Pilot Approach to Develop a DBT-like Threat Statement from Open Source Data

SAND2016-10879C

David Ek
Sandia National laboratories (drek@sandia.gov)

This presentation outlines the rationale and approach taken to develop a National Threat Statement as a basis for security requirements using open source data on terrorist and criminal events

Pilot Approach to Develop a DBT-like Threat Statement from Open Source Data

Developing a Threat criteria, such as a design basis threat based upon an assessment of the current threat is described as a Fundamental Principle in the Amendment to the CPPNM, and as an Essential Element in the IAEA Nuclear Security Series Fundamentals.

However, development of such a Threat Statement requires input from Intelligence and Law Enforcement Authorities. For some Competent Regulatory Authorities, gaining participation of these authorities to assist with conducting a Threat Assessment in support this effort can be very difficult.

2/3

Pilot Approach to Develop a DBT-like Threat Statement from Open Source Data

This presentation will describe the effort and approach undertaken to assist States to develop a meaningful threat criteria based on the assessment of the current threat, when involvement of the intelligence community was not realistic.

Gathering Threat Data

The START Program at the University of Maryland has collected data on terrorism events around the world, and have acquired extensive experience in gathering data on criminal and terrorist events.

They were contracted to gather regional and national data from numerous open sources, including:

- **News outlets**
- **Academic and other media sources**
- **Court records**

Please click on the boxes below.

Starting Point

Presenting in more detail

Zooming in

Navigation

Gathering Threat Data

The criteria around which the searches were conducted included:

- **Focused on 10-12 events for which adequate data was available**
- **Focused on the recent events (no older than 5-10 years)**
- **Priority of events were:**

Events occurring in	Involving RM/NM	TERRORISTS	CRIMINALS
THE STATE	1	2	3
NEIGHBORING STATES	2	3	4
THE REGION	3	4	5

Please click on the boxes below.

Starting Point → Presenting in more detail → Zooming in → Navigation

Evaluating Threat Data

Raw threat data was organized into motivation and capability categories in a spreadsheet:

ADVERSARY CHARACTERISTICS		Group 1	Group 2	Group 3	Group 4
MOTIVATIONS	Ideological	Y			Y
	Financial		Y		
	Political			Y	
CAPABILITIES	Group size	3	5	2	8
	Insider?	Y(1)	N	Y (2)	N
	weapons	handguns	grenades	Semi-automatic	none
	tools	Use of common hand tools	Ladder, wire cutters	Power tools	Hand tools
	etc				

Please click on the boxes below.

Starting Point

Presenting in more detail

Zooming in

Navigation

Evaluating Threat Data

A composite hypothetical adversary description was drawn from the many actual adversaries :

ADVERSARY CHARACTERISTICS		Composite Adversary
MOTIVATIONS	Ideological	Y
	Financial	Y
	Political	N
CAPABILITIES	Group size	5
	Insider?	Y(1)
	weapons	Handguns, grenades, semi-auto
	tools	Use of common hand tools and power tools
	etc	

Please click on the boxes below.

Starting Point

Presenting in more detail

Zooming in

Navigation

Evaluating Threat Data

The composite hypothetical adversary description was revised based on policy issues:

ADVERSARY CHARACTERISTICS		Composite Adversary	After Conservatism	After resources vs benefit	After Political Issues
MOTIVATIONS	**Ideological**	Y			
	Financial	Y			
	Political	N			***Y***
CAPABILITIES	**Group size**	5			
	Insider?	Y(2)		***(1)***	(1)
	weapons	Handguns, grenades, semi-auto			
	tools	Use of common hand tools and power tools			
	etc		***Cyber capabilities***	Cyber capabilities	Cyber capabilities

Please click on the boxes below.

Starting Point → Presenting in more detail → Zooming in → Navigation

The Resulting Threat Statement

- Based on open source data
- Using process steps to derive basis:
  - Composite adversary description
  - Modified for policy issues

ADVERSARY CHARACTERISTICS		THREAT STATEMENT
MOTIVATIONS	Ideological	Y
	Financial	Y
	Political	Y
CAPABILITIES	Group size	5
	Insider?	Y(1)
	weapons	Handguns, grenades, semi-auto
	tools	Use of common hand tools and power tools
	etc	Cyber Capabilities

Please click on the boxes below.

Starting Point → Presenting in more detail → Zooming in → Navigation