

Chapter 27

Layers of Preventive Measures for Soft Target Protection against Terrorist Attacks

Alex P. Schmid

The chapter opens by listing the most frequently hit soft and hard targets, with a focus on those attacked by jihadi terrorists. This is followed by a conceptual discussion about various types of terrorist targets, both physical and psychological (targets of violence, targets of terror, target of demands and targets of attention) and identifies ten audiences/conflict parties, terrorists aim to influence in one way or another. A survey of a number of empirical studies on terrorist targeting follows, and ten criteria underlying terrorists' physical target selection are identified. A trend towards increased attacks on soft targets, especially by single actors, is noticed. As a consequence, the number of attacks that could not be prevented has increased in recent years. This diagnostic part of the chapter is followed by one that focuses on improving the prevention of attacks against soft targets. A typology of preventive measures is presented, distinguishing between up-, mid- and downstream prevention. Subsequently, the main focus is on mid- and downstream prevention. A layered approach of combining 13 preventive measures (LPM) is suggested and the author's proposals are juxtaposed with the 13 Good Practices (GP) proposed by the Global Forum on Counter-Terrorism (GFCT)'s Soft Target Protection Initiative in 2017. There is also an Appendix with "Twelve Rules for Preventing and Countering Terrorism" developed by the author when he was Officer-in-Charge of the Terrorism Prevention Branch of UNODC. A bibliography of new literature on terrorist targeting concludes the chapter.

Keywords: prevention, soft targets, terrorist targeting, religious terrorism, jihadism

For an act of terrorism to occur, you need a motivated perpetrator, a suitable target, and the absence of capable guardians.¹ Soft targets have, by definition, no or few guardians present, and there are plenty of ill- or un-defended crowded places that highly-motivated terrorists find suitable. What can be done in terms of preventing terrorist attacks on targets that are not hardened?

Prevention presupposes that we can forecast, with a high degree of probability, what is likely to happen in the near future and - if it is something harmful - anticipating it, stopping it proactively in time from happening by intervening into the chain linking causes and effects. Preferably, this is to be done as early, upstream, and close to the source as possible. An important tool for predicting terrorist activity is analysing and learning from past events. In other words, if you want to be a futurologist, it helps if you are a historian as well. However, when it comes to terrorism, there are a few new things under the sun. In the past, the prototypical terrorist was a bomber without an air force; this has changed drastically, the 9/11 terrorists used hijacked passenger planes as guided cruise missiles, and today terrorists are turning commercial and homemade drones into a makeshift miniature air force.²

Terminology

The prevention of terrorism is the pre-attack part of counterterrorism. Some analysts distinguish between anti-terrorism – preventive and defensive measures against terrorism such as target hardening and enhanced patrolling – and the broader concept of counterterrorism that includes also active and offensive (both pre-emptive and retaliatory) efforts to prevent, deter, and combat politically motivated violence directed at civilian and non-combatant targets. In doing so, counterterrorism actors utilize a broad spectrum of responsive measures, such as law enforcement, political, psychological, social, economic and (para-)military measures.³ For the *Handbook of Terrorism Prevention and Preparedness*, the editor developed the following working definitions:

¹ A truism in criminology; cited by Martha Crenshaw and Gary LaFree. *Countering Terrorism*. Washington, DC: The Brookings Institution, 2017, p.218.

² Doffman, Z., ‘Warning over terrorist attacks using drones given by EU security chief’. *Forbes*, August 4, 2019. Available at: <https://www.forbes.com/sites/zakdoffman/2019/08/04/europes-security-chief-issues-dire-warning-on-terrorist-threat-from-drones/> - 272751b67ae4; see also: Ressler, D. (2018), “The Islamic State and drones: Supply, scale and future threats,” *Combating Terrorism Centre*. Available at: <https://ctc.usma.edu/app/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf> and: Haugstvedt, Havard and Jan Otto Jacobsen, ‘Taking Fourth-Generation Warfare to the Skies? An Empirical Exploration of Non-State Actors’ Use of Weaponised Unmanned Aerial Vehicles (UAVs – ‘Drones’)’, *Perspectives on Terrorism*, Vol. XIV, Issue 5 (quoted from MS).

³ Schmid, Alex P. (Ed.). *The Routledge Handbook of Terrorism Research*. New York and London: Routledge, 2011, p. 604 and p. 620. Another author, Olivier Lewis, defines counter-terrorism in these terms: “... the countering (1) of deliberately indiscriminate violence, (2) of threats of indiscriminate violence, and (3) of political demands made via threats of indiscriminate violence. More simply, CT is an act that seeks to provide non-combatants with physical, psychological and political security” (...) “[Counter-terrorism] strategies can be divided in a number of different ways, but they all cover the same three goals: (1) *strengthening* social, psychological, and material resilience; (2) *responding* to attacks by giving medical aid to victims and prosecuting perpetrators; (3) *preventing* attacks (via coercion, persuasion, and cooption) ...”; Lewis, Olivier, ‘Conceptualizing State Counterterrorism’; in: Scott N. Romaniuk et al (Eds.). *The Palgrave Handbook of Global Counterterrorism Policy*. London: Palgrave, 2017, p. 20 & p. 27.

“Prevention of terrorism involves the anticipation of risks factors giving rise to terrorist group formation, terrorist campaign initiation and/or specific attack preparations,

and responding to these by

Preparedness, that is, taking proactive and pre-emptive measures to reduce risks and threats and, if that turns out to be insufficient, reduce the negative impact of terrorist attacks through a set of planned precautionary measures aimed at strengthening governmental readiness and societal resilience.”

This chapter focuses on the prevention of terrorist attacks on soft targets.⁴ Yet, first we have to be clear about terminology. What are “terrorist targets” and, more importantly, are there also other categories besides “soft” and “hard” targets when it comes to terrorism? For one thing, there are many more soft than hard(-ened) targets. Here are some typical hard (-ened) and soft targets recently exposed to terrorist attacks.⁵

Typical Hard Targets

Typical hard targets include but are not limited to: individual top-level politicians, international summit meetings, government ministries, parliament, foreign embassies and diplomatic residences, commercial passenger airplanes, nuclear facilities (power plants), military compounds, and prisons.

Hard targets are typically surrounded by physical deterrents such as barbed wire fences or high walls as well as vision barriers. There are vehicle barriers at the gates and armed guards with bullet proof vests supported by x-ray machines, metal detectors and sniffers to find hidden explosives, with CCTV cameras and infrared movement sensors to monitor the fenced or walled perimeter. Access points are few and checkpoints can be passed only after ID verification against a computer-linked database and following luggage/baggage and body screening.⁶

⁴ Terrorism is understood here as in this author’s revised *Academic Consensus Definition* of 2011: “Terrorism refers, on the one hand, to a doctrine about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence and, on the other hand, to a conspiratorial practice of calculated, demonstrative, direct violent action without legal or moral restraints, targeting mainly civilians and non-combatants, performed for its propagandistic and psychological effects on various audiences and conflict parties. Terrorism as a tactic is employed in three main contexts: (i) illegal state repression, (ii) propagandistic agitation by non-state actors in times of peace or outside zones of conflict and (iii) as an illicit tactic of irregular warfare employed by state- and non-state actors.” - Alex P. Schmid (Ed.). *The Routledge Handbook of Terrorism Research*. London & New York: Routledge, 2011, p. 86. For the full academic consensus definition, see Available at: <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/schmid-terrorism-definition/html> .

⁵ Multiple sources, including: Counter Extremism Project. *Terror Targets in the West: Where and Why*. Available at: https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/CEP_Terror_Targets.pdf ; Andrew Silke, ‘Understanding Terrorist Target Selection’. In: Anthony Richards et al (Eds.). *Terrorism and the Olympics*. London: Routledge, 2011, p. 54. Available at: https://www.academia.edu/6062416/Understanding_terrorist_target_selection .

⁶ Clarke, Ronald D. and Graeme R. Newman. *Outsmarting the Terrorists*. Westport., Conn., Praeger Security International, 2006, pp. 190-193.

Typical Soft Targets

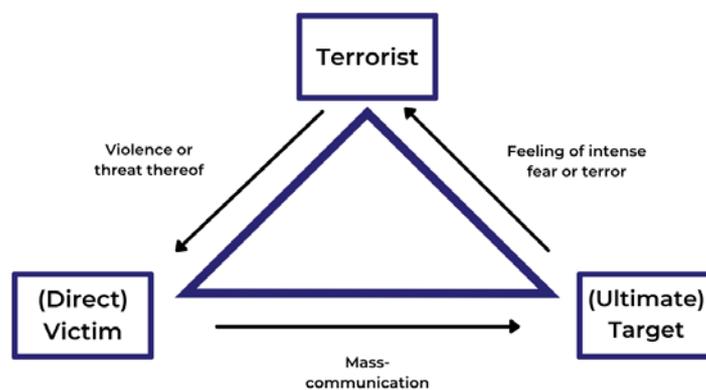
Typical soft targets include, but are not limited to: transportation systems (e.g. airport terminals, railway & bus stations, subway system, ferries) places of religious worship (e.g. churches, mosques, synagogues, temples), weddings, funerals, schools, hospitals, dormitories, market places, indoor shopping malls, museums, tourist destinations, hotels, restaurants, night clubs, theatres, cinemas, landmarks and iconic buildings with symbolic value, venues for special events, (e.g. sport stadiums, cultural arenas, concert halls), long queues of people at entrances gates to event sites, and pedestrian zones in urban areas.

Soft targets are undefended and/or under-protected open access locations with low or no security provided where civilians can be found in significant numbers.⁷ The Dutch intelligence service AIVD describes the distinction in these words: "... targets can be classified as "hard targets," meaning well-protected targets, or as "soft targets," meaning targets with little to no (possibility for) protection."⁸

Types of Terrorist Targets

However, the sole distinction between just soft and hard targets is not all-encompassing, as it fails to recognize an important feature of terrorism. Terrorists are often engaged in a particular kind of psychological warfare, meaning that terrorist attacks are motivated by more than just the aim to cause physical harm. Above all, terrorism is a means to communicate, and the people victimised at soft and hard target sites serve mainly as message generators to reach, via mass- and social media, one or several other "targets" and objectives. Figure 1 visualises this notion of the use of terrorism as a communication tool.⁹

Figure 1. The Triangle of Terrorism



⁷ Based on a great variety of sources, incl., for instance, Miller, Dennis H., Mary E., and Glover, Thomas J. Pocket Partner. Littleton, Colo.: Sequoia Publishing Inc., 2003, p. 240. - A Czech report noted that "There is no official definition for the term 'soft targets'. In ...security circles, however, the term is used to denote places with high concentration of people and low degree of security against assault, which creates an attractive target, especially for terrorists. On the contrary, the so-called 'hard targets' are well secured and guarded premises...." - Kalvach, Zdenek et al., *Basics of soft target protection – guidelines* (2nd version). Prague: Soft Target Protection Institute, June 2016, pp. 6-7.

⁸ Algemene Inlichtingen- en Veiligheidsdienst (AIVD). *Insights into targets. Fifteen years of jihadist attacks in the West*. The Hague: AIVD, 2019, p. 5.

⁹ Schmid, Alex P., *Political Terrorism*. Amsterdam: North-Holland Publications, 1984, p. 91.

In a study published in the mid-1980s, the present author distinguished between four types of targets:¹⁰

1. [Physical] targets of violence;
2. [Psychological] targets of terror;
3. Targets of (coercive) demands; and
4. Targets of attention

However, there are, in fact, more secondary and tertiary target audiences – targets of attention – to terrorist violence. These are ten terrorist audiences and/or conflict parties to be influenced:¹¹

1. adversary (-ies) – usually government(s);
2. society of the adversary (-ies);
3. direct victims and their relatives and friends;
4. others who have reason to fear that they might become next targets;
5. distrusted members and supporters of terrorist organizations (“traitors”);
6. other (rival) terrorist or political party organizations;
7. constituency terrorists claim to represent/act for;
8. potentially sympathetic sectors of domestic and foreign (diaspora) publics;
9. “neutral” distant publics which have not (yet) taken sides;
10. the media themselves, as message transmitters and amplifiers.

Looking only at the direct victims which are mostly found at soft target locations, misses the deeper meaning of terrorist victimisation. Yet, without direct physical victims, the terrorists’ violent message would not get a broad hearing and would therefore miss its main objective. The number of soft targets is almost endless, and if one soft target is hardened, terrorists can pick the next one of a seemingly unlimited choice of soft targets. In other words, displacement can make the hardening of specific targets a futile task as terrorists can move from a highly protected to a low security location. However, for most terrorists, the overarching aim is likely to bring their message across, “on air” and “online.” To put it differently, what really matters is whether their attack ends up being reported and discussed on television and on the internet. In our interconnected world, the physical location where a news-generating violent event takes place, has often become secondary. To illustrate this, the Christchurch shootings on a mosque and an Islamic centre in New Zealand on 15 March 2019 (where one hundred Muslims were injured or killed) was live-streamed on Facebook by the perpetrator Brenton Tarrant. Such events can have immediate reverberations on the other side of the globe, given the fact that social and mass media now serve as the nervous system of much of mankind.

¹⁰ In this study from the mid-1980s, I explained in more detail that “... it is critical to define the ‘targets’ of terrorism. Terrorism involves targets both direct and indirect. Focusing attention on the wrong target, or on only one target, may cloud our understanding of the actual objectives of the terrorist act. First, there are *targets of violence* – random or symbolic victims usually sharing class or group characteristics (e.g. passengers for Israel at an airport) which form the basis for their selection. Through previous use of violence, or the credible threat of violence, other members of that group or class are put in a state of chronic fear. This group becomes the *target of terror*. The overall purpose of terrorism is either to immobilise the *target of terror* (in order to produce disorientation and/or compliance) or to influence the *target of demands* (e.g. governments) or *targets of attention* (e.g. public opinion).” - Alex P. Schmid, ‘Goals and Objectives of International Terrorism’; in: Michael Stohl and Robert Slater (Eds.). *Current Perspectives on Terrorism*. New York: St. Martin’s Press, 1987, p. 48.

¹¹ Adapted from Alex P. Schmid, ‘Magnitudes and Focus of Terrorist Victimization’; in: Uwe Ewald and Ksenija Turkovic (Eds.). *Large-Scale Victimisation as a Potential Source of Terrorist Activities*. Amsterdam: IOS Press, 2006, p.4.

However, newsworthiness also depends on the physical location of the attack, and, to a great extent, on specific types of victims since not all victimisations at soft or hardened target locations convey the same message with the same intensity. If we know what messages a specific group of terrorists wants to convey to its intended audiences, we already would possess an important indication of potential targets. This is to say that context matters very much and so does the type of terrorism we prioritise to respond to.

It is also helpful to be aware of the ten main types of terrorism:¹²

1. single-issue terrorism;
2. lone wolf/actor terrorism;
3. vigilante terrorism;
4. separatist terrorism;
5. left-wing terrorism;
6. right-wing terrorism;
7. religious terrorism;
8. cyber terrorism;
9. CBRN terrorism; and
10. state (or regime) terrorism.

In the following, the focus is predominantly on an Islamist jihadist version of religious terrorism which has become the dominant type of transnational terrorism since 1979.

Protecting soft targets like people congregated in churches, synagogues and mosques or in outdoor spaces like at a Christmas market is a big challenge. There is a trade-off between keeping a society free and open, and keeping its citizens and visitors safe and secure. If the instruments of attack are everyday objects like a stolen truck driven at high speed into a crowd, there is not much that can be done downstream, in the minutes or seconds before it happens. Proactive measures like putting up physical security barriers – raising steel cylinders (bollards) hidden in the pavement in a public space to stop an approaching truck – takes more time than is usually available when such an attack seemingly comes out of the blue.

What then can be done realistically in terms of prevention and preparedness? To answer this question, we first have to look more closely at terrorist target selection.

Factors Determining Terrorist Target Selection

Typical for terrorists is to attack civilian and non-combatant targets; if terrorists would focus on military targets only, they would not be labelled terrorists but insurgents, guerrilla fighters, rebels, partisans, or perhaps resistance fighters. However, some terrorist groups attack, next to un- or ill-protected civilians, also police and military personnel, often when these are not on active duty. Such attacks are often also labelled terrorism, especially if they are conducted outside combat zones and in times of peace. While terrorist attacks are generally indiscriminate, they might be indiscriminate only within certain sub-groups of society.

¹² Derived from: Sarah V. Marsden and Alex P. Schmid, 'Typologies of Terrorism and Political Violence'; in: Alex P. Schmid (Ed.). *The Routledge Handbook of Terrorism Research*. London & New York: Routledge, 2011, pp. 158-200.

Target selection is a function of several factors, including ideology, strategy, capabilities, and opportunities. The strongest of these tends to be ideology.¹³ There are a number of factors that help determine target selection by terrorists:¹⁴

1. ideology;
2. strategy/tactic;
3. terrorist capabilities/resources;
4. opportunity;
5. newsworthiness;
6. expected counterterrorism security measures;
7. expected effects on supporters and sympathisers;
8. expected effects on other audiences and conflict parties (including rival groups);
9. internal decision-making processes within terrorist group preparing attack; and
10. post-incident getaway chances.

Ideology is the main determinant of target selection, even among non-religious terrorist groups. Luis de la Calle and Ignacio Sanchez-Cuenca looked at terrorist targeting in Western Europe over a forty-year period and analysed the distribution of 2,610 fatalities victimised by nationalist, extreme-left, vigilante, extreme-right, and neo-Nazi terrorists (see Table 1).

As can be expected, nationalist and leftist terrorists who claim to fight for the (or their) people prefer targeting representatives of the state, while vigilantes and those on the extreme right and neo-Nazis often tend to be more indiscriminate, target common people.

Turning now to religious terrorism and looking at data spanning the period 1994 to 2015, Petter Nesser found these patterns of Jihadist terrorism for Western Europe:

“It is noteworthy that as much as 70 percent of the plots involving single actors went undetected and reached the execution stage in the period surveyed, while group-based plots were foiled in almost 80 percent of the cases.” (...) Over time, an increasing proportion of jihadi plots in Europe were discriminate and aimed at sub-national entities, communities and individuals rather than the public. (...) In

¹³ In a seminal dissertation on factors which influence the selection of physical targets by terrorist groups, Charles Drake concluded in 1996: “Several factors influence the selection of physical targets by non-state terrorist groups. These include the ideology of the terrorist group concerned, the strategy adopted by the group and its capabilities, its need to take account of external opinion - including that of supporters, the measures adopted to protect likely targets, and the security environment within which the terrorist group operates. (...) However, it can generally be said that ideology sets out the moral framework within which terrorists operate - and which determines whether terrorists judge it to be legitimate to attack a range of targets. After this, the determination of which targets it will actually be beneficial to attack depends upon the strategy which the group has adopted as a means of achieving its political objectives. The determination of their strategic objectives depends upon the effects which the terrorists hope their attacks will achieve. Thus, strategy further refines the range of targets initially delimited by the group's ideology.” – Drake, C.J.M., *The Factors which Influence the Selection of Physical Targets by Terrorist Groups*. St. Andrews: University Ph.D. thesis, 1996. Available at: <https://research-repository.st-andrews.ac.uk/handle/10023/2715> . - The decisive role of ideology also emerges from a statistical analysis done by Austin Wright: “Using novel data on Western European terrorism from 1965 to 2005 and a multinomial logistic extension of statistical backwards induction, I find that ideology is the only consistent predictor of target selection under strategic constraints.” - Austin I. Wright. *Terrorism, Ideology and Target Selection*. Princeton, N.J.: Princeton University, Working Paper, n. d.

¹⁴ Partly based on Silke, Andrew, ‘Understanding Terrorist Target Selection’. In: Richards, Anthony et al (Eds.). *Terrorism and the Olympics*. London: Routledge, 2011, p.53 (Table 4.1. Key factors in terrorist target selection); Available at: https://www.academia.edu/6062416/Understanding_terrorist_target_selection .

Table 1: Target selection by ideology (1965-2005): Domestic terrorism in Western Europe - excluding jihadists¹⁵

	Nationalist	Extreme-Left	Vigilante	Extreme-Right	Neo-Nazi
Military	21.1	5.5	0.4	0.3	1.1
Police	33.2	47.8	1.2	7.8	2.2
Paramilitary	5.1	1.9	11.0	8.6	0.0
Politicians & public officials	3.2	13.3	0.2	0.8	0.4
Entrepreneurs	1.0	8.3	0.5	0.0	0.0
Other civilians	36.5	23.0	86.7	82.5	96.3

the period between 2001 and 2007, around 20 percent of plots were discriminate, whereas Al-Qaeda's mass casualty modus operandi dominated the picture. In the subsequent period between 2008 and 2013, as many as 55 percent of all plots were targeted discriminately and random attacks were decreasing. The majority of discriminate plots were aimed at institutions, artists, and politicians, and perceived as anti-Islam."¹⁶

Indiscriminate attacks are not the same as attacks on soft targets. An attack on a synagogue, church, or mosque for example, is discriminate if we look at society as a whole – believers and non-believers – but also aimed at a soft target. According to a survey of terrorist attacks worldwide over the period 1968-2005, 72 percent (8,111 attacks) were aimed at soft targets, while 27 percent struck hard targets.¹⁷

If we focus on religious terrorism of the Salafi-jihadist type, one study by the Norwegian researcher Cato Hemmingby, surveying 246 registered plots and initiated attacks in Europe between 1994 and the end of 2016, concluded:

“The main findings are that a soft target focus is dominant and increasing, while particularly well-protected targets are almost totally avoided. There is substantial mass casualty focus, but only few attacks lead to such results. Indiscriminate vs. discriminate targeting comes out evenly (...) Both lone actors and groups prefer soft targets ...”¹⁸

A more recent study by the Dutch Intelligence and Security Service (AIVD), surveying more than one hundred attacks in the period 2004-2018, concluded:

¹⁵ de la Calle, Luis and Ignacio Sanchez-Cuenca, “Terrorism as a European Innovation.” In: Chenoweth, Erica, Richard English, Andreas Gofas and Stathis N. Kalyvas (Eds.). *The Oxford Handbook of Terrorism*. Oxford: Oxford University Press, 2019, p. 552. -See also: Austin Wright 2011, p. 5.

¹⁶ Nesser, Petter. *Islamist Terrorism in Europe. A History*. London: Hurst, 2015, pp.59-60 & p.64. Nesser further noted that:” Another category of plots targeted military objects, in particular military personnel in public areas. A third category of plots targeted Jews. (...) A trend towards discriminate terrorism by jihadists in Europe is somewhat counterintuitive. Randomness is a hallmark of terrorism, given its aim of instilling fear in populations. Discriminate attacks are less suitable for frightening an overall population, but easier to justify politically and religiously than random ones.(...)Yet the threat against crowded public areas has largely remained constant (fifteen well-documented incidents before 2008 and nine in 2008-12). (...)The continued threat against public areas can only be interpreted as a sign that random mass casualty terrorism will not be fully abandoned by jihadis in Europe” (Idem, p.62).

¹⁷ Forest, James J.F., *Homeland Security: Protecting America's Targets*. St. Barbara: Greenwood, 2006, p. 70; cit. Wikipedia (English version), lemma “Soft target.”

¹⁸ Hemmingby, Cato, ‘Exploring the Continuum of Lethality: Militant Islamists’ Targeting Preferences in Europe’. *Perspectives on Terrorism*, Vol. 11, No. 5,2017, p. 25.

“Of the 112 attacks in the West in the past fifteen years, 76% can be considered succeeded, meaning that they were actually carried out and resulted in casualties and/or damage. The other 24% can be deemed failed; these attacks did not obtain the intended effect (damage or casualties), for example because explosives failed to detonate. In this regard too there has been a shift in the past fifteen years. During the first ten years of that period, half of all attacks succeeded, and half failed. In the past five years, however, the percentage of success has risen to 84%. So, not only have there been more attacks in the West in the past five years (three-quarters of all attacks of the past fifteen years), but these attacks also succeeded more often.

(...) When considering the whole fifteen-year period, 30% of all attacks in the West occurred in freely accessible public locations where the victims were random passers-by or other people present in the area. In the majority of cases these were exterior locations like streets and squares, and in a small number of cases the location was a freely accessible building like a shopping centre or restaurant. Police officers were the target in 21% of attacks, while 15% of attacks targeted the military.”¹⁹

To summarize, the various surveys and studies referred to in this chapter provide us with two main takeaways. First, that soft targets are the main targets for both single actors and groups of terrorists and attacks on soft targets have been increasing. Second, most single actor plots went undetected while the detection rate for multi-actor attacks was considerably higher - but experts disagree on how many prevention efforts could be considered “successful” as criteria for success vary.

Prevention of Terrorist Attacks against Soft Targets: A Layered Approach

After these more general observations, we can turn to what can be done to reduce harm to potential soft targets of terrorism. What is proposed here is a layered approach to the prevention of terrorist attacks – the idea being that more than a dozen preventive layers (PLM) should be created. While each of these layers might be insufficient to stop a terrorist attack, in combination these layers of defense can become a powerful instrument to prevent many if not most terrorist attacks - even in the case of soft targets.

Let us look at some of the possible prevention strategies and tactics. To begin with, one has to make a distinction between up-, mid-, and down-stream prevention. Terrorism prevention can be broken down into taking pro-active, precautionary measures at three moments in time. These phases of prevention of terrorism include:²⁰

- Upstream, primary (early) prevention: reducing the risk of the formation of a terrorist group or organization.
- Midstream, secondary (timely) prevention: reducing the risk of such a group or organization being able to prepare a terrorist campaign.

¹⁹ AIVD [General Intelligence and Security Service of the Netherlands] *Insight into targets. Fifteen years of jihadist attacks in the West*. The Hague: General Intelligence and Security Service 2019, pp.11 & 14. Available at: <https://english.aivd.nl/publications/publications/2019/07/29/publication-aivd-insight-into-targets---fifteen-years-of-jihadist-attacks-in-the-west>.

²⁰ Schmid, Alex P. ‘Terrorism Prevention: Conceptual Issues (Definitions, Typologies, Theories).’ Chapter 2 of Alex P. Schmid (Ed.) *Handbook of Terrorism Prevention and Preparedness*. The Hague: ICCT, 2021.

- Downstream, tertiary (late) prevention: reducing the risk of execution of individual terrorist operations by foiling and deterring these.

In other words, if terrorist group formation cannot be forestalled in an early phase by taking appropriate measures, the focus should be on preventing the preparation of terrorist campaigns in midstream and, if that also fails, prevention should seek to obstruct the occurrence of individual terrorist incidents.

Upstream prevention refers to structural measures that reduce the risk of terrorist attacks at the source and/or at an early stage, ideally even before terrorist group formation has taken place. Midstream prevention refers to situations halfway between root causes and events where a terrorist group is already formed. The goal here is to prevent a terrorist organisation from preparing a campaign of terrorist attacks. Downstream prevention refers to late prevention of specific and individual terrorist attacks.

In general, when one mentions prevention, one thinks more often of downstream and midstream prevention than of early, upstream prevention. While some of the upstream factors to prevent terrorism are beyond the control of a government (e.g. because the root causes lie abroad) at least one root cause of terrorist attacks is not. Terrorist acts are often revenge acts against foreign armed conflict participation by governments abroad, or reactions to government human rights violations at home. This has been shown by the Institute for Economics and Peace (IEP) which uses empirical data on terrorist incidents from the University of Maryland covering a quarter of a century identified two major upstream root causes of non-governmental terrorism in its Global Terrorism Index report of 2016:

“Statistical analysis has identified two factors which are very closely associated with terrorist activity: political violence committed by the state and the existence of a broader armed conflict. The research finds that 92 per cent of all terrorist attacks over the past 25 years occurred in countries where state sponsored political violence was widespread, while 88 percent of attacks occurred in countries that were involved in violent conflicts. The link between these two factors and terrorism is so strong that less than 0.6 per cent of all terrorist attacks have occurred in countries without any ongoing conflict and any form of political terror [by government].”²¹

In other words, not getting involved in armed conflicts and not violating human rights are two of the most important preventive measures that can be taken upstream.²² While the first measure – not getting involved in armed conflict – is not always a choice governments have since some governments are directly attacked even if they are not involved in foreign interventions, the second measure holding the moral high ground and adhering to human rights standards when fighting terrorism is a matter of choice and has been shown to reduce terrorism.²³ Democratic countries with secure rule of law, good governance, and a high degree of social justice are less prone to terrorist attacks – at least from domestic and home-grown

²¹ Institute for Economics and Peace. Global Terrorism Index 2015. Sidney: IEP, 2016, p.3. For other upstream measures, see Appendix of this chapter.

²² The list of 12 rules for preventing and countering terrorism in the Appendix puts conflict resolution at the top of the list.

²³ Cf. Parker, Tom. *Avoiding the Terrorist Trap. Why Respect for Human Rights is the Key to Defeating Terrorism*. London: World Scientific, 2019. See also Parker’s chapter 34 in this volume.

terrorists.²⁴ Such policies – and the political culture that comes from a healthy relationship between government and civil society and between ethnic and other domestic majorities and minorities – tend to dissuade many activist local groups from escalating their militancy in the direction of terrorist attacks.

Related to such dissuasion is dissuasion's stronger brother – deterrence. While deterrence is part of the instruments of prevention, its use in counter-terrorism is, however, limited. Deterrence depends on the fear of certain and severe punishment and retribution. However, one problem with deterrence of terrorists is that the perpetrators or groups responsible for terrorist attacks are hard to find; few have a known address where the perpetrators or their sponsors can be reached and punished before an attack. In the absence of the possibility of retaliation, deterrence is of limited utility. This is particularly true in the case of suicide bombers: if someone is not only risking his or her life in an attack but actively seeking death as a form of martyrdom in expectation of rewards in an imagined afterlife, the threat of being killed is absent and direct deterrence does not work. Sometimes it is, however, possible to threaten punishment for those who support terrorists.²⁵ There are some indirect ways to deter attacks: if the families of terrorists are living at a known location, their houses can be bulldozed – a tactic familiar to Palestinians around Israel.²⁶ However, that raises some important legal and ethical issues which, however, will not be discussed here.

If we look at the more familiar instruments available for terrorism prevention, most of them refer to downstream prevention. Here, time is short as the window between planning a terrorist attack and its execution is at best a few months and often only weeks or even less. Based on American data, Brent Smith, Kelly Damphousse, and Paxton Roberts noted in 2006 when analysing pre-attack planning and preparation of terrorist acts committed in the US:

“Planning and preparatory activities cannot be temporally separated. Meetings, preparation, training, and procurement of materials for terrorist incidents are not sequenced independent of each other (...). The onset of preparatory behavior typically began about three to four months prior to the planned terrorist incident. Preparatory conduct may include criminal, as well as noncriminal activity. The most common preparatory behaviors included meetings, phone calls, the purchase of supplies and materials, and banking activities ... Terrorist groups engaged in an average of 2.3 known behaviors per incident.”²⁷

A typical terrorist attack then is planned and prepared along the generic lines sketched by Charles Drake and Andrew Silke.²⁸

²⁴ For an explanation why, see: Schmid, Alex P., “Prevention of Terrorism. Towards a multi-pronged approach”; in: Bjørge, Tore (Ed.), *Root Causes of Terrorism. Myths, Reality and Ways Forward*. London: Routledge, 2006, pp. 226-227; see also: Eyerman, Joe, “Terrorism and democratic states: Soft targets or accessible systems.” *International Interactions*, Vol. 24, Issue 2, 1998, pp. 151-170.

²⁵ Cf. Wenger, Andreas and Alex Wilner. *Deterring Terrorism. Theory and Practice*. Stanford: Stanford University Press, 2012.

²⁶ Clarke, Ronald V. and Graeme R. Newman 2006 *Outsmarting the Terrorists*. Westport, Conn., Praeger Security International 2006, p.197.

²⁷ Smith, Brent, Kelly Damphousse, & Paxton Roberts, *Pre-incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct*. Washington, DC: National Institute of Justice, Department of Justice 2006, p.7. Available at: <https://www.ncjrs.gov/pdffiles1/nij/grants/214217.pdf>

²⁸ Silke, Andrew, ‘Understanding Terrorist Target Selection’; in: Anthony Richards et al (Eds.). *Terrorism and the Olympics*. London: Routledge, 2011, p. 60 (adapted in part from Charles Drake, 1998). Available at: https://www.academia.edu/6062416/Understanding_terrorist_target_selection .

1. Setting up a logistical network (safe houses, arms dumps, vehicles, ID, etc.). This is partially dependent upon how overt or covert the terrorists' ordinary lives have to be.
2. Selection of potential targets – generally based on ideological and strategic considerations.
3. Information gathering on potential targets.
4. Reconnaissance of potential targets (find out the likely location and protection of the target at a specific time).
5. Planning of the operation.
6. Insertion of weapons into the area of operation.
7. Insertion of operators into the area of operation.
8. Execution of the operation.
9. Withdrawal of the operational team (not applicable if successful suicide attack).
10. Issue of communiqués if appropriate.

The short window of time when terrorist planning and preparations can be detected points to the importance of looking at, not only downstream signs of preparation, but also mid- and even upstream indicators. However, some methods of detection of upcoming terrorist activity apply to all three phases, the most important of which is intelligence gathering in all its forms, signal and human, self-generated, or received in exchanges with other intelligence - and security agencies. In the case of the 9/11 attacks on New York and Washington almost two dozen opportunities have been identified where US intelligence agencies could have intervened if they had interpreted the early warning signs correctly.

A Layered Approach to the Prevention of Terrorist Attacks, with a Focus on Soft Targets

In the following section, layers of preventive measures (LPM) that apply to mid- and downstream pre-incident detection and intervention tactics and measures in the case of terrorist attack planning and preparation are identified, accompanied by brief comments on each layer. The general assumption here is that we are facing an indiscriminate attack on an unprotected crowded place.²⁹ The challenge is to pick up early warning signals and interpret these correctly. This is more difficult than simply connecting the proverbial dots. It is more in the nature of figuring out a puzzle with many missing pieces and, to make it worse, the pieces in front of the analyst most likely belong to more than one puzzle as several terrorist groups might be planning attacks on various targets. In such situations, linking the pieces to specific preparations becomes exceedingly difficult. The basic idea here is that while the target site is unprotected, there are intervention points at several mid- and downstream stages that can prevent the unprotected target site from being successfully hit. While these preventive measures are listed sequentially here, in reality their order might be different. A further assumption is that we are dealing with homegrown, domestic terrorism, rather than transnational terrorism, where planning and preparation occur largely abroad. In such border-crossing cases, prevention

²⁹ This scenario is based on the observation by the Dutch Intelligence and Security Service (AIVD) which concluded, looking at 112 attacks over the period 2004-2018: "The majority of attacks in the West in the past fifteen years (85%) was directed at easily approachable or accessible targets with little or no surrounding security measures. A relatively small number of attacks (8%) was directed against targets with some form of access control, for example entry tickets and bag checks. Of all attacks, 12% was directed against targets that were under physical protection by police officers or the military. Only 5% of all attacks in the West was directed against (very) well-protected targets, so called *hard targets*." – Algemene Inlichtingen- en Veiligheidsdienst. Insights into targets. Fifteen years of jihadist attacks in the West. The Hague: AIVD/Ministry of the Interior, 2019, p. 20.

becomes more difficult and depends very much on the close and time-sensitive international cooperation of intelligence and security agencies.

The 13 layers of preventive measures (LPMs) for mid- and down-stream soft target protection will be explained below.³⁰

LPM 1: Engage in ongoing collection of traditional open-source information (print media, radio, TV, academic studies and NGO reports) by professional monitoring agencies.

Explanation: Use Open-Source Information (OSI) to the fullest extent. While there is a certain mystique about secret intelligence, fact is that as much as 90 percent of all information intelligence agencies collect tends to come from open sources. Systematic data collection of traditional open-source information by academic institutions and think tanks can go a long way to make basic risk assessments when it comes to terrorism. The full exploitation of open-source information, when done in collaboration with academia, think tanks, and private sector stakeholders allows for basic monitoring of extremist groups and their activities and can help identify trends of targeting to discover patterns. Terrorist violence is often contagious; one new tactic, especially if successful, invites imitations by other groups or copycat crimes by mentally disturbed lone actors. Typical examples are increases in vehicle-based attacks and knife attacks. Sometimes terrorist spokesmen recommend certain easy-to-do attack types in video-messages on the internet and this tends to trigger a particular attack wave by gullible persons who identify with a terrorist cause without necessarily being part of a group. The thing to do, is to monitor terrorist communiques and other messages encouraging certain attack types. This is a form of mid- and downstream precaution which might not prevent a specific attack but it can also warn the public to look out for something that it would otherwise pay no attention to.

LPM 2: Monitoring extremist online activities with potentially violent consequences (e.g., hate speech that can be a predictor of hate crimes, incl. terrorism) in social media and on the dark and deep nest.

Explanation: The internet, to which now more than half of mankind has access, provides an abundance of additional information, and while many extremists try to hide behind encryption and in the deep and dark nets, they also have to reach out to potential recruits and appeal to their envisaged constituencies. Social media content can offer many cues. Monitoring hate speech is one measure that falls somewhere between midstream and downstream prevention. While most of those who engage in hate speech will not commit hate crimes themselves, incitement helps to create a political climate where hate crime, including terrorist crimes, are considered more legitimate among certain sectors of the public. Countering hate crimes is something that members of civil society can do as well, and sometimes better than government agencies. Its preventive effect is hard, if not impossible, to measure, but that should not be a reason for not monitoring and opposing hate speech. Monitoring hate speech is also necessary for late prevention. If, for instance, after a terrorist attack, people on the internet express support for a terrorist attack, they ought to be watched.

LPM 3: Intelligence collection from surveillance and eavesdropping on known and suspected extremist individuals and groups, and their sponsors (e.g. by bugging their phones, computers, cars, and homes).

³⁰ This list is based on multiple sources, including Bjørgero, Tore, *Strategies for Preventing Terrorism*. New York: Palgrave Macmillan, 2013, pp. 55-70.

Explanation: Surveillance and eavesdropping. Multiple methods of eavesdropping on terrorist communications exist and the main problem is not so much picking up such communications as decrypting, translating, and interpreting these in actionable time due to the huge volume of internet traffic. Surveillance takes many forms beyond monitoring someone's presence on the internet. Without technology (e.g. surveillance cameras which allow face recognition, car number registration, airline passenger identification, etc.) this cannot be done, as physical surveillance is personnel-intensive and costly, and beyond the means of all but very few governments. Surveillance can be done in various ways (e.g. bugging the homes, vehicles, phones and computers of suspects) if there are no legal restrictions. The thing to do is to monitor both former terrorists who have not deradicalized (e.g. those released from prison) and sympathisers of terrorist groups. Since this can apply to a large group of people, choices have to be made about the method and intensity of surveillance. This tactic would, however, not be successful against lone actors with homemade bombs.³¹ However, in many cases, such people might already have a criminal or a mental health history for which data exist and which might be worth looking into.

Given the multitude of soft targets, without guidance from collected intelligence, the defense of soft targets would be nearly hopeless. Intelligence, human and signal, open and classified, is the first line of defense. While many think the future is entirely unpredictable, fact is that many (but by no means all) events cast their shadows before them. Prognosis based on known precursor signals is possible to a certain extent. The detection, registration, and observation of more or less weak signals and indicators that point to the possibility and a growing probability of the occurrence of a harmful event requires monitoring in the form of systematic data-gathering. It also involves subsequent timely analysis and interpretation to produce risk assessments solid enough to forecast with a high degree of probability time and form of a terrorist attack. Then an early warning can be issued to those in the need to know and proactive rather than reactive counter-measures can be taken even when the exact location of the attack is not (yet) known.

LPM 4: Use of undercover agents for infiltration into violent groups and /or attracting informers from such groups (e.g. terrorists who are released from prison because they served their term and return to their group); use of sting operations where these are legal.

Explanation: Human intelligence. Due to the limitations of signal intelligence, human intelligence remains crucial. While infiltration of terrorist groups is difficult and dangerous (often a crime has to be committed first as proof of reliability when someone wants to join a group), winning informers from inside terrorist organisations or their support structures is a viable alternative. Unfortunately, the abundance of technical intelligence has in many agencies led to a neglect of cultivating human intelligence. Some intelligence services engage, in jurisdiction which allow to do so, in sting operations (entrapment) to attract militants seeking to obtain arms, ammunition and/or bomb-making equipment.

LPM 5: Exchange of finished (not raw) intelligence (signal and human), within and between government agencies, and with trusted intelligence- and security agencies abroad.

Explanation: Exchange of intelligence. Knowledge is power and information is knowledge. Its exchange between intelligence agencies within a country is often a problem and exchange

³¹ Bomb making at home is relatively easy since there are nearly 4,000 different chemicals which can be used to obtain an explosive reaction. However, the risk of unintended self-harm is high in inexperienced hands. – Kushner, Harvey W., *Encyclopedia of Terrorism*. Thousand Oaks: Sage Publications, 2003, p. 83.

between governments is an even bigger challenge due to, inter alia, source protection concerns. By exchanging only finished (not raw) intelligence, the problem of insufficient trust can be circumvented while it can result in the loss of actionable intelligence. Lack of sufficient reciprocity is often an obstacle to the exchange of sensitive intelligence but when it works between trusted partners it is of utmost relevance for the prevention of terrorist attacks. Time and again post-incident evaluations reveal that crucial information for prevention was “out there” or even “on file” but was not widely shared or not shared in actionable time due to organisational barriers and for other reasons.

LPM 6: Analyse terrorist propaganda and construct counter- and alternative narratives that are backed up by credible actions to prevent & counter (further) radicalisation.

Explanation: Terrorist propaganda often offers cues about the range of targets considered. Sometimes it has taken the form of open instructions in publications like *Inspire* (published by Al-Qaeda), or *Dabiq* and *Rumiyah* (published by ISIS). The study of public statements and captured documents from terrorist organisations offers important cues about likely targets.

LPM 7: Encourage family members and friends of radicalising young men and women to confidentially report their concerns to a trusted organisation (not the police or intelligence services), while assuring them that this does not lead to the arrest of their family member or friend, but will bring them in contact with counsellors in youth mentoring or de-radicalisation programs.

Explanation: The terrorist incidents hardest to prevent are those of single actors or members of a single family (e.g. two brothers). Since few preparations can be carried out undetected by those closest to the perpetrators, reaching out to concerned family members and friends is important. However, these do not want to see their sons or daughters arrested and sent to jail. Therefore, assurances have to be given to them that what they report does not directly go to law enforcement, but will be handled discretely by psychological counsellors or deradicalization units.

LPM 8: Monitor young people with a history of crime and/or mental health issues who appear inclined to join extremist groups and prepare special activity programs (e.g. sport and job training) for such youth at risk.

Explanation: While in the past a sharp distinction has, and could be, made between common criminals and political offenders, that line has become blurred as almost half of all violent extremists tend to have – at least in Europe – a criminal record for violence, theft, robbery, or fraud. A smaller, but still sizable, number of such extremists – perhaps one-third – also have mental health issues. Some have both a criminal background and problems with their mental health. Such people need to be watched for signs of violent radicalisation.³²

LPM 9: Offer incentives to disillusioned members of terrorist organisations to leave their group and subsequently publicise, if they agree, their testimonies and help them start a new career.

³² Cf. Basra, Rajan, Peter R. Neumann and Claudia Brunner, *Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus*. London: ICSR, 2016; Weening, Anton W. ‘Behavioral Problems and Disorders among Radicals in Police Files’ *Perspectives on Terrorism*, Vol. 9, No. 2, pp. 17-33.

Explanation: To leave a terrorist network is difficult as traitors will be punished if not downright killed. This makes leaving hard and should, therefore, be assisted by middlemen. Few counter-narratives are as powerful as the testimonies of former insiders who can point out how big the gap between professed ideology and actual practice in a terrorist organisation really is.

LPM 10: Offer rewards for information tip-offs from the general public that can help to prevent a terrorist attack and/or lead to the arrest of violent extremists and terrorists.

Explanation: Since informing on terrorists (“snitching”) can be costly in terms of revenge acts, substantial sums of money need to be offered to those who cross the line and come forward with information that can help to stop a terrorist plot.

LPM 11: Monitor and follow up specific ordinary crimes (such as theft of explosives) which might be perpetrated in connection with the preparation of a terrorist attack.

Explanation: While some terrorist attack preparations are not unlawful in themselves, others are, and might come to the notice of law enforcement through different channels than those routinely dealing with countering terrorism. Things like theft of police uniforms or explosives, and purchases of ammunition ought, therefore, to be investigated. “Follow the precursor crime” should become as important as “follow the money” when it comes to preventing terrorist acts.

LPM 12: Have rapid reaction protocols ready for dealing with credible attack warnings (e.g., on social media) received from the perpetrator or a spokesperson of the terrorist organisation.

Explanation: Some terrorist groups (e.g., the Provisional IRA) provide[d] warnings of an imminent attack because they do not want mass casualties, or because they want that the public puts the blame on the government when it fails to evacuate an area in time. The time between a warning and an explosion is often very short. It is, therefore, important that protocols are ready to deal with credible attack warnings.

LPM 13: Issue warnings via mass and social media to the general public when receiving credible new information about an impending terrorist attack and advise members of the public to be vigilant and look out for identified suspects and suspicious objects, opening a special phone hotline to report to responders.

Explanation: Sometimes authorities are, without having received a specific warning from the perpetrator group, aware that an attack can happen any moment since they have multiple clues but lack information about where such an attack is about to take place. In such cases, the government can appeal to the public to report about the whereabouts of certain extremists on the loose and warn it about the likely danger. This can, in some cases, help to prevent an attack at the last moment or at least help to reduce the number of possible victims.

Are these 13 suggestions going beyond the state of the art? One way of ascertaining that is to compare these preventive layers with those developed by a working group of the Global Counter Terrorism Forum (GCTF) which includes 29 member states and the European Union. In 2017, the GCTF presented the Antalya Memorandum³³ with 13 Good Practices (GP) on the

³³ The GCTF Soft Target Protection Initiative. Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context (September 2017). Available at: www.thegctf.org

Protection of Soft Targets in a Counterterrorism Context). These GCTF Good Practices for the Protection of Soft Targets³⁴ include:

- GP 1: Be alert to the nature and history of the threat, monitor what terrorists are saying, and closely watch and learn from what they are doing.
- GP 2: Threat analysis should keep pace with the evolving nature of the threat and adversary, including local conditions and emerging technologies.
- GP 3: Conduct risk assessments.
- GP 4: Prioritize targets because not all targets are equal. Therefore, it is essential to identify and prioritize targets according to a risk assessment based on, and relevant to, local factors.
- GP 5: Align soft target and critical infrastructure protection efforts.
- GP 6: Include all stakeholders in establishing an effective national counterterrorism framework that clarify[s] responsibilities for soft target preparedness – prevention, protection, mitigation, response, recovery.
- GP 7: Enhance cooperation between and among all levels of government, between government and the private sector, and enhance the exchange of information and experiences between States.
- GP 8: Establish a trusted relationship between government and private sector security entities and encourage industry to play a proactive role in security efforts.
- GP 9: Citizens and private staff can contribute to security by reporting suspicious activity.
- GP10: Identify the right tool or measure for the right circumstance.
- GP11: Test assumptions and institute a lessons-learned program that incorporates analysis of previous attacks.
- GP 12: Train.
- GP13: Develop a communications plan (before an attack, during an attack after an attack).

While the 13 points of the Antalya Memorandum mainly emphasise organisational aspects of defensive prevention more generally, the 13 points suggested here rather focus on practical proactive prevention. However, while these two sets of recommendations are partly on different levels of abstraction, there are overlaps - Good Practices number 1, 7, 9, and 13 of the Antalya Memorandum largely correspond with Preventive Layer Measures number 6, 5, 9, and 10.

Conclusion

In its 2017 Antalya Memorandum, the working group of the Global Counter-Terrorism Forum concluded that:

“Protecting soft targets is complex. It is a perennial and practical struggle to balance security and access, and the target set is virtually unlimited. If casualties are the paramount terrorist metric for success, then every undefended group of people becomes a lucrative target.”³⁵

³⁴ Ibid.

³⁵ Global Counterterrorism Forum (GCTF), The GCTF Soft Target Protection Initiative, Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context. Available at: www.theGCTF.org .

Given the reality that soft targets and crowded places are by definition unprotected or at least under-protected, preventive measures and interventions need to occur further upstream before a perpetrator can reach what the Antalya memorandum calls a target set that is virtually unlimited.” In other words, prevention needs to occur before potential perpetrators have acquired arms and bombs and preferably also before they have joined an extremist group and before they have come to believe that an unprovoked terrorist attack on a random group of strangers is legitimate. In other words, rather than trying to harden an almost endless number of soft targets, multiple prevention layers that can act like filters should be applied before a terrorist attack is imminent in order to minimise the chances of an attack being planned and prepared at all. The main emphasis when it comes to soft target protection should be in the form of pre-incident plot detection, should be on preventing radicalisation by, and recruitment into, terrorist organisations and, further upstream, on the prevention of terrorist group formation rather than on the costly hardening of multiple possible soft targets. Given the human cost of terrorist attacks and the costs of post-incident consequence management and recovery, such a shift of resources prevention in all its phases makes more sense.

Alex P. Schmid, the Editor of this Handbook on Terrorism Prevention and Preparedness, is a Research Fellow at the International Centre for Counter-Terrorism (ICCT) in The Hague. He is Editor-in-Chief of ‘Perspectives on Terrorism’ and former Co-Editor of ‘Terrorism and Political Violence’ – two of the three leading journals in the field of Terrorism Studies. Until 2009, Prof. Schmid held a chair in International Relations at the University of St. Andrews where he was also Director of the Centre for the Study of Terrorism and Political Violence (CSTPV). Previous positions include Officer-in-Charge of the Terrorism Prevention Branch of the UN Office on Drugs and Crime in Vienna (1999-2005) and a chair in Conflict Resolution at Erasmus University, Rotterdam (1991-1999). Between 1978 and 2018 professor Schmid also held various positions at Leiden University and at its The Hague Campus. He is Director of the Vienna-based Terrorism Research Initiative (TRI), a consortium of institutes and individual scholars seeking to enhance human security through collaborative research. Prof. em. Schmid has more than 200 publications and reports to his name, including the award-winning volume ‘Political Terrorism’ (1984, 1988, and 2006) and the ‘Routledge Handbook of Terrorism Research’ (2011, 2013).

Appendix: Twelve Rules for Preventing and Countering Terrorism³⁶

By Alex P. Schmid

1. Try to address the underlying conflict issues exploited by the terrorists and work towards a peaceful solution while not making substantive concessions to the terrorists themselves.
2. Prevent radical individuals and groups from becoming terrorist extremists by confronting them with a mix of 'carrot and stick' –tactics and search for effective counter-motivation measures.
3. Stimulate and encourage defection and conversion of free and imprisoned terrorists and find ways to reduce the support of aggrieved constituencies for terrorist organizations.
4. Deny terrorists access to arms, explosives, false identification documents, safe communication, safe travel and sanctuaries; disrupt and incapacitate their preparations and operations through infiltration, communication intercept, espionage and by limiting their criminal- and other fund-raising capabilities.
5. Reduce low-risk/high-gain opportunities for terrorists to strike by enhancing communications-, energy- and transportation-security, by hardening critical infrastructures and potential sites where mass casualties could occur and apply principles of situational crime prevention to the prevention of terrorism.
6. Keep in mind that terrorists seek publicity and exploit the media and the Internet to propagate their cause, glorify their attacks, win recruits, solicit donations, gather intelligence, disseminate terrorist know-how and communicate with their target audiences. Try to devise communication strategies to counter them in each of these areas.
7. Prepare for crisis – and consequence-management for both “regular” and “catastrophic” acts of terrorism in coordinated simulation exercises and educate first responders and the public on how to cope with terrorism.
8. Establish an Early Detection and Early Warning intelligence system against terrorism and other violent crimes on the interface between organized crime and political conflict.
9. Strengthen coordination of efforts against terrorism both within and between states; enhance international police and intelligence cooperation, and offer technical assistance to those countries lacking the know-how and means to upgrade their counter-terrorism instruments.
10. Show solidarity with, and offer support to, victims of terrorism at home and abroad.
11. Maintain the moral high-ground in the struggle with terrorists by defending and strengthening the rule of law, good governance, democracy and social justice and by matching your deeds with your words.
12. Last but not least: counter the ideologies, indoctrination and propaganda of secular and non-secular terrorists and try to get the upper hand in the war of ideas – the battle for the hearts and minds of those terrorists claim to speak and fight for.

³⁶ Schmid, Alex P. “12 Rules for Preventing and Countering Terrorism,” *Perspectives on Terrorism*, Vol. VI, Issue 3, 2012; originally formulated at the end of his tenure (2005) as Officer-in-Charge of the Terrorism Prevention Branch of the UN Office on Drugs and Crime (UNODC, Vienna).

Bibliography

- Abrahms, Max, Matthew Ward and Ryan Kennedy. Explaining Civilian Attacks: Terrorist Networks, Principal-Agent Problems and Target Selection, *Perspectives on Terrorism*, Vol. 12, No.1 2018, pp. 23-45.
- Ahmed, Rayna. 'Terrorist Ideologies and Target Selection'. *Journal of Applied Security Research*, Vol. 13, Issue 3, 2018, pp. 376-390.
- AIVD [General Intelligence and Security Service of the Netherlands], *Insight into targets. Fifteen years of jihadist attacks in the West*. The Hague: General Intelligence and Security Service 2019. Available at: <https://english.aivd.nl/publications/publications/2019/07/29/publication-aivd-insight-into-targets---fifteen-years-of-jihadist-attacks-in-the-west>.
- Asal, Victor, et al., 'The Softest of Targets: A Study on Terrorist Target Selection'. *Journal of Applied Security Research*. Vol. 4, Issue 3, 2009, pp. 258-278.
- Bell, J.B. IRA Tactics and Targets. Dublin: Poolbeg Press, 1990.
- Benova, Petra, Sarka Hoskova-Mayerova, and Josef Navratil. 'Terrorist Attacks on Selected Soft Targets'. *Journal of Security and Sustainability Issues*, Vol. 8, No. 3, March 2019, pp.453-471.
- Berman, Eli and David D. Laitin. 2005, 'Hard Targets: Theory and Evidence on Suicide Attacks'. Cambridge, Mass., National Bureau of Economic Research. 2005 (Working Paper 11740).
- Biberman, Y., Zahid, F. 2016. 'Why terrorists target children: Outbidding, desperation, and extremism in the Peshawar and Beslan school massacres.' *Terrorism and Political Violence*, Vol. 28, pp.1-16.
- Bjørgero, Tore. *Strategies for Preventing Terrorism*. New York: Palgrave Macmillan, 2013.
- Brandt, Patrick T., and Todd Sandler. 2010. 'What Do Transnational Terrorists Target? Has It Changed? Are We Safer?' *Journal of Conflict Resolution*, 54 (2): pp. 214-236.
- Calle, Luis de la and Ignacio Sanchez-Cuenca. 'Terrorism as a European Innovation'. In: Erica Chenoweth, Richard English, Andreas Gofas and Stathis N. Kalyvas (Eds.). *The Oxford Handbook of Terrorism*. Oxford: Oxford University Press, 2019, pp. 543-558.
- Coaffee, Jon. 2010. 'Protecting Vulnerable Cities: The UK's Resilience Response to Defending Everyday Urban Infrastructure.' *International Affairs* 86 (4): pp. 939-954.
- Crelinsten, Ronald. Perspectives on Counterterrorism: From Stovepipes to a Comprehensive Approach. *Perspectives on Terrorism*, Vol. 8, Issue 1, 2014, pp. 2-15.
- Dahl, E.J. 'The plots that failed: Intelligence lessons learned from unsuccessful terrorist attacks against the United States. *Stud. Confl. Terror*. 2011, 34, pp. 621-648.
- Department of Homeland Security. *Securing Soft Targets and Crowded Places Resources*. Available at: <https://www.cisa.gov/publication/securing-soft-targets-and-crowded-places-resources>
- Drake, Charles J.M. *The factors which influence the selection of physical targets by terrorist groups*. St. Andrews; University Ph.D. thesis, 1996. Available at: <https://research-repository.st-andrews.ac.uk/handle/10023/2715> .
- Drake, C.J.M. *Terrorist Target Selection*. Basingstoke: Macmillan Press, 1998.
- Drake, C.J.M. 'The Role of Ideology in Terrorists' Target Selection'. *Terrorism and Political Violence*, Vol. 10, Issue 2, 1998, pp. 53-85.
- Gordon, T., Sharan, Y. and Florescu E., 'Potential Measures for the Pre-Detection of Terrorism', *Technological Forecasting and Social Change* -123 (2016).
- Ervin, Clark Kent. *Open Target: Where America is Vulnerable to Attack*. New York: St. Martin's Press, 2006.

- Evers, Dennis H., Miller, Mary E., and Glover, Thomas J. *Pocket Partner*. Littleton. Colo.: Sequoia Publishing Inc., 2003.
- Eyerman, Joe. Terrorism and democratic states: Soft targets or accessible systems. *International Interactions*, Vol. 24, Issue 2, 1998, pp. 151-170.
- Forest, James J.F. *Homeland Security: Protecting America's Targets*. St. Barbara, Cal. Greenwood, 2006.
- Freilich, J. & Newman, G. (2009b). *Crime Prevention Studies; Reducing Terrorism Through Situational Crime Prevention*. (Vol. 25) Boulder: Lynne Rienner.
- Fussey, Peter. 'Deterring terrorism? Target-hardening, surveillance and the prevention of terrorism'; in: Andrew Silke. *The Psychology of Counter-Terrorism*. London: Routledge, 2011, pp. 164-185.
- Global Counterterrorism Forum. *The GCTF Soft Target Protection Initiative. Antalya Memorandum on the Protection of Soft Target in a Counterterrorism Context*. 2017. Available at: <https://www.thegctf.org/About-us/GCTF-framework-documents>
- Gill, Paul et al, 'Terrorist Decision Making in the Context of Risk Attack Planning, and Attack Commission'. *Studies in Conflict and Terrorism*, Published online on 27 March 2018. DOI:10.1080/1057610X.2018.1445501.
- Hemmingby, Cato and Tore Bjørge. *The Dynamics of a Terrorist Targeting Process: Anders Behring Breivik and the 22 July Attacks in Norway*. London: Palgrave Macmillan, 2016. Available at: <http://dx.doi.org/10.1080/17467586.2015.1040426>.
- Hemmingby, Cato. 'Exploring the Continuum of Lethality: Militant Islamists' Targeting Preferences in Europe'. *Perspectives on Terrorism*, Vol. 11, No. 5 (2017), pp.25-41.
- Hesterman, Jennifer. *Soft Target Hardening*. Boca Raton: CRC Press, 2015.
- Heywood, Taylor. *Determinants of Terrorist Target Selection: A Quantitative Analysis*. MA Thesis, University of Central Florida, 2017
- Hoffman, Bruce, 'Terrorist Targeting: Tactics, Trends, and Potentialities'. *Terrorism and Political Violence*, Vol. 5, Issue 2, 1993, pp.12-29.
- Hofreiter, L., V. Berezutskyi, L. Figuli and Z. Zvakova. *Soft Target Protection*. New York: Springer 2019 (published under the NATO Science for Peace and Security series – 2019). Available at: https://www.nato.int/cps/en/natohq/topics_168113.htm?
- Hsu, Henda Y. and David McDowall, 'Does Target-hardening Result in Deadlier Attacks against Protected Targets? An Examination of Unintended Harmful Consequences'. *Journal of Research into Crime Delinquency*, 54 (6) July 2017.
- Institute for Economics and Peace. *Global Terrorism Index 2015*. Sidney: IEP, 2016.
- Johnson, S., Guerette, R. & Bowers, K. (2014). 'Crime Displacement: what we know, what we don't know, and what it means for crime reduction.' *Journal of Experimental Criminology* 10: 549-571.
- Kalvach, Zdenek et al. *Basics of Soft Target Protection – Guidelines (2nd version)*. Prague: Soft Target Protection Institute, June 2016 Available at: <https://www.mvcr.cz/cthh/> .
- Kalyvas, Stathis N. 1999. 'Wanton and Senseless? The Logic of Massacres in Algeria' *Rationality and Society* 11 (3): pp. 243–285.
- Karlos, Vasilis, Martin Larcher and George Solomos. *Review on Soft target/Public space protection guidance*. 2nd edition, Brussels: Joint Research Centre, 2018. Available at: <https://ec.europa.eu/jrc>
- Kidd, Andrew H. and Barbara F. Walter. 'The Strategies of Terrorism', *International Security* 31 (1), 2006, pp. 49-80.
- Lewis, Olivier, 'Conceptualizing State Counterterrorism'; in: Scott N. Romaniuk et al (Eds.). *The Palgrave Handbook of Global Counterterrorism Policy*. London: Palgrave, 2017, pp. 3-38.

- Libicki, Martin C., Peter Chalk and Melanie Sisson, *Exploring Terrorist Targeting Preferences*. St. Monica, RAND, 2007.
- Li Piani, Tiziano, 'Operative Guidelines for Protection of Places of Worship, a new approach toward security design of sensitive buildings', Institute for Advanced Strategic and Political Studies. ISBN: 978889403-2-6.
- Lum, C., Kennedy L.W. and A.J. Sherley. 'The Effectiveness of Counter-Terrorism Strategies'. *Campbell Systematic Reviews*, Vol. 2, 2006, pp. 1-49.
- Marquise, R. *Preventing Soft Target Terrorist Attacks*. Washington, DC: Department of Justice, October, 2015.
- Nemeth, Stephen C. *A Rationalist Explanation of Terrorist Targeting*. Ph.D. Thesis, University of Iowa, 2010
- Nesser, Petter. *Islamist Terrorism in Europe. A History*. London: Hurst, 2015.
- Nilsson, Marco. 'Hard and Soft Target: The Lethality of Suicide Terrorism'. *Journal of International Relations and Development*, 21 (4) DOI: 10.1057/ijrd.2015.25
- Romaniuk, P. and Chowdhury Fink, N.C. *From Input to Impact: Evaluating Terrorist Prevention Programs*. New York: Center on Counterterrorism Cooperation, 2012.
- Schmid, Alex P., 'Goals and Objectives of International Terrorism'; in: Michael Stohl and Robert Slater (Eds.). *Current Perspectives on Terrorism*. New York: St. Martin's Press, 1987, pp. 47-87.
- Schmid, Alex P. *Thesaurus and Glossary of Early Warning and Conflict Prevention Terms*. London: FEWER, 2000.
- Schmid, Alex P., 'Prevention of Terrorism: Towards a Multi-Pronged Approach'; in: Tore Bjørgo (Ed.), *Root Causes of Terrorism: Myths, Reality and Ways Forward*. London: Routledge, 2005, pp.223-240.
- Schmid, Alex P. 'Magnitudes and Focus of Terrorist Victimization'; in: Uwe Ewald and Ksenija Turkovic (eds.). *Large-Scale Victimization as a Potential Source of Terrorist Activities*. Amsterdam: IOS Press, 2006, pp.3-19.
- Silke, Andrew. 'Understanding Terrorist Target Selection'. In: Anthony Richards et al (Eds.). *Terrorism and the Olympics*. London: Routledge, 2011. Available at: https://www.academia.edu/6062416/Understanding_terrorist_target_selection
- Smith, B., Damphousse, K. & Roberts, P. (2006). *Pre-incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct*. Washington, DC: National Institute of Justice, Department of Justice. Available: <https://www.ncjrs.gov/pdffiles1/nij/grants/214217.pdf>
- Taylor, Jeanne Haywood. *Determinants of Terrorist Target Selection: A Quantitative Analysis*. M.A. Thesis University of Central Florida, 2014.
- Torres-Soriano, Manuel Ricardo (2019), 'How Do Terrorists Choose Their Targets for an Attack? The View from inside an Independent Cell', *Terrorism and Political Violence*, Available at: <https://doi.org/10.1080/09546553.2019.1613983>
- United Kingdom, *National Counter-Terrorism Security Office, Crowded Places: The Planning System and Counter-Terrorism*. London: Home Office, 2012.
- Wright, Austin I. *Terrorism, Ideology and Target Selection*. Princeton, N.J.: Princeton University, Working Paper, n.d.

Web-based Resources

- CISA, *Security of Soft Targets and Crowded Places—Resource Guide*. Available at: https://www.cisa.gov/sites/default/files/publications/19_0424_cisa_soft-targets-and-crowded-places-resource-guide.pdf
- Counter-Extremism Project, *Terror Targets*, Available at: <https://www.counterextremism.com/news-free-tags/terror-targets>
- CTED Analytical Brief: Responding to terrorist threats against soft targets. Available at: <https://www.un.org/sc/ctc/wp-content/uploads/2019/09/CTED-Analytical-Brief-Soft-Targets.pdf>
- EU Science Hub, *Review on Soft target/Public space protection guidance*. Available at: <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/review-soft-targetpublic-space-protection-guidance>
- European Organization for Security, *Soft Target and Critical Infrastructures Protection Working Group*. Available at: <http://www.eos-eu.com/soft-target-protection>
- GCTF, Initiative on the Protection of Soft Targets in a Counterterrorism Context. Available at: <https://www.thegctf.org/What-we-do/Coordinating-Committee-Meetings/ArtMID/704/ArticleID/32>
- The Guardian, *From lizarding to lingering: how we really behave in public spaces*. Available at: https://www.theguardian.com/cities/gallery/2019/aug/01/lizarding-and-flex-allure-how-do-you-use-your-city-plaza-in-pictures-field-guide?fbclid=IwAR1ve4qaQ30bc4RLhEmCE8Qkzv8cawBQJyggvPzn9yyF2TXPgFnghZi_dI
- Jashari, Linda, *Soft Target Security: Environmental design and the deterrence of terrorist attacks on soft targets in aviation transportation*. Available at: <https://www.hsaj.org/articles/14522>
- Karlos, Vasilis, Martin Larcher, and George Solomos, *Review on soft target/public space protection guidance*. Available at: https://www.researchgate.net/publication/328419277_Review_on_soft_targetpublic_space_protection_guidance
- Lapkova, Dora, Lukas Kotek and Lukas Kralik, *Soft Targets – Possibilities of their identification*. Available at: https://www.daaam.info/Downloads/Pdfs/proceedings/proceedings_2018/053.pdf
- Lum Cynthia et al., *The effectiveness of Counter-Terrorism Strategies*. Available at: <https://onlinelibrary.wiley.com/doi/10.4073/csr.2006.2>
- Moeler, Hans Mathias, *Why soft target terrorist attacks will remain a threat*. Available at: <https://globalriskinsights.com/2016/07/soft-target-terrorist-attacks/>
- Silber, Mitchell D. *Terrorist Attacks Against Jewish Targets in the West (2012-2019): The Atlantic Divide Between European and American Attackers*. Available at: <https://ctc.usma.edu/terrorist-attacks-jewish-targets-west-2012-2019-atlantic-divide-european-american-attackers/>
- Securing soft targets and crowded places resources. Available at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjKjNT7voLwAhUDuKQKHbfHAasQFjAAegQIAxAD&url=https%3A%2F%2Fwww.cisa.gov%2Fpublication%2Fsecuring-soft-targets-and-crowded-places-resources&usq=AOvVaw0qZogrYH9NKzLCh4gDEU0f>