INSS Insight No. 667, February 24, 2015

Confronting Spontaneous Terrorist Attacks

Gabi Siboni

A prominent feature of many terrorist attacks in recent months in Israel and around the world by Islamic radicals is their independent, spontaneous, unplanned nature – sometimes called the work of lone wolves. Unlike the familiar phenomenon of suicide bombings, spontaneous terrorists operate without logistical, intelligence, or operational support, and without the help of an organizational infrastructure. Therefore the phenomenon presents a serious challenge to the security establishments in the nations where there has been a rise in the scope of spontaneous attacks, the West in general and Israel in particular.

The preventive doctrine developed by the General Security Services in Israel, which focused on suicide attacks, required comprehensive, invasive intelligence capabilities based on the assumption that most attacks are carried out with the help of some guiding hand. In most cases, there existed a supporting operational and logistical chain enhancing the conditions for a successful attack. These include: providing the attacker with intelligence about the target, constructing the explosives or other weapons required for the attack, briefing the attacker, transporting the attacker to the destination, and promising aid to the attacker's family to convince him/her that they will be provided for after the act. This logistical and operational setup provided the security services with the opportunity to gather intelligence in advance, assess the threat, and then foil the attack via a range of operational measures, including the security fence. The measures to foil attacks contributed significantly to the fact that in recent years, suicide attacks became increasingly less frequent.

By contrast, one of the key features of spontaneous attacks, such as the hit-and-run car attacks that occurred in the summer of 2014 in Jerusalem and Gush Etzion, the axe attack on New York City policemen in October, or the attack on the cafe in Sydney, Australia in December, was the lack of external direction and any connection to an organizational infrastructure. The perpetrators of these attacks all operated on the basis of independent motivation, apparently inspired by attacks carried out by organized cells but without their guidance or any direct connection to them. Confronting this type of attack requires adapting the existing preventive doctrine and constructing updated intelligence and

operational tools. A critical review of the spontaneous attacks and some of the perpetrators points to two key characteristics that could help formulate a current doctrine of *preventing* attacks.

The first is the basic profile of the attacker. We see profound identification of the attackers with fundamentalist Islamic ideology, often manifested in the discourse taking place in the new media between the attackers and in their social connections. An investigation of these connections shows that it is possible to identify the attackers' growing extremist jihadist tendencies, which would allow the security establishment to *score* potential attackers as security risks of various degrees and prioritize follow-up intelligence gathering as necessary.

The second characteristic is the behavior of the attackers just before the attack. At times, this window consists of only a few hours, given the spontaneous nature of the attacks. Still, an investigation of such attacks shows that in the span of hours or days leading up the act, the perpetrators engaged in intensive activity in the new media, made last minute arrangements of their affairs, and said goodbye to family and friends. In hindsight, it would have been possible to interpret this activity as preparations for an attack and the likelihood that these individuals would not come back alive. Such behavior by those who also match the basic profile of Islamic radicalization could serve as an indicator of the intention to carry out an attack and therefore serve as a foundation for concrete alerts and the need to foil an attack on short notice.

Based on the combination of both factors, it is possible to construct a profile of the potential attacker and assign him/her a risk threshold that if crossed would indicate the intention to act. This in turn would raise the level of the risk to one that must be foiled. The implementation of such an approach requires the integration of two main capabilities. The first is technological, allowing for the surveillance of a vast amount and scope of data and its rapid analysis. The second is operational, i.e., the ability to carry out a preventive arrest or other foiling activity on a here-and-now timetable.

The emphasis on technological capabilities is hardly new. The need to foil financial fraud on the internet, for example, forced commercial companies to find ways to minimize the phenomenon. Monitoring credit card fraud requires tools for gathering and analyzing big data within fractions of a second using advanced tools calculating the probability of anomalous credit activity requiring intervention or a halt to suspicious transaction. Such technologies are already in operation in intelligence gathering. Edward Snowden's leaks demonstrated the power and extent of the United States intelligence gathering from the internet and other media. The main effort needed to monitor intentions of carrying out spontaneous attacks and foiling them would be pinpointing and analyzing communications activity and the internet in real time.

The major intelligence challenge, then, is creating a methodology that would be suited to identifying spontaneous attackers ahead of time on the basis of existing technology adapted to this end. Such a methodology would have to be based on several components: characterizing the profile of the potential attacker and *scor*ing him/her on a scale of potential threat; rating the threat of at-risk groups based on community and ideological identification; and diagnosing the intensity of suspicious activity in the physical world and in cyberspace. Integration of the values to be measured for each component would help indicate the crossing of the risk threshold by the potential attacker. The intelligence to be gathered would have to entail sufficient geographical coverage and be supported by designated operational capabilities to foil attacks and carry out a preventive arrest within hours from the moment the warning is sounded.

A related issue is the ethical and legal aspects of the approach recommended herein. Without a doubt, intelligence and security establishments in the West are capable of meeting the challenge involved in adapting their technological and operational capabilities to spontaneous terrorism. However, the legal and ethical concerns related to implementation of these capabilities may represent serious hindrances. The construction of a risk profile of potential attackers and execution of preventive arrests on its basis will arouse opposition; surveillance that can be viewed as Big Brother control of civilians representing the violation of privacy on the basis of community and ideological identification will be difficult to institute. On the other hand, the increase in spontaneous attacks requires an unorthodox response, even if it means damage to personal privacy. Moreover, a comprehensive approach to the problem cannot be the effort of a single nation, no matter how advanced it is or what resources are at its disposal. The challenge needs an integrated effort of the security establishments of all the nations facing similar threats. Israel, as a nation possessing highly developed operational, intelligence, and technological capabilities, could be a partner or even a leader in the process of developing an adapted international doctrine of foiling spontaneous attacks.