appropriately. For further information and products see:

https://act.campaign.gov.uk/

When someone or something unusual is identified, staff should attempt to resolve their concerns via a follow-up interaction or escalate as required, as quickly as possible. Organisations also need to have in place an effective system to investigate reports such that they do not go into a 'black hole'. For example, if a member of the public reports to a member of staff, that employee needs to understand the importance of investigating or escalating immediately, and that there is a system in place that will seek to investigate and resolve the report. Ideally organisations should 'stress test' this system by 'mystery shopping' – deliberately planting a suspicious activity report from a 'stooge' member of the public via various mechanisms to ensure it is enacted on. Revisions to the system can then be made if required.

It is vital that sites have controls in place to stop someone carrying out an inappropriate action, for example calling 999, unlawfully detaining someone or in a worst-case scenario assaulting a member of the public.

Section 5:
Key components of good, specialist behavioural detection

5 Key components of good, specialist behavioural detection

5.1 Key considerations

What are your goals and priorities?
In terms of whether you are trying to detect, deny and/or deter the hostile and the current threat for your environment. For example, your priority might be to deter low level crime in a shopping centre, in which case specialist behavioural detection may be considered unnecessary. Or you might be responsible for detecting more serious criminal or terrorist activities at a tourist site, in which case specialist behavioural detection may have some benefit.

What is your environment?
Does it lend itself to behavioural detection via measures already in place (e.g. airport style screening) or will you need to put more dynamic measures in place to shape the environment to help elicit behaviours of concern? For example, via communications and deployment of visible security/customer engagement assets?

What are your available resources?
The potential success of behavioural detection may rely on factors such as how many staff you have, available budgets for staff and levels of training, the size of your location and the potential reach and impact of those who are trained.

Is your capability able to coordinate and integrate effectively with other measures?
To have maximum benefit, behavioural detection capability must coordinate with other security capabilities in place (e.g. Project Servator deployments (where operational), links to CCTV Control Room Operatives etc.). If you have staff and public vigilance initiatives in place, are your behavioural detection officers able to rapidly resolve suspicions that are flagged? Do you have the mechanisms in place to support this? For example, when a member of staff raises concern to your control room, the control room will contact behavioural detection officer(s) to investigate and resolve in a timely manner.

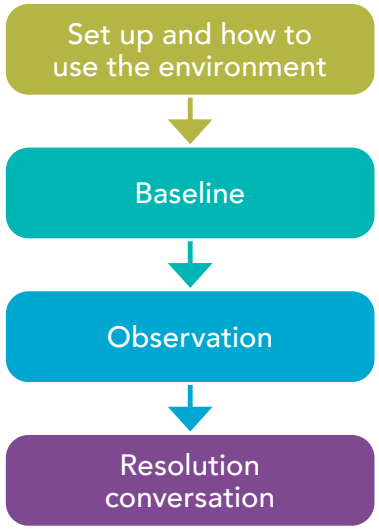
Have you made the most out of your other capabilities to DENY, DETECT and DETER (as outlined in Section 2.1), and are these working in synchrony with your capability and not against it?

Do you have the ability to collate and analyse evaluation measures?
As outlined previously, this is vital to know if your behavioural detection capability is working effectively and to defend it against any accusations of profiling particular groups or individuals (see Section 7 for guidance on evaluation).

5 Key components of good, specialist behavioural detection

5.2 Training components

Below illustrates the key components of good and comprehensive behavioural detection training.



Set up and use of the environment – If behavioural detection is likely to be 'Active', then training should include how to set up the environment, in order to stimulate fear of detection and to facilitate observations that might lead to detection. If more 'Passive' it should still include consideration of how and where the 'natural' environment may elicit behaviours and where, when and how a hostile is likely to operate. For example, when conducting hostile reconnaissance at a site, a hostile is most likely to be in areas where they can collect key information – e.g. staff movements around an entrance. As such, behavioural detection capability can be deployed strategically to maximise opportunities for staff to observe hostiles, and for hostiles to see staff in action.

Baseline – Training must include the importance of understanding the norms of the environment, and how to determine what might be unusual or suspicious in that environment – with and without any 'active' set up. Without this vital component, there is a high likelihood of false positives and negatives.

Observation – Training on how to recognise cues, why they may be exhibited (above and below the baseline) and how to determine the threshold of when this can be categorised as suspicious and worthy of further investigation. This should also include potential errors in observation and how to be aware of and mitigate these.

Verbal cues – What people say and how they say it can be one way to detect hostile individuals, for example if they struggle to answer questions that should be easy to answer, if their 'story' doesn't make sense or if they contradict themselves. In contrast, relying on non-verbal cues (e.g. if a person seems anxious or scared) is likely to lead to false positives and false negatives.

5 Key components of good, specialist behavioural detection

Resolution conversation – Training should include how to have friendly, polite but probing conversations via a short interaction in order to resolve suspicions. This is absolutely essential to the success of any behavioural detection capability. Without it, the potential for damaging false positives (e.g. members of the public who may be showing signs for innocent reasons) and missing true positives (letting someone with malicious intent go) is high. These kinds of conversations provide customer service to innocent members of the public, can increase customer satisfaction, and may lead to staff helping people who may be distressed because, for example, they are lost, late, or have mental health issues.

5.3 Developing and maintaining capability

Behavioural detection is a specialist skill – not everyone can do this – and it is one that needs to be practiced regularly so that skills are maintained. **It is important to note that staff who have undertaken only basic security awareness training should not be referred to as trained behavioural detection personnel.**

People with the necessary attributes (e.g. having natural observation and personal interaction skills) will perform more easily and effectively, and therefore training selection should seek to identify those with these skills and filter out those who do not enjoy interacting with the public.

Once trained, specialist skills then need to be maintained. As with any specialist skill, trained people need use their skills on a regular basis to ensure currency, and continued professional development is essential.

Evaluation is also essential – recording and analysing the outcomes of behavioural detection, both positive and negative, is vital to determine if training has been of benefit and if the capability is deploying to good effect (and therefore worthy of continued development and investment). Evaluation is also needed to ensure that it is not accidentally biasing or profiling certain visitors at a site (e.g. based on their gender, race or mental health issues). Indeed, reliable data is vital to defend the capability, should staff decisions and responses based on behavioural detection ever be raised, challenged or questioned.
See Section 7 for further insight into evaluation.

Section 6:
Procuring specialist behavioural detection training, technologies and tools

6 Procuring specialist behavioural detection training, technologies and tools

There is a range of behavioural detection capabilities available, in terms of training, technologies and tools. These vary dramatically in terms of their objectives, approaches and methods, and in terms of their effectiveness and successful implementation.

Companies should provide training that follows the structure and content outlined in Section 5.

Behavioural detection that does not include a resolution conversation to resolve suspicion should be avoided due to risk of false negatives and positives. Staff should be trained to interact with the public. Moreover, at sites where persons of concern can be/need to be interviewed, specialist staff should be trained in (i) how to effectively interview, (ii) how to look for cues of deception, and (iii) how to elicit cues of deception.

When considering behavioural detection training, companies should be required to provide evidence of how their approach and methods are applicable to: (i) requirements and environment; (ii) available resources; and (iii) existing measures and processes. They should also set out a clear plan of how they will measure (and/or how they will help to measure) and demonstrate success and impact.

Companies should be able to provide quantifiable evidence of the effectiveness of their training – not anecdotal examples or testimonies from satisfied customers – but clear and robust evidence (e.g. data) that demonstrates increased detection performance (after training, compared to pre-training). (Other measures can also be used as evidence of disruption, as discussed in Section 7.)

When procuring equipment and technology, organisations should again require suppliers to demonstrate how this will work for them. Companies should be expected to provide evidence that their product will be effective, and guidance on how this will specifically meet the organisation's requirements. Section 7 provides further details on evaluation of training, technology and equipment.

Procurement decisions should never rely on the background and experience of the supplier (e.g. ex-military / intelligence staff). Moreover, customers should be wary of 'scientific' looking papers and where possible, get these reviewed by a scientist in your team or by an independent expert. **Suppliers should also be required to demonstrate that their products (training/ technology/ equipment) will not have a negative impact on normal site users.**

The Register of Security Engineers and Specialists (RSES) has been established to promote excellence in security engineering and provides a benchmark of professional quality against which its members have been independently assessed. Organisations who supply behavioural detection training are encouraged to engage with this process. It offers potential clients the assurance that registrants have achieved a recognised competence standard through a professional review process.

For details about applying for the register and the application process please see https://www.cpni.gov.uk/register-security-engineers-and-specialists-rses

Section 7:
Evaluating your behavioural detection capability

7 Evaluating your behavioural detection capability

7.1 Key considerations for measuring effectiveness

It is important to understand that:

- **Simply providing staff trained in behavioural detection does not equal success.** Those considering the use of behavioural detection need to identify what they want to achieve (i.e. their 'measures of effectiveness').
- Single measures alone cannot provide a full picture of this: **A range of measures are best; which can then be triangulated to evaluate the impact** (e.g. on-the-spot arrests, number of reports, quality of reporting, number of complaints and other customer feedback).
- **Covert testing can provide insights and evidence of the effectiveness of behavioural detection, but this can be complex and costly** in terms of the time, effort and resources required to organise, run and manage.
- Behavioural detection can be applied to deter and disrupt criminal acts as well as terrorist attacks, but **measuring deterrence is hard, if not impossible, in most real-world contexts**.
- **One preferred proxy measure of deterrence is 'red teaming'.** This is usually delivered by an external company with the relevant skills and expertise to adopt a hostile 'mind-set' and evaluate the security posture and potential vulnerabilities of specific locations and sites.

7 Evaluating your behavioural detection capability

7.2 Evaluating behavioural detection capabilities: A 10-point checklist

Organisations should use the following checklist to ensure that they have sufficient evidence that behavioural detection is suitable and likely to be effective at their site. This can be applied to the procurement of behavioural detection training, technology and/or equipment.

1. Organisations first need to consider what they are seeking to achieve, in order to determine appropriate measures of 'success'/'impact' regarding behavioural detection capability. Organisations also need to consider their available resources, in terms of staff numbers and funding to spend on (i) the initial outlay, (ii) the ongoing maintenance, and (iii) the evaluation of their behavioural detection capability.
2. Organisations should explore different options regarding different behavioural detection products and different potential suppliers. They should discuss their requirements and available resources with potential suppliers. Suppliers should help them identify options and provide advice to help with this decision.
3. Organisations should only consider procuring products (training/ equipment/ technology) that have already been deployed and tested (or at least trialled) at a site similar to theirs (in terms of size, footfall, layout, numbers of staff etc.).
4. Suppliers should be required to describe and explain how they have previously tested/ trialled their product, and the metrics that were chosen to test their product. This could include measuring the number of 'stops' and referrals to the police made by staff trained in behavioural detection, customer satisfaction scores, and a baseline assessment of security measures made by Red Teaming experts.
5. Suppliers should present evidence that they have collected data on their chosen metrics before and after the implementation of their product at a similar site.
6. Suppliers should clearly outline how they collect data on these metrics. For example, self reports from staff and/or the public, observations of staff, data from the police, Red Teaming.
7. Suppliers should demonstrate that they have measured the effectiveness of their product by analysing data collected before and after the implementation of their product. This analysis should show that this resulted in a positive effect (e.g. more 'stops' and referrals, increased customer satisfaction scores, increased deterrence effects as assessed via Red Teaming experts).
8. Suppliers should provide detailed guidance and advice on the best deployment approach for your site, for example, in terms of where and when to deploy their product at the site to maximise its impact.
9. Suppliers should design a plan of how they will trial/test their product at your organisation's site(s).
10. Suppliers should demonstrate how their product is practical, feasible, affordable and proportionate to your organisation's requirements and available resources.

7 Evaluating your behavioural detection capability

7.3 Evaluating the evidence: A final note

It is worth noting that behavioural detection has only been properly tested against criminal activity[16]: As yet, we do not have robust evidence that it can be effective in the detection of terrorists. This is because it is hard to collect data due to the low number of terrorist activities that might actually be observed by those trained in behavioural detection: This has resulted in a lack of quantifiable data on terrorist activities. However, significant effort has been made to understand how lessons from the extensive literature on criminality can be applied to understand and disrupt terrorists. Research has demonstrated that these different types of hostiles think, feel and operate in the same way[17]. We do not yet have significant evidence that behavioural detection can be effective in disrupting terrorist activities. However, our research suggests that it is very likely that it can.

16. https://www.cpni.gov.uk/disrupting-hostile-reconnaissance
17. Unpublished academic research that included an analysis of 90+ terrorist autobiographies and a synthesis of court, police and open-source documents regarding over 100 terrorist plots.

Section 8: Conclusion

Behavioural detection capability has the potential to detect, deter, and deny hostiles from operating in a range of contexts and environments. However, behavioural detection should only be deployed as part of an integrated system to ensure that it complements and is complemented by other security measures. It is important that the set-up of the environment is conducive to and organised in a way that can maximise the potential success of behavioural detection, and that training provides skills and techniques that are evidence-based and tailored for different audiences. Those considering the procurement and deployment of behavioural detection capability should ensure that they do so in an appropriate and proportionate way and have the resources to do so. The guidance provided here aims to assist those responsible for the security of different environments, to ensure that any application of behavioural detection meets requirements, is effective and is successful.

CPNI
Centre for the Protection of National Infrastructure

ACT
ACTION COUNTERS TERRORISM

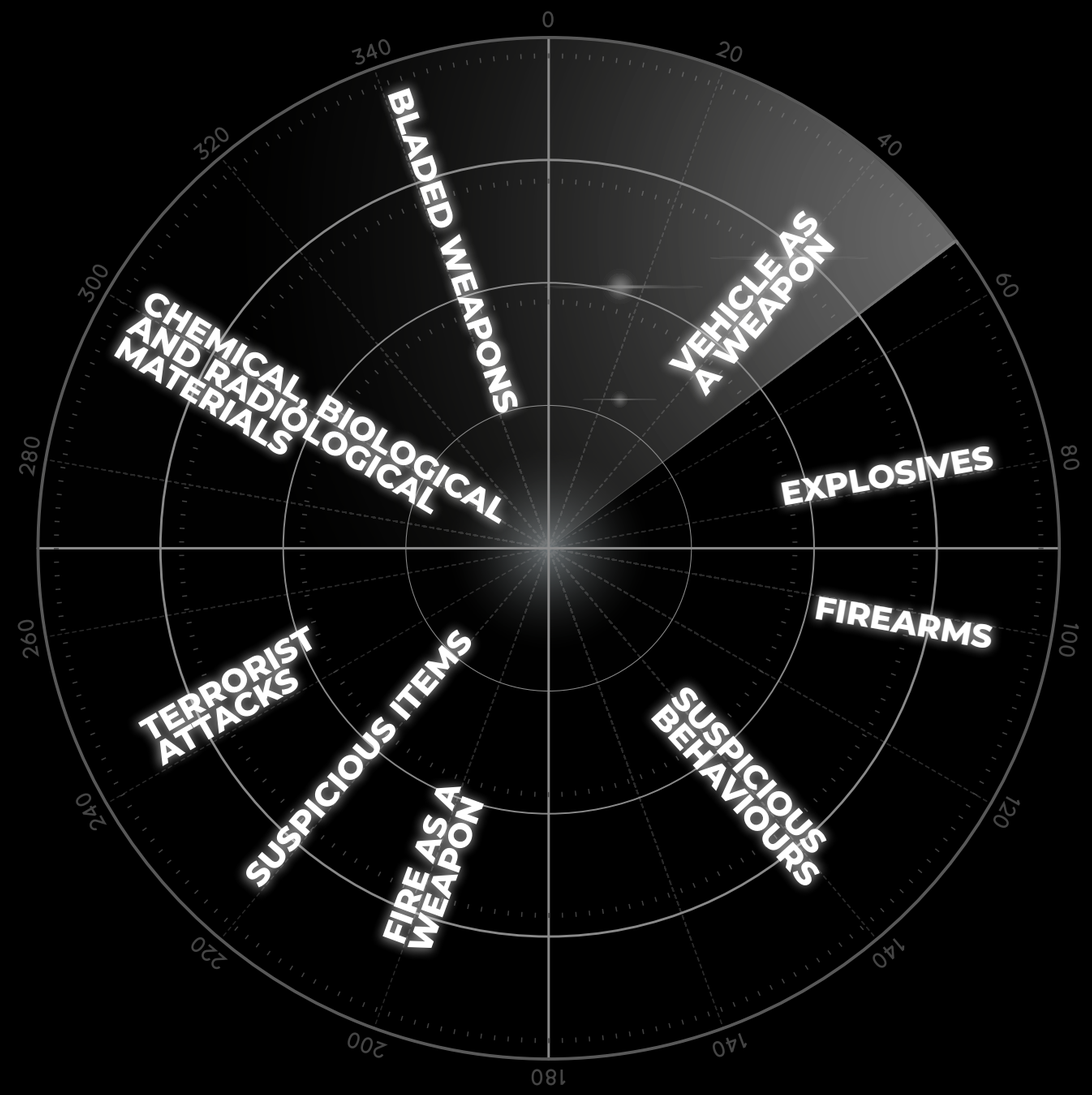
FURTHER GUIDANCE

CPNI provides a range of guidance products to help sites protect and mitigate against a variety of threats. For further information visit the CPNI or NaCTSO websites.

www.cpni.gov.uk

www.gov.uk/nactso

If you require further information please contact your CPNI adviser or your local Counter Terrorism Security Adviser.



RECOGNISING TERRORIST THREATS

For the security professional

CPNI
Centre for the Protection of National Infrastructure

ACT
ACTION COUNTERS TERRORISM

The UK faces a serious and challenging threat from terrorism. Acts of terrorism vary in scale and purpose. They are often violent and indiscriminate with far-reaching consequences.

This guide contains helpful information for security professionals to improve their ability to recognise threats, their key components and other attack indicators and to respond appropriately.

Your security manager will be able to provide you with more details on the measures in place to protect your site. Additional guidance is available on the CPNI and NaCTSO website.

www.cpni.gov.uk

www.gov.uk/nactso

CONTENTS

THREATS

When assessing the threat, it is important to consider both where you are working and who or what you are trying to protect. You can be sure that your attackers are doing the same.

It is possible that any of the threats covered in this booklet could occur and the specific threats that you face could change rapidly. Therefore, it is essential that you understand the current risks associated with your site and any vulnerabilities.

Different attackers will use different tools and methods depending on their competence, experience and what they have available to them. Physical attacks can have different levels of sophistication and could be made up of a combination of one or more different methodologies.

It is important to keep a wider situational awareness, even when dealing with incidents and ensure that all issues are reported, as attackers may take advantage of external events.

Whilst there are a significant number of possible attack methodologies, there are some methods that appear frequently, both in attacks and terrorist instructional media.

These include the use of:

- bladed weapons
- firearms
- vehicle as a weapon
- fire as a weapon
- explosives
- chemical, biological or radiological materials

The above methods are not all equally likely and will be influenced by a number of factors including the availability of materials, instructional media, publicity and overall difficulty, both actual and perceived.

What threats are you protecting your site from?

Whilst on duty or during your everyday life it is important to maintain good situational awareness, looking for items, people or events that are out of the ordinary.

The combination of these indicators may provide you with a greater understanding of the situation. It could be your vigilance that provides the warning necessary to prevent a terrorist attack.

SUSPICIOUS ITEMS

H Is it **hidden** from view, not in clear sight?

O Is it **obviously** suspicious because of its appearance or the circumstances of its discovery?

T Is it **typical** of what you would expect to find in this location?

BRITISH TRANSPORT POLICE

Pre-attack indicators, both obvious and subtle could include:

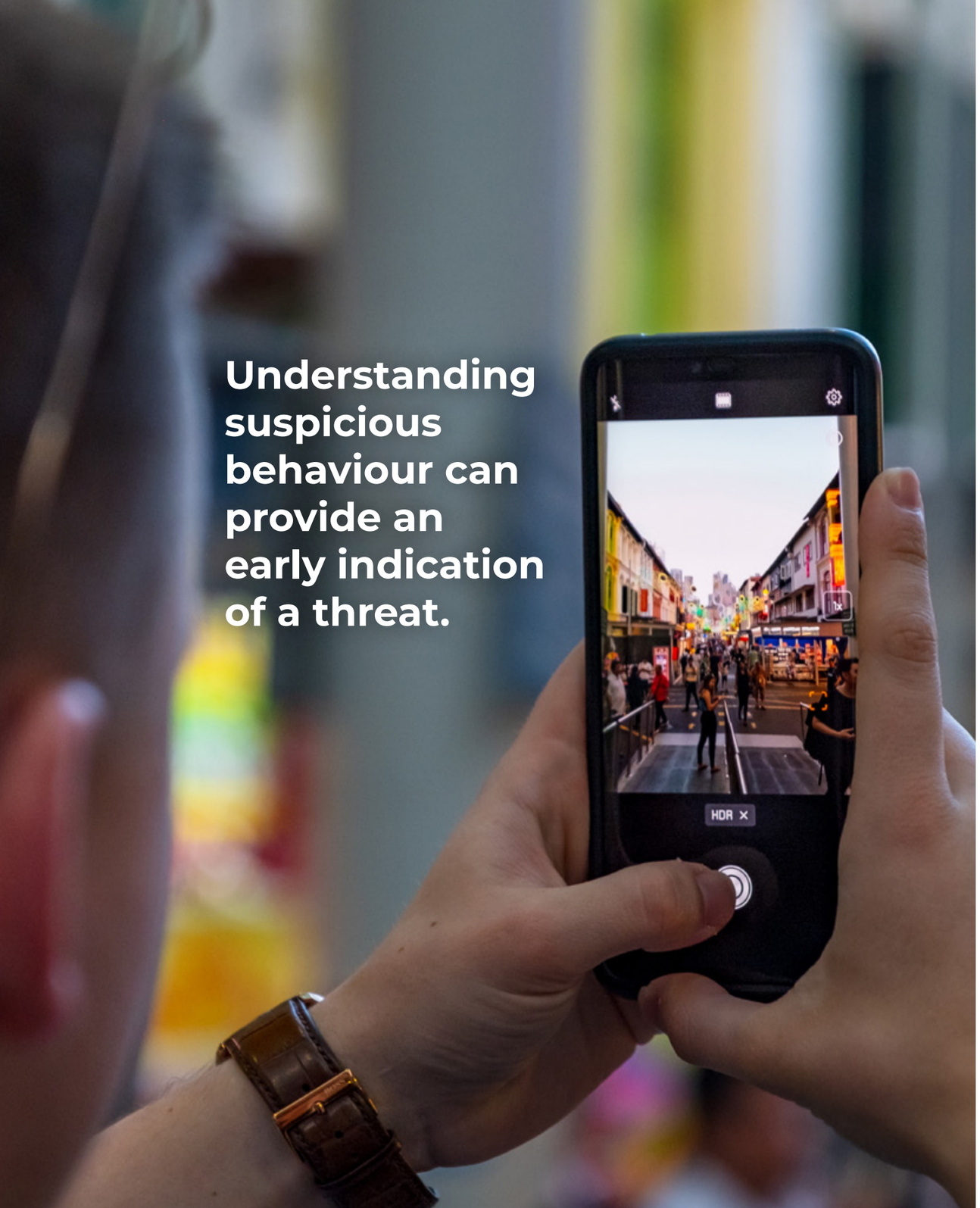
- Presence of a firearm or bladed weapon
- Frequent sighting of the same vehicle either parked or moving
- Unusual, dangerous or erratic driving
- Vehicles parked or driven in an unusual location
- Bulky or non-typical clothing
- Bags, cases or other items that are out of place
- Unusual items or combinations of items
- Items that show signs of tampering
- Unusual odours.

This list is not exhaustive. Suspicious items and other indicators should be considered in context on an individual basis using the H-O-T protocol.

A pre-attack warning may be given, in this case you should follow your local response plan.

?

What would you consider suspicious at your site?



SUSPICIOUS BEHAVIOURS

The behaviour of individuals or groups prior to an attack may give an indication of their intentions and provide opportunities for disrupting their plans.

- **W** **What** - are they doing?
- **H** **How** - are they behaving?
- **A** **Alone** - or acting with others?
- **T** **Threat** - what type do they pose?

By understanding when suspicious behaviour, such as hostile reconnaissance, can occur and how individuals undertaking it may feel, you have an early indication of potential attack planning and the opportunity to disrupt attacks.

Prior to an attack, it may be necessary for individuals to undertake final preparations such as readying a weapon or priming a device. This behaviour may appear suspicious or out of the ordinary for your location. The W·H·A·T protocol should be considered when evaluating suspicious behaviour.

BRITISH TRANSPORT POLICE

?

Do you actively look for individuals or groups undertaking suspicious activity at your site?

What would suspicious behaviour at your site look like?

Have you identified locations on your site where suspicious activity is likely to go unobserved?

PROHIBITED ITEMS

It is an offence to carry certain items in public without relevant licences. This includes some sharp or bladed weapons, improvised weapons, firearms and certain hazardous chemicals.

If you see anyone carrying one of these you should report it to the police immediately.

Sites should have policies defining the items that should be prevented from entering the site. As well as explosives and weapons these prohibited items may include aerosols, fireworks, flares, protest items or electronic equipment including phones and cameras. Categorising items as essential to detect or desirable to detect may help you prioritise your detection requirements.

The security procedures to identify and prevent access of these items will differ between sites, but may include search and screening procedures. Implementation of search and screening procedures, relevant to the site requirements, will help prevent carriage of prohibited items onto site.

?

What items are essential to detect on your site?

Do your search procedures allow you to identify prohibited items?

What is the procedure for dealing with prohibited items?

TERRORIST ATTACKS

Terrorist attacks can be fast-moving, violent incidents where assailants may move through a location aiming to find and kill or injure as many people as possible. Most deaths occur within a few minutes from the start of the attack.

The different methodologies that could be used during an attack, either individually or in combination, are:

- bladed weapons
- firearms
- vehicle as a weapon
- fire as a weapon
- explosives
- chemical, biological or radiological materials

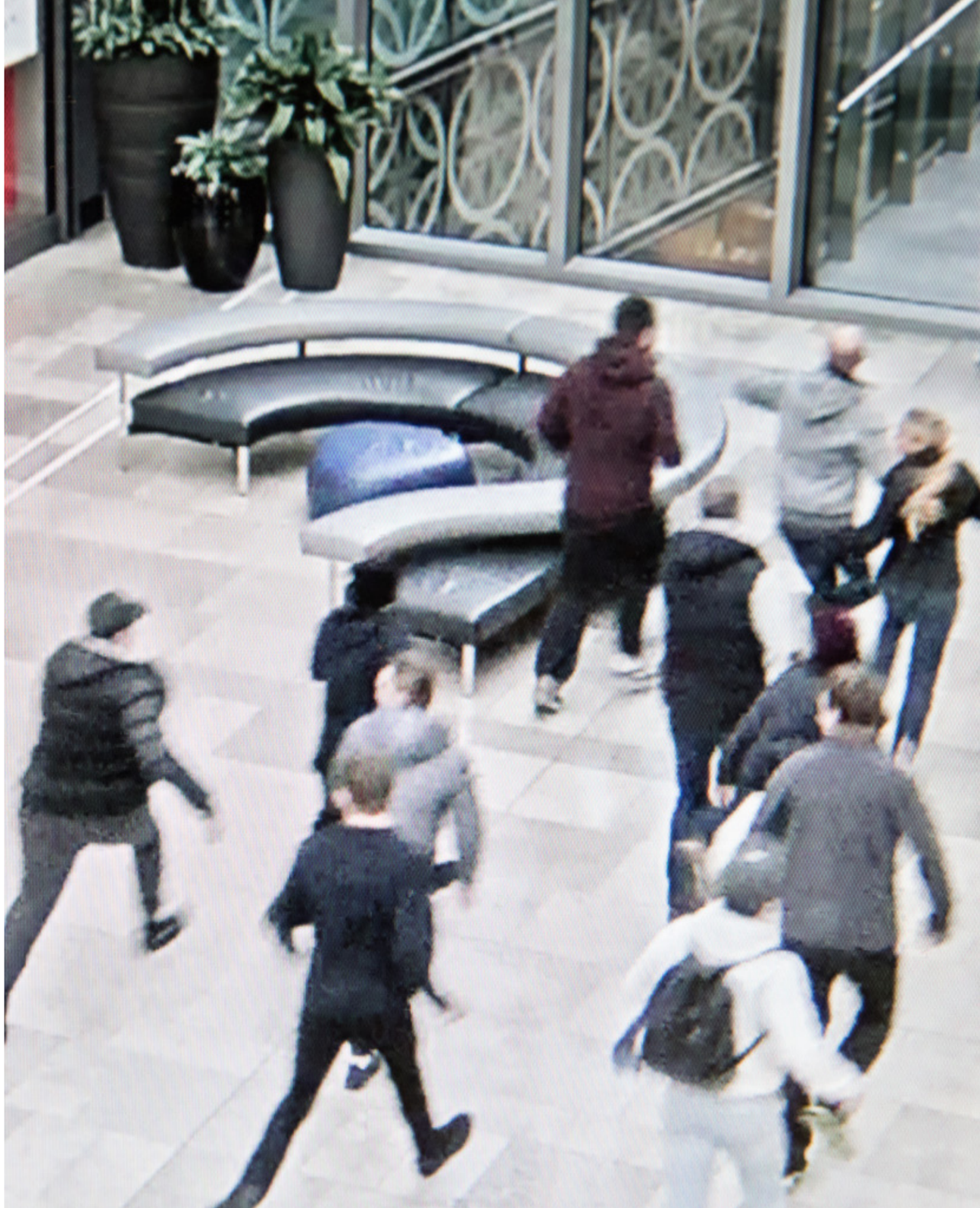
An attack could unfold in many different ways and there is not a set order that terrorists always follow. The situation is fluid and weapons and targets can be opportunistic. There could be a combination of methodologies, such as an initial vehicle as a weapon phase or explosive attack, with the terrorist taking advantage of the subsequent confusion to conduct further attacks. Therefore, it is important to maintain an awareness for potential secondary attacks, especially during the aftermath of a major incident. Critical decisions will need to be made under severe time pressure.

An attack could take place in the public realm, a privately owned/operated space or crowded place. Bear in mind the attack may not be stationary and could move between these areas.

How would you spot an attack starting?

Could you prevent an attacker gaining entry to your location?

Have you determined what areas could be vulnerable to an attack?



ATTACK INDICATORS

There are a number of indicators that an attack has started. These include sights, sounds and smells.

Visual

- Individuals running into or out of a building or crowded space
- People moving together in the same direction, forming a crowd
- Dead or dying animals, birds or plants
- Unexplained smoke and/or fire
- Structural damage e.g. windows blown out
- Unusual presence of chemicals, such as liquids, powders or vapours.

Sounds

- Alarms, including fire alarms, panic alarms and attack detection systems
- Gun shots
- Screaming
- Vehicles revving their engines or accelerating quickly
- Tyres screeching
- Unexpected sounds of objects being crashed into
- An explosion.

Casualties

- Casualties can be an indicator of an attack, consider in conjunction with other indicators
- Multiple casualties in close proximity for no obvious reason (e.g. without any other indicators) – consider whether to proceed – this could be an indicator of a CBRN incident.

Context

- Each scenario will require your own experience and organisation-specific context to determine its nature e.g. suspicious indicator combinations or number of unexplained casualties.

?

Would you recognise the indicators of an attack?

Have you considered your response to a terrorist attack?

BLADED WEAPONS

There are restrictions on the purchase and carriage of bladed weapons in the UK. However, they are available legally on the high street or via the internet throughout the country.

Most bladed weapons are metallic, but other materials, such as ceramic blades, are becoming more common. Depending on their size, bladed weapons may be concealed on a person or in a bag or other carried item.

Everyday items, such as tools, also have the potential to be used as offensive weapons so it is important to consider the context in which any such items are being carried.

?

How likely is the item to be used to cause harm or disruption?

What potential threat items are readily available at your location? e.g. for sale to the public.

FIREARMS

Firearms are not widely available to the UK public, but they can cause serious harm and disruption in the wrong hands.

Firearms can be classified according to a number of different features, however, their general function remains consistent. Broad categories of firearms include handguns, shotguns and rifles. Some common features that aid identification include:

- barrel
- trigger
- magazine
- ammunition
- firing pin.

The firearm may be a fully functioning weapon, deactivated (so not a threat to life but will still cause fear and panic in a terrorist incident) or it may be broken down into component parts. The components can be made using different materials, including different metals and plastics, and may be disguised to look like other objects.

Should a firearm attack occur it is likely to be well planned and may feature multiple attackers. Therefore, it is important to maintain a high level of vigilance, even when you believe you have identified all threats. The police response to a firearm attack will involve armed officers. They will want to know how many attackers are present and if the weapons they are armed with have a long barrel (e.g. rifles) or short barrel (e.g. handguns). You do not need to provide specific makes and models.

PARTS OF A FIREARM

What procedures do you have in place if you find a firearm, ammunition or firearm components?

VEHICLE AS A WEAPON (VAW)

Vehicles (such as cars, vans and lorries) are widely available and easy to use. Consequently, driving a vehicle into crowds of people is a common attack method compared to more complex alternatives.

Vehicles may be purchased, rented, stolen or hijacked by terrorists. Whilst it is possible to prevent vehicles entering specific areas, it is often not practical or proportionate to protect everywhere from a VAW attack.

In general, VAW attacks have been the first part of a layered attack. The attacks frequently begin on public roads with little or no warning and are often followed by a wider firearms or bladed weapon attack.

During a VAW attack, the terrorist is unlikely to comply with the rules of the road. Terrorists may park illegally just before the attack then speed, ignore traffic signals, drive on the wrong side of the road, mount footways and enter pedestrianised zones.

However, as attackers intend to harm as many people as possible during a VAW attack, they are unlikely to drive in a manner that risks ending the attack prematurely, rendering the vehicle unusable or seriously injuring themselves. Consequently, the terrorist may tend to avoid obstacles, including relatively insubstantial ones.

The end of a VAW attack may look similar to a road traffic incident: the vehicle losing control and crashing into barriers, buildings, street furniture or other vehicles. Individuals may approach the vehicle to help the occupants, inadvertently becoming targets for a follow-on bladed weapon or firearms attacks.

?

Does your site have areas where people congregate and can a vehicle drive at speed into them?

What vehicles do you expect at your site and where? Which ones would stand out?

What does 'normal' driving behaviour look like at your site?

Are there times of the day when you need to be more aware of vehicle movements?

FIRE AS A WEAPON (FAW)

FAW is the deliberate use of fire with the intent to cause harm. This may include death or injury to people, premeditated damage to property, or a combination of both.

A FAW attack may not require extensive planning. However, due to fire legislation and emergency service cover in the UK, should a fire start, it is unlikely that the fire will spread uncontrollably. Fires are normally quickly reported and result in rapid responses from the emergency services.

FAW can be employed as a distraction tactic, as a means to augment another methodology, or as a disruption or deterrence to the standard emergency services response. Devices used in FAW may contain petrol, flammable gas cylinders and other flammable materials within their device. Attackers may not have received extensive training or undertaken significant planning.

?

Have you considered the impact of a fire on your ability to respond to an ongoing attack?

Would your overall response to a terrorist attack change if the building was on fire?

EXPLOSIVES

Explosives have been used by terrorists for a variety of different goals, including to cause mass casualties or fatalities, destruction of property and infrastructure, assassination of specific individuals, armour penetration and for incendiary purposes.

There are various sources of explosives including military, commercial or improvised explosives. Within the UK, military and commercial explosives are not widely available to the public and there is regulation controlling access to the chemicals required to make improvised explosives.

However, attempts to use explosives as a method of attack continue to be seen.

An explosive will typically be deployed as part of an Improvised Explosive Device (IED) and will cause damage through blast, fragmentation and thermal effects.

Explosives have a wide range of different appearances and colours, including crystalline powders, liquids, gels or putty-like materials.

Explosives are hazardous, both chemically and explosively. Any packaging or container may display hazard or warning symbols or contents descriptors; however, these may not be accurate or could have been removed.

?

What are your local procedures if explosives are found?

Do you have plans for evacuation away from suspected explosives?

CHEMICAL, BIOLOGICAL OR RADIOLOGICAL (CBR) MATERIALS

CBR encompasses a vast range of potential attack methodologies that could cause both harm to people and, potentially, damage to infrastructure.

CBR materials are typically not available to the public, and due to their inherent hazards, specialist handling equipment may be necessary.

Attacks can involve the use of corrosive or flammable chemicals, toxic materials or radioactive sources. The damage and injury caused by a CBR attack depends on the material and the manner in which it is used, for example as a device or by introducing the material into the environment.

Their appearance can vary widely from a solid to a liquid or gas and they may be colourless, odourless, and require specialist equipment for detection. Solid forms can include gels, putties or crystalline powders. The small quantities of CBR materials present is not a good indicator of the potential harm; small quantities of certain chemicals can result in large numbers of casualties.

If using a commercial or industrial material, the packaging may display hazard labels or contents descriptors. However, these may have been removed.

?

Are you aware of indicators for a CBR attack?

Have you got procedures in place for responding to a CBR attack?

IMPROVISED DEVICES

Explosives and some CBR materials may need incorporating into a device to function successfully.

In addition to the chemical, biological, radiological or explosive materials, a device is likely to contain certain key components:

- packaging
- switch or timer and power source
- initiator
- dispersion method.

There are a number of methods for the deployment and firing of improvised devices, these can be combined to produce many different types of devices. Different devices could be hidden or abandoned at strategic locations, attached under vehicles or transported to targets by suicide operators. Common firing methods include switches, timers, remote control, mechanical and victim operated (which could include anti-handling measures).

The size of the device will depend on the goals of the terrorist, their knowledge and the materials available. Terrorists will have to balance the challenges in acquiring the materials necessary to undertake an attack with their desired outcomes.

Remember, not all of the components may be visible (they may be hidden inside the packaging) or may not be present. Context is key. Consider what is normal for the location/situation.

?

Do you actively look for suspicious devices?

Is the presence of the device suspicious/ unexpected?

Does the device contain other indicators such as unusual packaging, wiring or dissemination methods?

PACKAGING

When constructing a device the terrorist will use the packaging to hold everything together allowing the components to be easily and safely transported. There may also be an element of concealment or camouflage in the packaging selected.

The packaging is usually the first thing that you see and could be an everyday item. In these cases, whilst there may be some clues that a device is a threat it may not be immediately obvious. Remember to apply the H-O-T Protocol, Hidden, Obvious, Typical.

There are few limits on the different packages available to be used. Some generic examples include large letters and parcels, metal pipes, rucksacks, cars or trucks. If an item can be modified to include an internal compartment there is a possibility it can be used as packaging.








SWITCHES, TIMERS AND POWER SOURCES

Terrorists may want to have control over when a device functions to cause maximum damage or to provide time to escape.

To do this a terrorist could include a trigger system comprised of electronic, mechanical or chemical components. The switch or timer could be as simple as joining two wires together.

The power for the trigger signal will typically come from a battery. This can vary in size and may either be stand-alone or incorporated with other electrical components. Although the most common, the signal does not have to be electrical and both mechanical or chemical systems can be used as improvised power sources.

More complicated devices may include multiple timers and power sources. The inclusion of additional components should not affect the functioning of the device.

INITIATOR

An initiator, which takes the trigger signal from a switch or timer, provides the output needed for an explosive to explode and is an essential component. The output can either be heat (from an ignitor) or explosive shock (from a detonator).

Initiators are essential in the safe, legitimate use of explosives and therefore many different types are available. However, due to their nature, they are prohibited from being sold to the general public.

Initiators are typically small and may incorporate a small quantity (around a gram) of sensitive explosives. They are used by the military and in commercial applications such as demolition, quarrying and fireworks. They can be improvised using sensitive explosives and may include items that get hot, such as light bulbs.

Due to the hazardous nature of initiators they should not be handled. If you suspect you have identified an initiator you should follow your local procedures and call the police for assistance.




CBR EXPOSURE METHODS

CBR materials need to be introduced into the environment in order to have an effect.

Potential dispersion and exposure methods include:

Spraying (liquids or powders)

- May feature components such as nozzles, hoppers, reservoirs or more simple victim-operated ‘spring-loaded’ devices

Gas release (this may be highly energetic)

- May feature compressed gas cylinders or perforated containers

Contamination (e.g. food/drink/surfaces)

- May not be obvious other than possible discoloration

Material left in-situ

- Pooled liquids or radiological sources.

Other exposure routes include via an explosion and will include the key components of an explosive device.

If you suspect someone has been exposed to a hazardous material the instructions in Remove, Remove, Remove may be followed.

RESPONSE

All security personnel need to have a clear understanding of the procedures to be followed in the event that any of these threats or indicators are encountered.

Nationally, “Run, Hide, Tell” and “Remove, Remove, Remove” provide guidance to the public and emergency services on how to respond to terrorist events.

It is important to link any response plans with local stakeholders, including, Police, Fire and Rescue Service, Ambulance and the Local Authority as their assistance will be integral to managing the consequences of an attack.

These should include confirming the presence of a threat, clearing the location, cordoning and controlling the area and checking the surroundings for additional threats. Ensure you are familiar with your site response and business continuity plans.

Depending on the incident, when the police arrive the police responders’ first job will be to deal with the threat and prevent further casualties:

- they may be armed and may not be in police uniform
- they may not be able to distinguish who is a threat
- they may treat everyone present firmly.

It may take a long time for the site to return to normal, during this time it is important that you:

- obey all instructions
- do not make sudden movements or gestures that can be perceived as a threat
- stay calm, don’t shout or wave
- keep hands visible at all times to show you are unarmed.

The police may ask for details about the building, locations of suspect items, the attackers, hostages, and casualties. Provide as much detail as you are able, but do not be afraid to say if you do not know.

?

When was the last time you exercised your response plans?

YOUR LOCAL RESPONSE PLAN IS...

IN THE RARE EVENT OF
a firearms or weapons attack

RUN
HIDE
TELL

RUN - to a place of safety. This is a far better option than to surrender or negotiate. If there's nowhere to go, then...

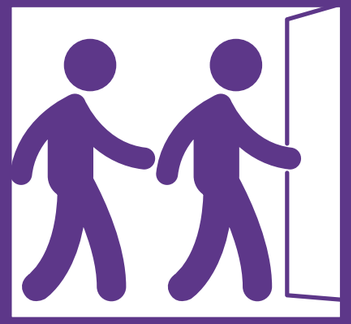
HIDE - Remember to turn your phone to silent and turn off vibrate. Barricade yourself in if you can.

TELL - the police by calling 999 when it is safe to do so.

If you think someone has been exposed to a **HAZARDOUS SUBSTANCE**

Use caution and keep a safe distance to avoid exposure to yourself.

TELL THOSE AFFECTED TO:



REMOVE THEMSELVES...

...from the immediate area to avoid further exposure to the substance. Fresh air is important.

If the skin is itchy or painful, find a water source.

REMOVE OUTER CLOTHING...

...if affected by the substance.

Try to avoid pulling clothing over the head if possible.

Do not smoke, eat or drink.

Do not pull off clothing stuck to skin.

REMOVE THE SUBSTANCE...

...from skin using a dry absorbent material to either soak it up or brush it off.

RINSE continually with water if the skin is itchy or painful.

ACT QUICKLY. These actions can **SAVE LIVES.**

CISA
CYBER+INFRASTRUCTURE

Cybersecurity and Infrastructure Security Agency

Security of Soft Targets and Crowded Places–Resource Guide

April 2019

This page intentionally left blank.

Letter from the Assistant Director

The cornerstone of our democracy is a free and open society where citizens can enjoy a wide range of activities without fear of harm. People across the U.S. should expect that they will be safe and secure as they cheer on a favorite team at a sporting event, shop at a mall, attend a house of worship, go to school, dine out with family and friends, or go to a concert.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) works closely with public and private sector stakeholders to mitigate risk to our infrastructure. This mission includes working to secure soft targets and crowded places in partnership with our stakeholders.

Soft targets and crowded places—a term more recently used—are typically defined as locations or environments that are easily accessible, attract large numbers of people on a predictable or semi-predictable basis, and may be vulnerable to attacks using simple tactics and readily available weapons. CISA works with stakeholders to increase security and reduce the risk of a successful attack or, for those that do occur, limit the impacts to life and property.

The "Security of Soft Targets and Crowded Places—Resource Guide" is a key tool in our efforts to raise awareness of the capabilities that are available to support risk mitigation. The Guide provides an easy to use method to quickly find information on a wide range of free capabilities that can be incorporated into the security practices of organizations of all sizes. I strongly encourage you to consider these capabilities as part of your risk mitigation strategy.

As CISA's Assistant Director for Infrastructure Security, I assure you that we continue to work diligently to identify innovative means through which we can collectively mitigate the risks we face as a nation generally, and those posed by terrorists and other violent extremist actors to soft targets and crowded places specifically. Thank you for your partnership and commitment to securing our nation.

Sincerely,

Brian Harrell
Assistant Director for Infrastructure Security

Table of Contents

1 Resource Matrix

Segments of our society are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, parks, restaurants, shopping centers, special event venues, and similar facilities. Securing these locations is essential to preserving our way of life and sustaining the engine of our economy. The Infrastructure Security Division (ISD), part of the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), is committed to improving the security and resilience of soft targets by providing relevant tools, training, and programs to both the public and private sectors, and the general public. This guide is a catalog of ISD soft target resources, many of which were created in collaboration with our partners to ensure they are useful and reflective of the dynamic environment we live in.

Legend: Type of Resource

Fact Sheet | Guide | Informational Materials | In-Person Training | Online Training | Tool | Video | Website

For **Everyone**

CATEGORY	RESOURCE	TYPE
Understand the Basics	Tools and Resources to Help Businesses Plan, Prepare, and Protect from an Attack	
Identify Suspicious Behavior	"If You See Something, Say Something" Campaign® Informational Video and Radio PSA	
	"If You See Something, Say Something" Campaign® Informational Print Materials PSA	
	Insider Threat Video	
	Pathway to Violence Action Guide	
	Pathway to Violence Video	
	What's in Store: Ordinary People, Extraordinary Events Video	
Protect Against Unmanned Aircraft Systems	Unmanned Aircraft Systems (UAS) Critical Infrastructure Drone Pocket Card	
	Indicators of Suspicious Unmanned Aircraft Systems (UASs)	
	UAS Frequently Asked Questions	
Prepare and Respond to Active Assailants	Action Guide – Active Shooter Attacks: Security Awareness for Soft Targets and Crowded Places	
	Action Guide – Chemical Attacks: Security Awareness for Soft Targets and Crowded Places	
	Action Guide – Vehicle Ramming: Security Awareness for Soft Targets and Crowded Places	
	Action Guide – Fire as a Weapon: Security Awareness for Soft Targets and Crowded Places	

Legend: Type of Resource

Fact Sheet | Guide | Informational Materials | In-Person Training | Online Training | Tool | Video | Website

CATEGORY	RESOURCE	TYPE
Prepare and Respond to Active Assailants, continued	Action Guide – Mass Gatherings: Take Charge of Your Personal Safety	
	Active Shooter Booklet	
	Active Shooter Preparedness Program Website	
	Active Shooter Event Quick Reference Guide	
	Active Shooter Poster	
	Active Shooter Pocket Card	
	Options for Consideration Active Shooter Preparedness Video	
	Vehicle Ramming Attack Mitigation Video	
Prevent and Respond to Bombings	Security and Resiliency Guide for Countering-IEDs (SRG C-IED) and Annexes	

For **Businesses**

CATEGORY	RESOURCE	TYPE
Understand the Basics	Business Continuity Planning Suite	
	Independent Study Training Courses	
	Critical Infrastructure Tabletop Exercise Program (CITEP)	
Identify Suspicious Behavior	Bomb-Making Materials Awareness Program (BMAP)	
	Nationwide Suspicious Activity Reporting (SAR) Initiative – Private Sector Security Training	
	No Reservations: Suspicious Behavior in Hotels Video	
	Suspicious Behavior Advisory Posters	
	At-A-Glance Guide for Protecting Faith-Based Venues	
	Check It! – Bag Check Video	
	Evacuation Planning Guide for Stadiums	
	Patron Screening Best Practices Guide	
	Protective Measures Guides	
	Sports Venue Bag Search Procedures Guide	
	Sports Venue Credentialing Guide	

Legend: Type of Resource

Fact Sheet | Guide | Informational Materials | In-Person Training | Online Training | Tool | Video | Website

CATEGORY	RESOURCE	TYPE
Identify Suspicious Behavior, continued	Vehicle-Borne Improvised Explosive Device (VBIED) Identification Guide	
	Vehicle Inspection Guide	
	Vehicle Inspection Video	
Protect Against Unmanned Aircraft Systems	Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges	
	Unmanned Aircraft Systems – Critical Infrastructure Video	
Prepare and Respond to Active Assailants	Active Shooter Preparedness In-Person Workshops	
	Active Shooter Emergency Action Planning Guide	
	Active Shooter Emergency Action Planning Template	
	Active Shooter Emergency Action Planning Video	
	Active Shooter Recovery Guide	
	Action Guide – Mass Gatherings: Security Awareness for Soft Targets and Crowded Places	
	Recovering From An Active Shooter Incident Action Guide	
Prevent and Respond to Bombings	Counter-IED and Risk Mitigation Training	
	Sports and Entertainment Venues Bombing Prevention Solutions Portfolio	
	Technical Resource for Incident Prevention (TRIP*wire*) Website	
	What to Do – Bomb Threat Website	
	Bomb Threat Procedures Checklist	
	Bombing Prevention Lanyard Cards	
	DHS-Department of Justice (DOJ) Bomb Threat Guidance	
	What You Can Do When There is a Bomb Threat Video	
Connect with CISA	Homeland Security Information Network – Critical Infrastructure (HSIN-CI)	
	Regional Offices	
	Assist Visits and the Infrastructure Survey Tool	

For **Government**

CATEGORY	RESOURCE	TYPE
Protect, Screen, and Allow Access to Facilities	Interagency Security Committee Best Practices for Mail Screening and Handling Processes	
	Occupant Emergency Programs: An Interagency Security Committee Guide	
Prepare and Respond to Active Assailants	Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide	
Prevent and Respond to Bombings	Multi-Jurisdictional Improvised Explosive Device (IED) Security Planning	
Connect with CISA	Interagency Security Committee	

For **First Responders**

CATEGORY	RESOURCE	TYPE
Protect, Screen, and Allow Access to Facilities	Crisis Event Response and Recovery Access (CERRA) Framework	
Protect Against Unmanned Aircraft Systems	Unmanned Aircraft Systems: Considerations for Law Enforcement	
Prevent and Respond to Bombings	National Counter- Improvised Explosive Device Capabilities Analysis Database (NCCAD)	

2 Resource Descriptions & Links

This section includes brief descriptions of each of the available resources and includes links to the resources or where you can find more information.

Understand the Basics

The following resources provide an introduction to facility security and can serve as a good first step for businesses. Resources include fact sheets, guidance, and online training and education courses that cover topics such as Implementing Critical Infrastructure Security and Resilience Programs and Workplace Security Awareness.

Tools and Resources to Help Businesses Plan, Prepare, and Protect from an Attack

Provides business owners and their employees with an overview of the Hometown Security Initiative, specifically how to apply the four steps: Connect, Plan, Train, and Report to their workplace and communities. The Hometown Security Report Series (HSRS) provides reports on community infrastructure and institutions, including commercial office buildings, commuter rail systems, hotels, hospitals, and institutes of higher education. The reports are one of the free tools and resources provided under the initiative.

Link: https://www.dhs.gov/sites/default/files/publications/Hometown-Security-Fact-Sheet-04062016-508.pdf

Link: https://www.dhs.gov/hometown-security

Audience  Type 

Business Continuity Planning Suite

Helps businesses create, improve, or update their business continuity plan to reduce the potential impact of a disruption to business. The suite includes business continuity planning training, business continuity and disaster recovery plan generators, and a business continuity plan validation.

Link: https://www.ready.gov/business-continuity-planning-suite

Audience  Type 

Independent Study Training Courses

Provide individuals, businesses, first responders, and law enforcement with the information needed to improve security at their facilities. The self-paced, online courses hosted by the Federal Emergency Management Agency's (FEMA) Emergency Management Institute cover topics such as levels of protection and design-basis threat, active shooter, insider threat, workplace security, hidden hazards in retail spaces, and suspicious activity surveillance. All courses require a FEMA student identification number. For more information on how to register, please visit: https://cdp.dhs.gov/femasid/register.

Link: https://training.fema.gov/is/

Audience  Type 

Critical Infrastructure Tabletop Exercise Program (CITEP)

Assists the critical infrastructure community in conducting their own tabletop exercises by allowing users to leverage pre-built exercise templates and tailor them to their specific needs in order to assess, develop, and update emergency action plans, programs, policies and procedures. These resources provide exercise planners with tools, scenarios, question sets, and guidance to support the development of a discussion-based exercise. There are over 30 CITEP exercise templates, including ones for outdoor events and insider threats.

Link: https://hsin.dhs.gov/ci/sites/exerciseinfo/Pages/CITEP_Learnmore.aspx

Audience  Type 

Identify Suspicious Behavior

These resources help all citizens, business owners and employees, and private sector security personnel understand what suspicious behaviors may pose a threat and what steps to take to report the behavior to authorities.

Nationwide Suspicious Activity Reporting (SAR) Initiative – Private Sector Security Training

Assists private sector security personnel in recognizing what kind of suspicious behaviors are associated with pre-incident terrorism activities, understanding how and where to report suspicious activities, and protecting privacy, civil rights, and civil liberties when documenting information.

Link: https://nsi.ncirc.gov/hsptregistration/private_sector/

Audience  Type 

No Reservations: Suspicious Behavior in Hotels Video

Helps hotel employees identify and report suspicious activities and threats in a timely manner by highlighting the indicators of suspicious activity. The video is also available in Spanish.

Link: https://www.dhs.gov/video/no-reservations-suspicious-behavior-hotels

Audience  Type 

Suspicious Behavior Advisory Posters

Serve as a quick-reference resource to help businesses, first responders, and local governments identify suspicious activities and behaviors and prevent the illicit sale of explosive precursor chemicals and components. The posters are available under the Suspicious Activities and Bomb Threats – What to Do section of the TRIP*wire* Website.

Link: https://tripwire.dhs.gov/IED/resources/jsp/loginPopup2.jsp

Audience  Type 

"If You See Something, Say Something" Campaign®

Provides outreach materials such as posters, brochures, and Web graphics that can be provided to partners at no cost to help raise public awareness of the indicators of terrorism and terrorism-related crime. Also available are video and radio public service announcements to raise public awareness of the indicators of terrorism and terrorism-related crime. The public service announcements are available in English and Spanish, but the U.S. Department of Homeland Security (DHS) is able to work with partners to address specific language needs. The topics include *Protect Your Everyday* for all citizens, *Hospitality* for travelers and owners and operators of hotels, and *Officials* focused on the major sport leagues.

Link: https://www.dhs.gov/see-something-say-something/campaign-materials

Audience  Type 

Pathway to Violence Action Guide

Explains warning signs that may lead to violence and what individuals can do to mitigate a potential incident.

Link: https://www.dhs.gov/sites/default/files/publications/dhs-pathway-to-violence-09-15-16-508.pdf

Audience  Type 

Pathway to Violence Video

Identifies behavior indicators that assailants often demonstrate before a violent act based on expert research. The video describes the six progressive steps that may be observable by colleagues, engagement strategies, and recommended responses.

Link: https://www.dhs.gov/pathway-violence-video

Audience  Type 

What's in Store: Ordinary People, Extraordinary Events Video

Helps owners, managers, and staff at shopping centers and retail establishments identify and report suspicious activity and threats by highlighting the indicators of suspicious activity in retail settings.

Link: https://www.dhs.gov/video/whats-store-ordinary-people-extraordinary-events

Audience  Type 

Insider Threat Video

Discusses how insider threats manifest in a variety of ways including terrorism, workplace violence, and breaches of cybersecurity. The video can be found under the Insider Threat tab.

Link: https://www.dhs.gov/insider-threat-mitigation

Audience  Type 

Bomb-Making Materials Awareness Program (BMAP)

Serves as a source of continued information on Improvised Explosive Device (IED) materials, tactics, and Counter-IED Training. A Community Engagement Website serves as the dashboard for BMAP programs across the Nation to track, gather, and disseminate materials, successes, and lessons learned from the BMAP team's instructor-led courses and site visits.

Link: https://www.dhs.gov/bmap

Audience  Type 

Protect, Screen, and Allow Access to Facilities

Many large facilities want to screen patrons before allowing them to enter facilities, others may want employ a credentialing process. Resources in this section provide suggestions and guidance on how to put these programs in place.

At-A-Glance Guide For Protecting Faith-Based Venues

Lists the different resources available for houses of worship including security assessments, tabletop exercises, and other training.

Link: https://www.fema.gov/faith-resources

Audience  Type 

Patron Screening Best Practices Guide

Provides options for businesses to develop and implement patron screening procedures for major sporting events, concerts, horse races, award ceremonies, and similar gatherings.

Link: https://www.dhs.gov/sites/default/files/publications/patron-screening-guide-03-16-508.pdf

Audience  Type 

Check It! – Bag Check Video

Provides information facility employees need to properly search bags to protect venues and patrons.

Link: https://www.dhs.gov/video/check-it-bag-check-video

Audience  Type 

Occupant Emergency Programs: An Interagency Security Committee Guide

Provides important information to assist department and agency security planners as they develop and review Occupant Emergency Programs for the safety and security of employees and visitors.

Link: https://www.dhs.gov/sites/default/files/publications/isc-occupant-emergency-programs-guide-mar-2013-508.pdf

Audience  Type 

Evacuation Planning Guide for Stadiums

Assists stadium owners and operators with preparing evacuation plans and helping to determine when and how to evacuate, shelter-in-place, or relocate stadium spectators and participants. It also includes a template that can be used to create a plan that will incorporate the unique policies and procedures of state and local governments, surrounding communities, and specific stadium characteristics.

Link: https://www.dhs.gov/sites/default/files/publications/evacuation-planning-guide-stadiums-508.pdf

Audience  Type 

Protective Measures Guides

Provide businesses with an overview of threats and offer suggestions for planning, coordinating, and training activities that contribute to a safe environment for guests and employees. The guides are For Official Use Only (FOUO), but businesses can request access to them through the Commercial Facilities page of the Homeland Security Information Network – Critical Infrastructure (HSIN-CI), which requires registration to access.

- Protective Measures Guide for U.S. Sports Leagues
- Protective Measures Guide for the U.S. Lodging Industry
- Protective Measures Guide for Mountain Resorts
- Protective Measures Guide for Outdoor Venues
- Protective Measures Guide for Commercial Real Estate

Link: https://www.dhs.gov/commercial-facilities-publications

Audience  Type 

Sports Venue Credentialing Guide

Provides suggestions for developing and implementing credentialing procedures at public assembly venues that host professional sporting events. Venue owners, operators, and event organizers should use additional resources (e.g., law enforcement) when available to implement the procedures outlined in this guide.

Link: https://www.dhs.gov/sites/default/files/publications/sports-venue-credentialing-guide-508.pdf

Audience  Type 

Sports Venue Bag Search Procedures Guide

Provides suggestions for developing and implementing bag search procedures at venues hosting major sporting events. Venue owners, operators, and event organizers should use additional resources (e.g., consult law enforcement) to implement the procedures outlined in this guide.

Link: https://www.dhs.gov/sites/default/files/publications/sports-venue-bag-search-guide-508.pdf

Audience  Type 

Interagency Security Committee (ISC) Best Practices for Mail Screening and Handling Processes

Provides mail center managers, their supervisors, and agency security personnel with a framework for understanding and mitigating risks posed to an organization by the mail and packages it receives and delivers on a daily basis.

Link: https://www.dhs.gov/sites/default/files/publications/isc-mail-handling-screening-nonfouo-sept-2012-508.pdf

Audience  Type 

Crisis Event Response and Recovery Access (CERRA) Framework

Provides voluntary guidance for state, local, tribal, and territorial (SLTT) authorities for planning and developing an access management program. The framework provides mechanisms, tools, processes, and approaches for coordinating, approving, and enabling access during response and recovery operations.

Link: https://www.dhs.gov/sites/default/files/publications/Crisis%20Event%20Response%20and%20Recovery%20Access%20%28CERRA%29%20Framework.pdf

Audience  Type 

Vehicle-Borne Improvised Explosive Device Identification and Vehicle Inspection Guidance

Assist stakeholders in identifying suspected Vehicle-Borne Improvised Explosive Device IEDs (VBIED) and provide instruction for vehicle search techniques for use by law enforcement, bomb squads, HAZMAT teams, and other emergency and professional security personnel involved with inspection of vehicles that may pose a terrorist bomb threat. The Vehicle Inspection Guide, Vehicle Inspection Video, and VBIED Identification Guide are all available to registered users on TRIP*wire*.

Link: https://tripwire.dhs.gov/IED/appmanager/IEDPortal/IEDDesktop?_nfpb=true&_pageLabel=LOGIN

Audience  Type 

Protect Against Unmanned Aircraft Systems (UAS)

UAS, also known as drones, can be used to benefit a community by transporting supplies or assisting search and rescue, but they can also be used for malicious purposes. The resources in this section provide an overview of this threat and steps businesses, the public, and first responders can take to protect against the malicious use of drones.

Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges

Provides an overview of the threats posed by UAS and actions that owners and operators can take to protect their facilities.

Link: https://www.dhs.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf

Audience  Type 

Unmanned Aircraft Systems Critical Infrastructure Drone Pocket Card

Provides a quick reference guide for critical infrastructure security and operations officers and the general public on how to identify the different categories of UAS, how to report UAS activity including what information to share, and what actions to take to respond to a threat.

Link: https://www.dhs.gov/sites/default/files/publications/uas-ci-drone-pocket-card-112017-508.pdf

Audience  Type 

Unmanned Aircraft Systems Frequently Asked Questions

Provides answers to common questions about the requirements and operation of UAS.

Link: https://www.dhs.gov/unmanned-aircraft-systems-faq

Audience  Type 

Unmanned Aircraft Systems – Critical Infrastructure Video

Provides information on critical infrastructure challenges associated with the UAS threat, counter-UAS security practices, actions to consider for risk mitigation, and specific preparedness efforts for facilities and organizations. The video can be found under the UAS and Critical Infrastructure – Understanding the Risk tab.

Link: https://www.dhs.gov/uas-ci

Audience  Type 

Unmanned Aircraft Systems: Indicators of Suspicious UAS

Provides a reference aid to increase situational awareness for those who may encounter a suspicious UAS through the Office for Bombing Prevention (OBP) TRIPwire OSINT Team's Emergency Responder Note (ERN). The document can be found under the Emergency Responder Notes (ERN) section.

Link: https://tripwire.dhs.gov

Audience  Type 

Unmanned Aircraft Systems: Considerations for Law Enforcement

Provides an overview of UAS and the legal and operational considerations for law enforcement before taking action, and a list of additional resources.

Link: https://www.dhs.gov/sites/default/files/publications/uas-law-enforcement-considerations-508.pdf

Audience  Type 

Prepare and Respond to Active Assailants

DHS provides a number of resources to help prepare for, and respond to, active assailant incidents, including in-person and online training, tools to prepare emergency action plans, and guidance on the actions to take during an incident.

Action Guide – Active Shooter Attacks: Security Awareness for Soft Targets and Crowded Places

Lists potential active shooter warning signs, along with steps to take if an incident occurs. Helpful tips are included to assist in developing protective measures to mitigate future attacks.

Link: https://www.dhs.gov/sites/default/files/publications/Active%20Shooter%20Attacks%20-%20Security%20Awareness%20for%20ST-CP.PDF

Audience  Type 

Action Guide – Chemical Attacks: Security Awareness for Soft Targets and Crowded Places

Identifies potential scenarios and symptoms of possible chemical exposures. The guide also explains how individuals can respond to and mitigate against future attacks.

Link: https://www.dhs.gov/sites/default/files/publications/Chemical%20Attacks%20-%20Security%20Awareness%20for%20ST-CP.PDF

Audience  Type 

Action Guide – Vehicle Ramming: Security Awareness for Soft Targets and Crowded Places

Identifies warning signs that individuals planning a vehicle ramming attack may exhibit. The guide also includes suggested mitigation strategies and protective measures to consider.

Link: https://www.dhs.gov/sites/default/files/publications/Vehicle%20Ramming%20-%20Security%20Awareness%20for%20ST-CP.PDF

Audience  Type 

Action Guide – Mass Gatherings: Security Awareness for Soft Targets and Crowded Places

Identifies ways that businesses can prepare for and mitigate against future attacks, including protective measures that provide some basic actions for consideration.

Link: https://www.dhs.gov/sites/default/files/publications/Mass%20Gatherings%20-%20Security%20Awareness%20for%20ST-CP.PDF

Audience  Type 

Action Guide – Fire as a Weapon: Security Awareness for Soft Targets and Crowded Places

Serves as an awareness guide to help people identify potential indicators of an attack by use of fire and provides mitigation strategies and proper response procedures.

Link: https://www.dhs.gov/sites/default/files/publications/Action-Guide-Fire-as-a-Weapon-11212018-508.pdf

Audience  Type 

Action Guide – Mass Gatherings: Take Charge of Your Personal Safety

Provides potential indicators of an attack on a mass gathering and identifies steps that individuals can take in response.

Link: https://www.dhs.gov/sites/default/files/publications/Mass%20Gatherings%20-%20Take%20Charge%20of%20Your%20Personal%20Safety.pdf

Audience  Type 

Active Shooter Preparedness In-Person Workshops

Features scenario-based workshops with facilitated discussions to engage private sector professionals and law enforcement representatives from federal, state, and local agencies to learn how to prepare for, and respond to, an active shooter situation. Through the course of the exercises, participants evaluate current response concepts, plans, and capabilities for coordinated responses to active shooter incidents.

Link: https://www.dhs.gov/active-shooter-workshop-participant

Audience  Type 

Active Shooter Emergency Action Planning

Describes the fundamental concepts of developing an Emergency Action Planning (EAP) for an active shooter scenario, including important consideration of EAP development.

- **Video:** guides viewers through important considerations of EAP development through the first-hand perspectives of active shooter survivors, first responder personnel, and other subject matter experts who share their unique insight.
  Link: https://www.dhs.gov/active-shooter-emergency-action-plan-video
- **Guide:** provides the information needed to develop an Emergency Action Plan.
  Link: https://www.dhs.gov/sites/default/files/publications/active-shooter-emergency-action-plan-112017-508v2.pdf
- **Template:** provides the framework for businesses to create their own Emergency Action Plan.
  Link: https://www.dhs.gov/sites/default/files/publications/active-shooter-emergency-action-plan-template-112017-508.pdf

Audience  Type 

Vehicle Ramming Attack Mitigation Video

Provides information to assist in mitigating the threat of vehicle ramming attacks with technical analysis from public and private sector subject matter experts. The video leverages real-world events, and provides recommendations aimed at protecting organizations as well as individuals against a potential vehicle ramming incident.

Link: https://www.dhs.gov/private-citizen

Audience  Type 

Active Shooter Preparedness Resource Materials

Assist businesses, government offices, and schools in preparing for, and responding to, an active shooter. These resources are also available in the following languages: Arabic, Chinese, Korean, Punjabi, Russian, Somali, Spanish, and Urdu.

- **Active Shooter Booklet:** provides information on how to respond to an active shooter in your vicinity, how to react when law enforcement arrives, and how to train staff and prepare for an active shooter situation, including roles and responsibilities.
  Link: https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf
- **Active Shooter Event Quick Reference Guide:** provides key information in a shorter, easy-to-read format.
  Link: https://www.dhs.gov/sites/default/files/publications/active-shooter-pamphlet-2017-508.pdf
- **Active Shooter Poster:** highlights key information for how to respond when an active shooter is in your vicinity.
  Link: https://www.dhs.gov/sites/default/files/publications/active-shooter-poster-2017-508.pdf
- **Active Shooter Pocket Card:** contains all the information needed to respond to an active shooter in an accessible format.
  Link: https://www.dhs.gov/sites/default/files/publications/active-shooter-pocket-card-508.pdf
- **Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide:** includes helpful information and best practices for federal agencies that can be applied more broadly by anyone who may be involved in an active shooter situation.
  Link: https://www.dhs.gov/sites/default/files/publications/isc-planning-response-active-shooter-guide-non-fouo-nov-2015-508.pdf
- **Options for Consideration Active Shooter Preparedness Video**: demonstrates possible actions to take if confronted with an active shooter scenario. The video also shows how to assist authorities once law enforcement enters the scene.
  Link: https://www.dhs.gov/options-consideration-active-shooter-preparedness-video

Audience  Type 

Active Shooter Recovery Materials

Help organizations proactively put in place policies and procedures to help effectively recover from an active shooter incident while providing a support structure for all involved.

- **Active Shooter Recovery Guide:** outlines what to do in the short-term and long-term to aid in recovery.
  Link: https://www.dhs.gov/sites/default/files/publications/active-shooter-recovery-guide-08-08-2017-508.pdf
- **Recovering From An Active Shooter Incident Action Guide:** provides information on how to establish a recovery process and breaks down necessary actions for short-term and long-term recovery following an active shooter incident.
  Link: https://www.dhs.gov/sites/default/files/publications/recovering-from-an-active-shooter-incident-fact-sheet-08-08-2017-508.pdf

Audience  Type 

Active Shooter Preparedness Program Website

Provides access to a number of DHS products, tools, and resources to help everyone prepare for and respond to an active shooter incident.

Link: https://www.dhs.gov/active-shooter-preparedness

Audience  Type 

Prevent and Respond to Bombings

The resources in this section are designed to increase the capabilities of everyone—the public, business owners and staff, government employees, law enforcement, and first responders—to prevent, protect against, and respond to bombing incidents. The resources include an easy-to-use checklist, planning assistance, in-person and online training, materials and videos that provide guidance, and an online network to access additional resources and share information.

Technical Resource for Incident Prevention (TRIP*wire*) Website

Serves as a 24/7 online, collaborative information-sharing network for bomb squads, first responders, military personnel, government officials, intelligence analysts, and security professionals. Developed and maintained by the Office for Bombing Prevention (OBP), TRIP*wire* combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist source materials to help users anticipate, identify, and prevent IED incidents. TRIP*wire* requires registration to access information, or partners can log-in using their HSIN account. To login, please visit: https://tripwire.dhs.gov/IED/appmanager/IEDPortal/IEDDesktop?_nfpb=true&_pageLabel=LOGIN

Link: https://www.dhs.gov/sites/default/files/publications/obp-tripwire-fact-sheet-2016-508.pdf

Overview Video: https://tripwire.dhs.gov/IED/resources/jsp/tripwireVideo.jsp

Audience  Type 

Sports and Entertainment Venues Bombing Prevention Solutions Portfolio

Provides information on and direct access to the trainings, products, and resources that support sports and entertainment organizations and venues with building counter-IED capabilities. The interactive product connects leadership within these organizations to the counter-IED resources that meet their needs, and empowers all venue personnel to play a role in security.

Link: https://tripwire.dhs.gov/IED/resources/docs/Sports%20Entertainment%20Venue%20Bombing%20Prevention%20Solutions%20Portfolio.pdf

Audience  Type 

What to Do – Bomb Threat Website

Provides guidance and resources including in-depth procedures for responding to bomb threats or encounters with suspicious items or behaviors and provides information to help prepare and react appropriately during these events. The Website also provides information regarding other planning and preparedness resources.

Link: https://www.dhs.gov/what-to-do-bomb-threat

- **DHS-DOJ Bomb Threat Guidance:** provides detailed information on how to assess and react to a threat.

  Link: https://tripwire.dhs.gov/IED/resources/docs/OBP_DHS_DOJ_Bomb_Threat_Guidance.pdf
- **Bomb Threat Procedures Checklist:** provides basic procedural guidelines and a checklist to document important information if a bomb threat is received.

  Link: https://tripwire.dhs.gov/IED/resources/docs/DHS%20Bomb%20Threat%20Checklist.pdf
- **What You Can Do When There is a Bomb Threat Video:** demonstrates how to specifically respond to a phoned in bomb threat and was developed in partnership with the University of Central Florida and the International Association of Chiefs of Police (IACP).

  Link: https://www.dhs.gov/what-to-do-bomb-threat
- **Bombing Prevention Lanyard Cards:** provide quick-reference information and key reminders to empower action, both on the job every day and in the event of an incident.

  Link: https://tripwire.dhs.gov/IED/resources/docs/Bombing%20Prevention%20Lanyard%20Cards%20(Lined%20Version).pdf

Audience  Type 

Multi-Jurisdictional Improvised Explosive Device Security Planning (MJIEDSP) Program

Assists communities with collectively identifying roles, responsibilities, and capability gaps; and optimizing limited resources within a multi- jurisdictional planning area. The MJIEDSP process includes coordination with stakeholders in an area to conduct familiarization briefs and training, data collection activities, and facilitated scenario-based workshops.

Link: https://www.dhs.gov/mjiedsp

Audience  Type 

Counter-IED and Risk Mitigation Training

Provides participants—including municipal officials and emergency managers, state and local law enforcement and other emergency services, critical infrastructure owners and operators, and professional security personnel— with general information and strategies to prevent, protect against, respond to, and mitigate bombing incidents.

To request direct delivery trainings, please contact your local Protective Security Advisor (PSA) or email OBP@ hq.dhs.gov for additional information. For more information, or for a full list of Counter-IED and Risk Mitigation trainings, visit the Counter-IED Training Courses Website or the Counter-IED & Risk Mitigation Training Factsheet.

Link: https://www.dhs.gov/bombing-prevention-training-courses
Fact sheet: https://www.dhs.gov/sites/default/files/publications/obp-training-fact-sheet-2017-508.pdf

Audience  Type 

National Counter-Improvised Explosive Device (IED) Capabilities Analysis Database (NCCAD)

Provides an assessment program managed by the Office for Bombing Prevention (OBP) that uses a consistent and repeatable methodology to assess and analyze the capabilities of units with a counter-IED mission throughout the United States. NCCAD assessments measure the capabilities of and identify gaps in Personnel, Organization, Equipment, Training, and Exercises (POETE) required for effective prevention, protection, and response to IED threats.

Link: https://www.dhs.gov/nccad

Audience  Type 

Security and Resiliency Guide for Countering-IEDs (SRG C-IED) and Annexes

Provide individuals, businesses, first responders, and law enforcement with guidance to enhance their preparedness for potential IED incidents in their communities. The guide includes IED risk information, a framework of 10 common C-IED preparedness goals, planning considerations, and available federal resources. The guide is complemented by four annexes with additional information relevant to venues at high risk of IED-related incidents: lodging, outdoor events, public assembly, and sports leagues and venues.

Link: https://www.dhs.gov/publication/security-and-resiliency-guide-and-annexes

Audience  Type 

Connect with CISA

This section lists ways that businesses; first responders; and state, local, tribal, and territorial governments can access not only the resources listed in this guide, but additional resources available through CISA. These resources can help identify the tools, resources, and training that are right for each facility and its risks.

National Infrastructure Coordinating Center (NICC)

Serves as the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the Nation's critical infrastructure. For more information, please email NICC@hq.dhs.gov.

Link: https://www.dhs.gov/cisa/national-infrastructure-coordinating-center

Audience  Type 

Regional Offices

Engage with state, local, tribal, and territorial (SLTT) government partners, businesses, and critical infrastructure owners and operators in their regions to provide access to steady-state DHS risk-mitigation tools, products, and services, such as training and voluntary vulnerability assessment programs.

The 10 Regional Offices also support National Special Security Events (NSSEs) and Special Event Assessment Rating (SEAR) events; support response to all-hazard incidents through field-level coordination and information sharing; and provide expertise on reconstituting affected critical infrastructure.

- Regional Office Fact Sheet: https://www.dhs.gov/sites/default/files/publications/IP-Regional-Enhancement-Fact-Sheet-508-F.pdf
- Regional Office Website: https://www.dhs.gov/node/29611
- Protective Security Advisor (PSA) Program Fact Sheet: https://www.dhs.gov/sites/default/files/publications/PSA-Program-Fact-Sheet-05-15-508.pdf

Audience  Type 

Homeland Security Information Network – Critical Infrastructure (HSIN-CI)

Serves as the primary information-sharing platform between the critical infrastructure sector stakeholders and government. HSIN-CI enables federal, state, local, and private sector critical infrastructure owners and operators to communicate, coordinate, and share sensitive and sector-relevant information to protect their critical assets, systems, functions, and networks at no charge to sector stakeholders. To request access to HSIN-CI, please contact hsinci@hq.dhs.gov.

Link: https://www.dhs.gov/hsin-critical-infrastructure

Audience  Type 

Interagency Security Committee (ISC)

Develops policies, standards, and recommendations related to the security of nonmilitary federal facilities across the Nation. The ISC does this by, with, and through its members.

Link: https://www.dhs.gov/about-interagency-security-committee

Audience  Type 

Assist Visits and the Infrastructure Survey Tool

Informs critical infrastructure owners and operators of the importance of their facilities, how they fit into the broader critical infrastructure sector, and provides an overview of the CISA resources available to help enhance security and resilience. The visits, conducted by PSAs with critical infrastructure facility representatives, help build relationships and increase communications. One of the CISA resources available to facility owners and operators is the Infrastructure Survey Tool (IST).

Assist visits: https://www.dhs.gov/assist-visits
Infrastructure Survey Tool: https://www.dhs.gov/infrastructure-survey-tool

Audience  Type 

3 Contacts

KEY CONTACTS			
AGENCY/DIVISION/PROGRAM	**PHONE/EMAIL**	**WEBSITE**	**INFORMATION PROVIDED**
National Infrastructure Coordinating Center	NICC@hq.dhs.gov	https://dhs.gov/national-infrastructure-coordinating-center	For more information about the NICC
Regional Offices	Please see Website for contact information	https://www.dhs.gov/node/29611	For more information on the Regional Offices, including locations, services, and contact information for each region

ADDITIONAL CONTACTS			
AGENCY/DIVISION/PROGRAM	**PHONE/EMAIL**	**WEBSITE**	**INFORMATION PROVIDED**
Active Shooter Preparedness Program	ASworkshop@hq.dhs.gov	https://www.dhs.gov/active-shooter-preparedness	For information on Active Shooter Preparedness workshops and materials
Commercial Facilities Sector-Specific Agency	CFSteam@hq.dhs.gov	https://www.dhs.gov/commercial-facilities-sector	For more information on available DHS resources
Homeland Security Information Network – Critical Infrastructure	hsinci@hq.dhs.gov	https://www.dhs.gov/hsin-critical-infrastructure	To request access to HSIN-CI include the following information: name, company, official email address, supervisor's name and phone number, and critical infrastructure sector
Insider Threat Mitigation Program	InTMitigation@hq.dhs.gov	https://www.dhs.gov/insider-threat-mitigation/	For information on Insider Threat Mitigation
Interagency Security Committee	isc.dhs.gov@hq.dhs.gov	https://www.dhs.gov/interagency-security-committee	For more information on policies, standards, and best practices that can be applied
National Counter-Improvised Explosive Device Capabilities Analysis Database	nccad@hq.dhs.gov	www.dhs.gov/nccad	For more resources on NCCAD program.
Office for Bombing Prevention	OBP@hq.dhs.gov	https://www.dhs.gov/obp	For more information on resources or to request training
Soft Target Security	Softtargetsecurity@hq.dhs.gov	https://www.dhs.gov/securing-soft-targets-and-crowded-spaces	For more information on soft target security resources
TRIP*wire* Help Desk	1-866-987-9473; TRIPwirehelp@dhs.gov	https://tripwire.dhs.gov	TRIP*wire* is available at no cost to registered subscribers and now also features a public-access homepage with valuable preparedness information for the whole community

CISA
CYBER+INFRASTRUCTURE

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Washington, D.C. 20528