Terrorisme anno 2035: wat wordt onze aanpak?

Hedendaags terrorisme
Terrorisme is een fenomeen dat op mensen of de gehele maatschappij gericht is, waarbij geweld of het oproepen daartoe gebruikt wordt om politiek of besluiten van overheden of organisaties te beïnvloeden. Als er naar het verleden wordt gekeken, dan leert men dat het probleem terrorisme eigenlijk helemaal niet nieuw is. Zolang er mensen bestaan, zijn er terroristen geweest. De beweegredenen van terroristen zijn in de loop der jaren wel veranderd. Tegenwoordig is terrorisme voornamelijk religieus van aard, zoals de gewelddadige acties van de terreurgroep Islamitische Staat (IS). Als er een woord is dat terrorisme op dit moment het beste omschrijft, dan is dat fragmentatie. Lange tijd is de focus gelegd op terroristische groeperingen als bijvoorbeeld Al Qaida, IRA en de ETA.

Vanaf 2005 is er meer aandacht gekomen voor eenlingen, de zogenaamde 'lone wolfs'. De laatste jaren is het onderscheid tussen terroristische groeperingen en eenlingen steeds meer vervaagd. Een voorbeeld hiervan zijn de aanslagen in Parijs van november 2015. Hierbij waren de broers Abdeslam waarschijnlijk het brein achter deze aanslagen, maar ze zijn hiertoe wel geïnspireerd dan wel geholpen of hebben de opdracht hiertoe gekregen van terroristische groepen of netwerken wereldwijd. Dus met fragmentatie ontstaan er grotere uitdagingen, doordat groeperingen als IS en Al Qaida niet meer één groep zijn, maar er diverse divisies in verschillende landen bestaan die het niet per definitie met elkaar eens zijn over hun handelswijze.

Welk risico loopt het bedrijfsleven?
Hedendaags terrorisme is vooral gericht op zogenaamde 'soft targets', oftewel het zorgen voor zoveel mogelijk burgerslachtoffers tijdens bijvoorbeeld festiviteiten (aanslag op feestgangers Quatorze Juillet, boulevard Nice, 2016) of op het normale dagelijks leven (aanslag winkelcentrum München, 2016). Terroristen kiezen hun locaties en doelwitten heel bewust uit. Ondanks dat terroristische aanslagen op bedrijven niet vaak voorkomen, kunnen deze op individuele organisaties ook verregaande gevolgen hebben: menselijke slachtoffers, imagoschade en bedreiging voor de bedrijfscontinuïteit. Aanslagen op bedrijven uit de vitale sectoren, zoals kerncentrales of (petro)chemische industrie zijn per definitie zorgwekkend.

Het belangrijkste verschil tussen terrorisme en bijvoorbeeld arbeidsveiligheid is dat terrorisme altijd intentioneel van aard is, terwijl in principe niemand met opzet een arbeidsongeval veroorzaakt. Het risico van een terroristische aanslag op het Nederlandse bedrijfsleven is door de jaren heen niet groter of kleiner geworden. Veiligheidsdeskundigen hebben nog weleens de neiging om zich te focussen op de uitzonderingen. Het is belangrijk om hiervoor te waken en te kiezen voor een realistische en proportionele aanpak van terrorisme.

Terrorisme in 2035
In de komende jaren zal terrorisme zich nog meer gaan ontwikkelen op technologisch vlak. Er bestaan eigenlijk allemaal doemscenario's op terroristisch gebied: wat als terroristen een (digitaal) virus kunnen verspreiden? Wat als terroristen nucleair materiaal, zoals chemische wapens tot hun beschikking hebben? Zolang dergelijke wapens bestaan, is er ook een risico dat deze in verkeerde handen vallen. Kennisdeling over kunstmatige intelligentie en genetische modificatie vormt ook een risico voor individuen met slechte intenties. Tegelijkertijd is de verwachting dat terrorisme zoals wij dat zullen meemaken de komende 20 jaar relatief weinig veranderd ten opzichte van nu. Ook in de afgelopen jaren zijn er vrij 'amateuristische' aanslagen geweest, namelijk met gebruikmaking van messen of op publiek inrijdende auto's. Juist omdat dit type aanslagen zo eenvoudig te organiseren is, zal dit ook blijven plaatsvinden.

De aanpak in 2035
De onderlinge verbondenheid van bedrijven en sectoren zal alleen maar groter worden. Hierdoor is het belangrijk om ervoor te zorgen dat processen ook onafhankelijk van elkaar kunnen blijven functioneren als er iets mis gaat. Het schetsen van een aantal realistische scenario's kan helpen om met het personeel te oefenen hoe zij moeten handelen bij een terroristische aanslag of dreiging. Een veiligheidsdeskundige moet zowel in het kader van preventie als repressie zich continu bewust zijn van het feit dat terroristen aandachttrekkerij als doel hebben. Het blijft ook voor terrorismebestrijding belangrijk om het basisveiligheidsniveau van de organisatie op orde te hebben. Fysieke veiligheidsmaatregelen zoals toegangspoorten of elektronische maatregelen - toegangscontrolesystemen en camera's - vormen ook een bescherming tegen terroristen. Hiervoor is

het niet noodzakelijk om (extra) te investeren, omdat deze algemene veiligheidsmaatregelen vaak al worden toegepast. Aandacht voor terrorismebestrijding betekent dus niet automatisch extra kosten of extra inspanning. Tevens is het van belang dat organisaties door een inventarisatie zicht hebben op alle risicovolle objecten die zich in het bedrijf of op het bedrijfsterrein bevinden. Hierdoor kunnen er dreigingsanalyses worden opgesteld, bijvoorbeeld als onderdeel van de algemene risicoanalyse. Een veiligheidsdeskundige moet in het kader van de aanpak van terrorisme beseffen dat het een grensoverschrijdend en gemeenschappelijk probleem is. Hierbij is samenwerking met andere (buitenlandse) organisaties van belang door best practices van terrorismebestrijding met elkaar te delen.

Voor een veiligheidsdeskundige wordt het ook steeds belangrijker rekening te houden met impactmanagement. In het geval er iets mis gaat, is de communicatie van organisaties meestal gericht op voorkoming van imagoschade: 'wij hebben er in ieder geval alles aan gedaan' of het probleem wordt geheel ontkend. Dergelijke crisiscommunicatie zal niet meer werken. Een veiligheidsdeskundige moet een duidelijke visie hebben voor de aanpak van terrorisme en dit uitstralen naar de buitenwereld. Een behoorlijk improvisatievermogen omdat iedere situatie weer anders kan zijn, is hierbij ook geen overbodige eigenschap van een veiligheidsdeskundige.

In het algemeen geldt dat de veiligheidsdeskundige moet bijblijven en actuele kennis nodig heeft op technologisch en op cyber gebied. Big data gaan een grotere rol spelen bij de aanpak van terrorisme. Echter, het beschikken over meer informatie is niet per definitie beter. De voorspellende waarde van data wordt wellicht ook wel overschat. De suggestie wordt gewekt dat terrorisme kan worden voorspeld en dat daarvoor een inbreuk op de privacy gemaakt moet worden. Het is maar zeer de vraag of dat daadwerkelijk zo is. We willen zo graag dat het werkt, maar of het werkt dat weten we eigenlijk niet. Daar zou de komende jaren meer onderzoek naar gedaan moeten worden om te kunnen bewijzen of gebruikmaking van big data een effectieve aanpak voor terrorismebestrijding is.

Dit artikel is samengesteld op basis van inzichten uit interviews met mevr. Liesbeth van der Heide en mevr. Quirine Eijkman. Liesbeth van der Heide is onderzoeker en docent bij het Centrum voor Terrorisme en Contraterrorisme (Universiteit Leiden) en verricht tevens onderzoek voor het International Centre for Counter-terrorisme (ICCT) in Den Haag. Quirine Eijkman is senior-onderzoeker, docent Veiligheid & Rechtsstaat en lector Toegang tot het Recht bij de Hogeschool Utrecht. Ook doceert zij aan verschillende masteropleidingen van de Universiteit Leiden vakken op het gebied van terrorismebestrijding, cybergovernance, internationaal crisis- en security management en mensenrechten.

Opgesteld door: dhr. S. Kraaijenbrink
Functie en organisatie: Junior Onderzoeker bij Crisislab