The GCTF Soft Target Protection Initiative

Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context

Background

Soft targets are places which support community and economic prosperity, where people congregate to study, shop, dine, conduct business, be entertained, worship, or travel. In general, they are open to facilitate access and thus have little or no security in order to be accessible to the public. Typical soft targets may include schools, hospitals, hotels, restaurants, nightclubs, shopping malls, tourist sites, concert halls, museums, religious facilities, sports stadiums, parks and streets, and public areas around transportation systems — anywhere people assemble. They can be publicly or privately owned and are inherently vulnerable to a terrorist attack especially in the face of an increasing number of simple yet ruthless attacks.

Mass-casualty attacks have long been the goal of terrorists. Although attacking soft targets is not a new phenomenon, they have become all too frequent and widespread over the past few decades.[1] The threat is global. Victims vary according to the target selected. Although presenting different narratives and ideological foundations, these organizations are similar in selecting their targets and tactics. In a sense, they are inspired by each other's success. Terrorist groups encourage targeting civilians and soft targets as they have the effect of wreaking havoc and garnering media and government attention. Some groups encourage their followers to use this tactic, as the aggregate effect of small attacks in many places may undermine confidence in government as much as a major attack. Smaller attacks are easier to plan and leave little opportunity for defending governments to detect and disrupt their planning. In the past some terrorists groups were reluctant to attempt mass casualty attacks for fear of losing grassroots support. This is not a concern for an increasing number of terrorist groups and their followers.

The shift to attacking soft targets has included both complex attacks and simple attacks. While complex coordinated attacks against soft targets has had its tactical success in the relatively recent past, with attacks like the November 2015 Paris attack or the one in Brussels in March 2016, it was not without some cost to the terrorist cells responsible for them. Simpler attacks, such as those using vehicles and knives, have the benefits of demanding less planning, little-to-no need for controlled substances or weapons, and ease of execution by an individual with no detectible connection to other terrorists. Therefore, terrorist groups will continue to pose a serious threat by directing, enabling, or inspiring supporters to conduct smaller attacks against soft targets, which remain relatively easy to execute.

[1] During the elaboration of the Antalya Memorandum, participating states mentioned among others, al-Qaida-related attacks in Bamako, Grand Bassam, Madrid, Ouagadougou, and Sharm el-Sheikh; the al-Shabaab attack in Nairobi; the Aum Shinrikyo attack in Tokyo; ISIS-related attacks on Baghdad, Barcelona, Brussels, Istanbul, Manchester, London, Nice, Orlando, Paris, and Tunis; the Lashkar-i-Taiba attack in Mumbai; the Jemaah Islamiyah attack in Bali; PKK-related attacks in Ankara and Istanbul; the Riyad-us Saliheen Brigade of Martyrs attacks on Beslan and Moscow; Tehrik-i-Taliban attack in Peshawar."

Terrorist attacks on these targets have varied. The recent uptick in knife and heavy vehicle attacks, breaking from the use of armed individuals or teams of gunmen, sometimes accompanied by suicide bombers, shows flexibility and willingness to accept smaller casualty counts. Some of the assaults have turned into hostage situations, including the October 2002 terrorist attack on the Dubrovka Threatre in Moscow and killing of Russian Ambassador to Turkey Andrey Karlov (December 2016) in the Center for Contemporary Art in Ankara. Such brutal attacks directly affect the daily lives of citizens, serve the goals of the terrorist groups by increasing the risk of stigmatization of certain groups and the polarization of the society along ethnic or religious lines. They may shake public confidence in the government's ability to provide security for its citizens.

The threat actors are varied, from returning foreign terrorist fighters, to homegrown violent extremists, and certain segments of domestic populations who have been radicalized.[2] The GCTF Lifecycle Toolkit provides recommendations regarding key countering violent extremism (CVE) topics and can be a source for additional information.[3]

Attacks on "soft targets" are often committed by individual terrorists, who become radicalized to commit acts of violence, including through the Internet. Terrorist groups continue to use social media and other technologies to attract new supporters and continue their terrorist activities. In this regard, special attention should be paid to countering the spread of terrorist ideology, wherever it manifests.

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. While inconveniencing the public is certainly a business concern, visibly bolstering security can also be a confidence-building measure and can provide a competitive advantage. The challenge is how to tailor both visible and invisible security measures and apply resources judiciously, thus decreasing the likelihood and consequences of an attack while reinforcing the confidence of the public.

Experience demonstrates the benefits of preparedness. National and local governments, international organizations, and private industry needs to plan and work together to counter the evolving threat to potential soft targets. Governments should develop or expand national plans that address disaster preparedness; emergency response; crisis management; and critical infrastructure protection, security, and resilience. Such plans can be improved by developing and implementing capabilities to create risk-informed priorities among soft targets for government attention, capabilities to protect soft targets from terrorist attacks before they happen, such as training for staff of likely targets to increase their readiness to confidently know when to report suspicious behavior, and other good practices. To address terrorist attacks against soft targets, these plans should go beyond national preparedness for addressing natural disasters, pandemics, and armed attacks, to include a focus on information sharing, risk-based decision making, and public-private partnering.

[2] See GCTF document: The Hague – Marrakech Memorandum on Good Practices for a More Effective Response to the FTF Phenomenon.
[3] https://toolkit.thegctf.org/

Introduction[4]

The non-binding good practices contained in this document are intended to inform and guide governments and private industry as they work together to develop policies, practices, guidelines, programs, and approaches in protecting their citizens from terrorist attacks on soft targets. In recognition of the fact that no plan or strategy can protect all potential targets, this memorandum seeks to synthesize the expertise collected on the topic, beginning with the December 2016 launch meeting in Antalya and continued in 2017 regional workshops in Singapore, Senegal, and at the European Commission in Brussels.

Discussions occurred in the context that it is the primary responsibility of States for ensuring security in their territory and protecting their civilians in accordance with the UN Charter, as well as the relevant role of States outlined in UN Security Council resolution 2341 (2017) on protection of critical infrastructure and particularly vulnerable targets, such as public places, from terrorist attacks. Three issues were common themes in the workshops and are further examined in this document, specifically the importance of:

1. Understanding the threat and then identifying and prioritizing soft targets based on continuous risk assessments and established effective information sharing that promotes practical cooperation and collaboration at all levels of government (international, national, regional, and local);
2. Building public-private sector partnerships to enable and improve security cooperation, and engaging the public and industry through clear and consistent messaging on the nature of the threat and proper preparedness; and
3. Preparing, planning, and protecting by prioritizing resources, engagement, exercises, and training to improve government, industry, and public awareness and preparedness for prevention, response, and recovery.

These workshops also reinforced that discussions and ongoing exchanges among governments and industry can help identify and refine good practices to raise awareness and improve preparedness. These good practices can also be used as the basis for technical or other capacity building assistance.

Good Practices

A. Assessing the Threat, Prioritizing Soft Targets, and Sharing Information

Knowing the enemy is a core principle in protecting soft targets. Today's terrorist organizations seek to inspire their followers domestically and abroad to carry out attacks on their behalf. The rise of ISIS in particular, has increased the trend toward attacking soft targets. Exhortations disseminated through online magazines such as *Dabiq* from ISIS and *Inspire* from Al-Qaida in the Arabian Peninsula and on social media platforms are designed to attract new supporters and also to identify categories of likely targets, suggested tactics, and instructions to readers in the use of weapons and the construction of explosive devices.

[4] The UNSC in resolution 2341 directs the Counter Terrorism Committee (CTC), with the support of the Counter-Terrorism Committee Executive Directorate (CTED), to examine Member States efforts to protect critical infrastructure from terrorist attacks as relevant to the implementation of resolution 1373 (2001) with the aim of identifying good practices, gaps and vulnerabilities in this field. In line with the request, close collaboration between GCTF and CTED can boost efforts of States to protect both ST and CI.

When a tactic works in one venue, both AQ and ISIS tend to recommend it to others. These techniques include using knives, cars, trucks, and making homemade explosives. Terrorist propaganda has often foreshadowed methods of attacks.

Many recent high-profile soft target attacks have been carried out by individuals inspired by ISIS but neither directed by nor otherwise connected to the group's leadership — essentially entrepreneurs. The following Good Practices should be considered in sequential order.

Good Practice 1: Be alert to the nature and history of the threat, monitor what the terrorists are saying, and closely watch and learn from what they are doing. Information need not be sensitive or classified to be valuable. Terrorists often identify targets and offer operational instructions through their online, publicly available publications. Governments and their industry partners can learn a good deal about terrorist tactics by reading terrorists' public material and listening to their broadcasts. This publicly available information can be analyzed to assess enemy capabilities and intentions, particularly when they advertise so openly about techniques and tactics they consider successful (or not) and what they exhort their followers to use.

Every attack is a learning experience and an unfortunate incentive for the international community, the public and private sector, and security services to learn about terrorist capabilities and review current policies. Governments should fuse different sources of information (law enforcement, intelligence, terrorist communication, network analysis — classified and open source) to produce a robust analysis and comprehensive assessment of the threat posed to soft targets. Intelligence should be leveraged for this analysis and made available to the people who need it both inside and outside of government, as appropriate. It is important that public information complement intelligence in producing tailored analysis for engagement with owners and operators of industry.

For example, ISIS has published a guide for would-be attackers, noting that vehicles are "extremely easy to acquire" and unlike conventional weapons, will not arouse the suspicions of citizens or authorities. The ISIS online magazine *Rumiyah* recommended followers in Europe to tap into criminal networks to obtain weapons. ISIS also instructs lone offenders on how to use trucks in an attack, and recommends attacking outdoor markets and rallies, parades, and congested streets. Governments should therefore consolidate this public information, and combine it with official sources, historical data, human intelligence (including employees) and other information to raise public awareness and for discussion with industry which may then use it to support business decisions on security from training to investments in technology.

Good Practice 2: Threat analysis should keep pace with the evolving nature of the threat and adversary, including local conditions and emerging technologies. Understanding the terrorist threat requires balancing an understanding of what terrorists are saying and doing around the world, with a detailed assessment of the threat in a local context. Local factors such as terrorist capabilities and target vulnerabilities are central to accurately assessing and mitigating the local threat. Governments and industry needs to always be most attuned to what is happening in their own countries.

Along with a primary focus on the most likely methods of attack, governments need to also be mindful of new technologies and unexpected tactics to anticipate less obvious, less likely threat developments. As terrorists continue to pursue emerging technologies, like commercial unmanned aerial systems (C-UAS) or drones, and additive manufacturing (3-D printing), governments should devote both attention and effort to assessing these various types of threats. Terrorist use of chemical, biological, radiological or nuclear (CBRN) materials is often cited as the classic high impact, event. CBRN is much less likely than other, simpler attack methods, but proactive risk management

should include consideration of emerging threats, especially those with potential dire consequences. However, preparing for "worst-case" scenarios at the expense of more simplistic and likely attacks is counterproductive. Threat assessments should consider the range of risks posed by adversaries, while also remaining accurate about the nature of this threat.

Good Practice 3: Conduct risk assessments. Risk assessment is a continuous and iterative process that improves preparedness and prioritizes scarce resources. The process of assessing risk begins with a straightforward analysis to identify what could go wrong, how bad it could be if it does go wrong (e.g., economic impact, loss of life), and how likely it is for that to happen. The risk assessment should integrate this information so you can compare the expected harm (e.g., dire consequences) of one type of event with others in order to gain an idea of how you should manage priorities and allocate resources. Terrorism risk assessment helps policymakers, government officials, and business executives implement decisions about providing safety and security to citizens and property in a dynamic threat environment. Governments should consider aligning the threats with a comprehensive list of potential targets based on analysis of terrorist capabilities, intentions, and past attacks, and conduct risk assessments regularly to keep pace with the evolving nature of the threat and adversary. Governments should also update contingency planning, such as guidance, exercises and training for law enforcement and industry to keep pace with actual threats, which will help stakeholders adapt to evolving threats.

Establishment of tactical risk analysis units in major bus and train stations and customs gates could also be considered. One participant used such units for detecting suspicious travelers through face-to-face interviews and checking of belongings. Often these interviews and searches provided important clues regarding a potential foreign terrorist fighter profile, e.g. finding of materials (binoculars or military camouflage, etc.) in the luggage of the traveler that does not fit the stated purpose of visit. Such measures are to be taken in full compliance with obligations under international human rights law and shall respect the rule of law.

Evaluating the strategic risk to soft targets includes assessing whether or not there is a person or group with the capability and intent to attack a vulnerable target. Data to inform risk assessment can come from a variety of sources. National assessments by government security experts will incorporate sensitive and classified information accessible only to official national representatives. They should then be integrated with open source information and information from industry and the private sector in a form accessible to the local security forces which need it. The public and private sectors both use risk analysis to identify and mitigate vulnerabilities in physical infrastructure and in their standard operating procedures and response plans. During several workshops, private sector colleagues discussed their rigorous processes for determining the risk at their facilities, and how they use risk analysis to connect security activities to budget priorities. Governments should encourage the private sector to share their risk analyses with security agency contacts. Government can also support industry assessments with its own expertise and information, which can lead to joint efforts, training, and exercises.

Good Practice 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. Decision makers managing risk should make resource decisions. Identifying and prioritizing potential targets will inform governmental decisions on how much and where and sometimes when to allocate resources. Factors will vary from country to country. Some targets and events offer terrorists opportunities for large-scale massacres of unsuspecting civilians. Successful attacks on certain target categories — schools or certain religious facilities for example — could have profound psychological consequences, adverse political consequences, or both. In other situations, the affiliation or relationship of a certain target with the government might make it a target, such as

hotels used for government conferences, iconic locations with historical significance, and venues frequented by government officials. Governments should both study previous attacks and consider local context to develop plausible and realistic scenarios that allow them to both prepare and allocate finite resources more effectively.

Prioritizing targets might also affect who will assume primary responsibility for security. While soft targets are often privately owned, for some potential soft targets the government will take direct responsibility for their protection or share responsibilities, offer guidance, or mandate minimum levels of security. Another possibility is hiring private security guards or contractors (cost is always a factor especially here, including who bears the burden of paying for heightened security). Many nations have experience protecting critical infrastructure and thus have a base of expertise and experience that can be applied to soft target protection.

Soft targets are not specific and can potentially be any place where large numbers of people congregate or gather. For this reason, the concept of protection should be dynamic, focused, and organized by geographic area instead of a more or less static concept of protection with a focus on a specific object. The dynamic concept of protection should be based on information and risk assessment. In addition, security measures can be visible as well as invisible.

Good Practice 5: Align soft target and critical infrastructure protection efforts. Critical infrastructure, such as power grids, dams, and government facilities, will continue to remain high on the terrorist target list. Soft targets are often part of the critical infrastructure frameworks in many nations. This ensures the infrastructure risk management systems addresses the threat against soft targets. For example: Attacks on people in a train station are part of the suite of potential attack scenarios against transportation systems (air, rail, maritime). Many of the key principles that governments follow when protecting critical infrastructure against terrorist attacks can also be effective for protecting soft targets. These principles are discussed in this document: risk assessment, information sharing, and public-private partnering. Both soft target protection and critical infrastructure security and resilience require the same basic policy and practical framework for preparedness: prevention, protection, mitigation, response and recovery. They should be mutually reinforcing efforts. The UN Security Council passed resolution 2341 (2017) on the protection of critical infrastructure against terrorist attacks in February 2017. While focused primarily on critical infrastructure, it also noted that it will be for States alone to decide what constitutes a soft target and what their critical infrastructure is. Regardless, soft target assessments should be done in conjunction with the assessment of a government's capacity to develop plans and partnerships to protect critical infrastructure. In some cases, soft targets and critical infrastructure may overlap (commercial facilities) and in other cases they may not be the same (energy sector).

As we learned in the regional workshop in Senegal, the term "soft target", or sites that are relatively vulnerable to a terrorist attack due to their open access and limited security, does not translate universally. For example, in some countries, soft targets also may include diplomatic buildings (embassies, consulates, cultural centers), frequented by diplomats and other potentially internationally protected persons. In certain developing countries where resources are limited, it is common that what is typically considered critical infrastructure, such as energy, transportation, water and other essential facilities, is poorly protected.

Governments should therefore coordinate and integrate critical infrastructure and soft target protection efforts to ensure expertise is shared across sectors, and consider how the risk environment within their country would help them prioritize both critical infrastructure and soft target risk management efforts. Where resources are limited, this coordination can serve to extend protective measures beyond the sum of the parts. Critical infrastructure protection efforts have also

long included a focus on resiliency. Continuity of operations plans and quick restoration of normalcy are part of resiliency for critical infrastructure, and when implemented following a soft target attack may go far towards limiting the psychological, economic, and other impacts of the attack.

B. Building Public-Private Partnerships

While some soft targets, such as national museums, some train stations, public squares, or certain sporting venues, may be government-run, soft targets are largely privately owned and operated. Effective security therefore requires a strong and sustained partnership between government and private owners and operators and among businesses themselves.

Since soft target protection is a shared responsibility, national frameworks and mechanisms should support risk-based decision-making, information sharing and public-private partnering for both government and industry. With a shared situational awareness of the threats and vulnerabilities, government can more easily determine how to use its preparedness resources for improving overall security and can encourage the private sector to do the same. Ideally, government and industry can then work together to determine priorities and jointly develop relevant products and tools such as general guidelines on detecting surveillance or specific suggested protective measures for different types of facilities — such as stadiums, hotels, malls, or schools.

Information sharing between government and industry can be a challenge, but workshop participants — government and industry — all acknowledged that it is essential to protecting soft targets. Several participants at the Antalya workshop noted that attacks were disrupted because of timely sharing of information. Governments should therefore encourage routine and urgent information sharing both within the government and with and by the public, including industry. Regular dialogue and activity, especially training among public and private stakeholders, promotes understanding and builds trust among those that may have to respond to and recover from an attack. One partner nation recalled a program designed to bring business leaders closer to government by having chief executive officers or other company leadership chair meetings with local law enforcement on shared security issues. This offers a sense of ownership and can enable more effective engagement and better information flow in both directions.

Along with promoting mutual understanding, public-private partnerships can also lead to joint efforts on terrorist tactics such as use of rental vehicles, falsified documents, stolen uniforms or explosives. For example, while governments may not be familiar with the rental car business, they can explain to industry the threat and assist industry in tailoring training materials to combat the misuse of their vehicles. Moreover, an industry will have its own ideas about how terrorists might misappropriate its products, services, systems, or facilities and can work with governments to reduce this risk.

The public should also be educated in what to look for. The public needs to appreciate the importance of situational awareness and how it contributes to security, even if a terrorist attack on soft targets has not occurred in their country. They need to know how to contact those charged with security and to help reinforce the importance of this, the public should be able to receive some type of acknowledgment or response. Several workshop participants described how one person — a tour guide, a truck driver, a passing citizen — observed and reported something out of the ordinary, and by doing so averted an attack and saved innocent lives. The challenge is developing and shaping a centralized, managed program that articulates key indicators and encourages meaningful reporting.

Good Practice 6: Include all stakeholders in establishing an effective national counterterrorism framework that clarify responsibilities for soft target preparedness—prevention, protection, mitigation, response, recovery. Ensuring that all relevant entities understand the nature of the threat, how it directly impacts their interests, as well as clearly defining their roles and responsibilities, is critical to effective preparedness. National frameworks should identify and organize stakeholders in soft target protection, since organization will vary from country to country and between the various levels of government, as well as across industry sectors, and outline clear roles, responsibilities, and engagement opportunities. Key relationships include those among law enforcement organizations (national, regional, local), between various government agencies and levels, and between the government and the private sector.

Frameworks should outline an inclusive planning process for improving preparedness — prevention, protection, mitigation, response, recovery — for soft target protection. In many cases, the same organizations and people who plan for other circumstances — pandemics, natural disasters, critical infrastructure protection — should be involved in planning for soft target attacks. The planning process should not just include but also integrate the efforts of stakeholders who share responsibility for soft target protection at the national, regional, and local levels within government and private industry, in order to promote a unity of effort. Each of the stakeholders has information, equities and relevant capabilities. Governments should also expose the private sector to information and opportunities, resources, and training, which can be used to enhance a collective situational awareness and ensure preparedness.

Involving stakeholders such as community leaders and entities with local knowledge can have immediate benefit to government efforts to unearth tip-offs and location-specific knowledge for counterterrorism planning and response. Locals are often the first to notice suspicious activities. They are also the first responders and therefore critically important to minimizing the impacts of an attack. Additionally, preparing for soft target attacks can expose gaps in protection and in response duties, such as confusion as to who leads what. If everyone is responsible, nobody is responsible.

Good Practice 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. Information sharing cannot begin during a crisis. Coordination mechanisms and trust should already exist among the various shareholders before organizations come together to deal with a threat or attack to avoid wasting precious time. Developing and sustaining relationships between various levels of government — international, national, regional, and local — and between government and industry, are crucial to passing essential information, such as intelligence, indicators of suspicious activity, and/or attack preparation. Government and industry should routinely discuss the threat environment and industry's specific concerns and needs as well as their ideas and suggestions related to soft target protection. Industry should also be encouraged to share information outside of scheduled exchanges. Even information that may seem meaningless or inconsequential at the time may prove useful — either before an attack or after during forensic analysis. In return, relevant information should be shared by governments with the appropriate stakeholders in a timely manner so that it can be acted upon.

Networks of government, industry and civil society focal points can facilitate prompt information sharing. One country's program brings police and private industry together on a sector-specific basis (e.g., hotels, entertainment, real estate) serving the unique needs of each constituency. Law enforcement should provide training services to assist public and private sector entities in detecting and defending against terrorism, and in return should ask that information flow in both directions to promote ongoing situational awareness and preparedness. Just as the police can assist private sector partners in identifying the threat and preparing for and preventing an attack, those partners in turn

can assist police by sharing their perspective, knowledge, and contingency plans for a possible terrorist attack. This information exchange, through these established relationships, can also assist governments and local responders following an attack.

A private sector security clearance program can also be effective for granting the proper access to those who need to know, including industry representatives who own and operate critical infrastructure or soft targets. This enables sharing classified information across departments and agencies as well as with cleared industry representatives. A process for downgrading information can also help. Protecting sensitive information is critically important, but should not be a barrier to governments providing useful information to the private sector, first responders, and others who can help protect soft targets.

Good Practice 8: Establish a trusted relationship between government and private sector security entities and encourage industry to play a proactive role in security efforts. Outreach, exercises and training should ideally be nationally led, regionally coordinated, and locally delivered. Governments can coordinate and orchestrate specific activities but to be effective, governments should also involve a diverse set of public and private stakeholders. Local officials, including law enforcement, are the most likely to be able to build strong partnerships with the owners and operators of soft targets. These local officials will be first on the scene to either respond to a threat or to make a difference in responding to an attack. Developing partnerships between industry and government is a low or no-cost investment and there can be an immediate pay-off in the form of information sharing and exchanging of best practices, and over the longer-term building a relationship of trust necessary for successful preparedness efforts. An effective government outreach program to private owners and operators should include for example: defined stakeholders (e.g., geographic, industry specific); regular outreach (e.g., phone calls, in-person meetings, webinars), relevant activities (e.g., training on active shooter preparedness), and resources that promote improved awareness and preparedness (e.g., identifying and reporting suspicious activities).

Most countries have adopted a voluntary framework for public-private partnering on preparedness, and are building or expanding those plans to cover soft target protection. A few countries have adopted a regulatory approach to securing certain infrastructure, such as hotels, considered nationally critical. Governments can raise industry awareness through clearly worded websites, guidance, manuals, handouts, and posters that communicate instructions and guidance for specific industry audiences that promote understanding of threats and good practices. They can also develop both general and customized materials, such as training for hospitality staff on how to react to an active shooter, or for hardware stores to identify suspicious purchases of precursors to improvised explosive devices.

The private sector should be a partner in developing plans, drafting written products, and be included in government exercises and training. This is especially true in specialized sectors such as surface transportation — trains, subways, and subway stations — where there may be a mix of both public and private security involved in protection activities. For example, in some countries the private security may be the primary security providers, whereas in others, special divisions of the public police have direct responsibility for transportation security. In other states, security is under direct police supervision, but includes contracted security personnel. Regardless of the mix, these personnel will know the facilities, staff, and passengers, and are better able to identify anomalies as well as plan and practice coordinate among them. A legal or regulatory framework, if employed, should delineate functions, responsibilities, and limitations of private security, and be regularly updated in accordance with evolving security needs.

Good Practice 9: ***Citizens and private sector staff can contribute to security by reporting suspicious activity.*** Governments should develop programs framed by a strict legal framework in order to ensure the respect of human rights and the rule of law, that promote awareness of one's surroundings and encourage reporting of suspicious activities and anomalies. Employees involved in certain industries, regular commuters on transportation systems, and others can often detect suspicious activity more easily than police or security personnel can. Governments should therefore put processes in place to receive, review, and respond to public reports and establish continuous education for the public and industry on what constitutes suspicious activity. This can include making the public an asset in detecting threatening activity (e.g., ask them if they "See Something, Say Something"), making sure the public knows what to look for and who to call when they see it. For example, cautionary signage, billboards, and advertisements on public transportation or in public places can enhance public awareness, and public information campaigns can work if properly focused. Use radio and TV to air public service announcements. For those countries without an existing public communications plan, regular face-to-face meetings with trade organizations or owners and operators of locations of particular concern are a good starting point.

Community outreach is an important part of policing. Several participants mentioned their effective use of police liaison officers who engage with the community, explain laws and help people understand (especially immigrants) what their rights are and what the police expect from them in return. This is essentially a preemptive measure aimed at detecting and resolving issues before they escalate.

One participant noted the implementation of a special program entitled "Inform and Prevent." It comprises tailor-made social activities targeting vulnerable youth groups; outreach to families; and informational meetings at schools and universities. Through this program they have been able to communicate directly with more than 700,000 people in the past year and are considering expanding the practice to include tour operators and guides, as well as small business operators in the tourist regions, informing them about terrorist profiles and terrorist attacks.

C. Preparing, Planning & Protecting

All participants expressed concern that terrorist targets and tactics are constantly evolving. Therefore, government plans for everything from protection to response to command and control and communications must be well-practiced, and regularly exercised — both in table-top and in operational simulations — and updated based on lessons learned. A coherent National framework should set forth roles and responsibilities, which are defined and delineated *before* an incident occurs. This includes determining which entity has jurisdiction, authority, and the capability to respond to either a threat or actual incident. As outlined above, private industry should be involved in this process since planning together in advance promotes preparedness and especially, effective responses.

Our goal is to reduce the risk of attacks against soft targets, even as we accept that eliminating the threat entirely is not possible. One size most certainly does not fit all situations. Protecting a stadium is a far more complex task than protecting a theater. Certain events require massive preparation — inaugurations, large public sporting events, parades and such require complex security arrangements.

We should not, however, underestimate the importance of making the terrorists' task more difficult. Law enforcement and other security preparations, including the use of counter-surveillance, can narrow the terrorists' choice of targets. By exercising standard and specific scenarios, governments and their partners can help determine what tools are most appropriate and consider whether

legislation or regulation could be useful. Exercises involving stakeholders at all levels of government, can be especially helpful in identifying gaps in preparedness, including response capability of local governments and emergency services.

Good Practice 10: Identify the right tool or measure for the right circumstance. Visible security (guards, cameras, barriers) projects strength and are a common, and often most effective, way to deter soft targets attacks. At the same time, visible physical measures need to be strategically integrated along with training, technology, and other measures. There are also opportunities for further collaboration to consider how to incorporate "Security by design" into new construction and renovations of soft target facilities. No security measure is foolproof, so a layered approach that includes comprehensive preparation and response planning should continue since some locations — even if hardened — will always be attractive to terrorists.

Several participants provided examples of methods for making the terrorists' task more difficult, such as placing barriers in high-profile public events or in crowded places, centralizing detailed records (especially photos) of suspicious people and vehicles across locations, in order to determine whether a specific person or vehicle is repeatedly identified on different shifts or at different sites, and "beat cop"-style patrols by local law enforcement. Virtually all member state participants noted the use of closed circuit television (CCTV) cameras to monitor activity in public places to some extent, and many emphasized the importance of using proven mobile technology that is reliable (X-ray machines at airports, sports matches, and festivals). Insider threats, which are especially challenging to detect, should be considered and should be addressed with a variety of physical and non-physical measures. This can include employee-monitoring technology to access controls to training management and staff on how to spot a potential insider threat.

Another useful tool is behavior detection. This approach assumes that the potential attacker is a high-risk individual who does not want to get caught and thus show signs of excessive fear and stress. Several countries have relied on behavior detection as a preventive tool, including questioning and extra screening for people who appear nervous or who act suspicious. Behavior detection can be enhanced by technological innovations, big data solutions, and artificial intelligence. Technology is advancing rapidly and can help with many challenges, including in the field of behavior detection and biometric identification. Crowd behavior analysis technology that uses security camera footage to better understand the behavior of crowd and the early detection of unusual conditions and individuals is one such opportunity.

One participant applies regular and random security checks on inter-city roads, as well as at the main entry points of big cities aimed at deterring and disrupting plans for terrorist attacks. Considering the fact that terrorists often use rental or stolen vehicles, they have also started a new program with rental car companies. These companies are now obliged to record information about people who rent a car and to share immediately this information with the police. Moreover, all major roads and parking areas of shopping malls are screened through vehicle plate recognition systems that are directly connected to the Police in real time.

Good Practice 11: Test assumptions and institute a lessons-learned program that incorporates analysis of previous attacks. Regularly challenging assumptions and revisiting security strategies, including review by experts not directly involved in protecting the facility, is important, and a useful tool for both government authorities and private owners and operators. Frequent testing of the security measures or response to alarms — particularly when un-announced — offer important insight into preparedness and the effectiveness of existing measures. Organize the effort to focus on lessons learned and not merely lessons observed, where mistakes are scrutinized and efforts are directed at identifying and addressing vulnerabilities within one's own organization. Those lessons

should be applied on the ground, and then continuing to regularly identify and share lessons learned should be part of the overall effort.

The utilization of "Red Teams" — thinking like terrorists and planning operations and tactics to expose vulnerabilities in their adversaries — can assist security officials in examining vulnerabilities or improvements in mitigation and response activities. In controlled exercises, red teams could also test security responses.

Good Practice 12: Train. Most military organizations have a common saying: "Train like you fight". The organizations responsible for protecting soft targets should apply the same approach. Several participants noted the value of conducting exercises to improve preparedness among the various stakeholders, such as industry, the public, emergency responders, hospitals, and traffic officials. The exercises were useful on several levels, first, as a reminder that the threat from terrorists is real. Second, training was particularly useful following an attack in a neighboring country for nations that have not yet suffered an attack, or applying the lessons from a recent attack locally.

Participants emphasized that gathering stakeholders together helped designate roles, set expectations, and establish better communications particularly among first responders, both local and national. Table-top exercises are an affordable and useful way to acquire lessons learned for updating procedures. However, simply establishing ground rules and responsibilities for various levels and types of responders is not sufficient — as the threat changes and as personnel cycle through organizations, procedures need to be updated, reinforced, and practiced regularly. Simulations with first responders can help incorporate planning efforts and expertise from other types of incidents (fires, natural disasters) that can be relevant to terrorist attacks. Exercises can also strengthen information exchange with owners and operators of facilities if they are willing to host.

The various entities involved in responding to soft target attacks — fire, police, emergency services, hospitals — should also train together to respond specifically to a soft target attack. Interagency training, exercises and coordination will help identify gaps and needs as well as improve the effectiveness of their collective response, and continue to help build trusting relationships. One participant shared how its joint operations center conducts 'cross-training and integration'. Training should also include how to assist law enforcement, military, first responders, and others from becoming targets in the course of their work.

Good Practice 13: Develop a communications plan. All relevant government agencies should agree on the facts and the approach, as well as the appropriate advice for the public. Terrorism is violence calculated to create fear, overreaction, chaos, and apprehension. Consistent messaging helps bolster public confidence in emergency response and security measures.

- **Before an attack:** Share realistic assessments of risk to manage public expectations. The goal is to maximize the utility of warnings, and avoid allowing terrorists to drive threat perceptions. The challenge is educating the public and offering useful advice without unintentionally echoing the terrorist's message or overwhelming the public with constant information and creating threat fatigue.

- **During an attack:** Establish how best to respond, and what information to release. The public communications portion of a government's response plan is just as important as the operational details. Provide clear instructions to the public about areas to avoid, available shelters, and other practical information. As noted above, balance the information so that it does not unintentionally echo the terrorist's message.

- **After an attack:** Get back to normal life as quickly as possible. Be prepared on social media — craft messages before an attack that you will want to convey in the aftermath. It is also critical to assess communications plans in the immediate aftermath of an attack to capture lessons learned.

The ongoing challenge for all governments is how to provide citizens with information that will enable them to make judgments about their own security, providing them with warnings when intelligence indicates danger, but without contributing further to threat fatigue by de-sensitizing people through constant public alarms. It is critical to be prepared *before* an event occurs, and a major part of this preparation includes having a prepared message ready to transmit to the public.

Governments should provide accurate information to victims and the public while avoiding losses to operational security, fueling further alarm, or losing credibility if original statements turn out to be wrong. In hostage situations, terrorists may access real-time media information so they can avoid police movements. Without distorting events, authorities should work to reduce needless alarm, while also making sure citizens do not ignore the threat and are informed of the appropriate precautions to take. For this to work in real time, the responsibility for managing media matters during crises should be clearly assigned beforehand. The media can also directly or indirectly influence public opinion and actions during and following a soft target attack.

The media can also directly or indirectly influence public opinion during and in relation to attacks on soft targets, which tend to reverberate and cause public outcry.

In preparing after-attack response policies, authorities should aim to minimize the sense of public terror and panic. For example, the full re-operationalization of Istanbul Atatürk Airport just 10 hours following a mass-casualty terrorist attack in 2016 demonstrated trust and confidence in returning business to normal.

Several participants raised useful lessons learned from communication with their publics in response to terrorist attacks. They stressed that public advisories provide critical guidance to the public, but should be calibrated to avoid both over- or under-inflating the threat. One participant suggested using multiple communication methods, including social media and mobile phone apps that allow law enforcement and industry partners to communicate swiftly and facilitate better calibration of the audience — allowing both private communication but also mass distribution where desired. Each country will have different ways — radio, mass text message, television — to convey information based on what is determined to be most effective to reach the broadest target audience. Use training and drills at potential soft targets to provide employees specific instructions on what to do (and not to do) if an attack takes place and/or a hostage situation follows. This should include how to deal with other civilians, such as guests, customers, vendors at the location, as well as how to assist one another.

Conclusion

Organizational dynamics may vary from country to country, between the various levels of government, and across private industry, but soft target protection is a shared responsibility. This initiative has revealed a broad GCTF constituency eager to continue to share threat information, experiences, best practices and lessons learned on the protection of soft targets from terrorist attacks. Governments should seize the opportunity to work with the private sector to improve security and overall preparedness for the benefit of all.

Workshop participants acknowledged both the importance of continual re-assessment of tactics and trends, and of bringing together multiagency and industry experts to deepen understanding of risk assessment, behavior detection and insider risk, and tracking emerging technologies. Several participants also mentioned the need to focus on building a resilient society and a resilient public while raising awareness and improving preparedness for soft target attacks.

As governments assess their efforts against these good practices, particularly as the terrorist threat evolves, the GCTF should look for opportunities for further collaboration on soft target protection.