



TO HACK A TERRORIST

Modellierung der Entscheidungen von Attentätern

Ron Scheucher
Managing Partner
Mainland Labs



Notes on Risk Management

In welcher Welt leben wir, wo gleich zwei mörderische Konflikte direkt vor unserer Haustüre um unsere Aufmerksamkeit wetteifern? Mit welchen Risiken wird unser Land, wird ganz Europa, in Zukunft leben müssen, und was können bzw. müssen wir von den "Brandstiftern" erwarten? Dies sind entscheidende Fragen, die von der Politik bzw. den sicherheitsrelevanten Institutionen, wie dem Militär und Polizei (inklusive ihrer jeweiligen nachrichtendienstlichen Einheiten), zeitnah zu beantworten sind.

Wir wollen hier einen wichtigen Schritt beschreiben, der geeignet ist, das Sicherheitssystem unseres Landes deutlich leistungsfähiger und effektiver zu machen. Ausgangspunkt bildet dabei die Erkenntnis, dass moderne Risikomanagement-Systeme (wir sprechen hier nicht von Cyber-Risiken) bisher im Bereich der heimischen Sicherheitsbehörden noch nicht breit implementiert sind. Und das, obwohl diese, wie auch "schweres" Gerät (z.B. Kampf- und Schützenpanzer), selbstverständlich zur notwendigen modernen Sicherheitsinfrastruktur gehören. Gearbeitet wird heute weiterhin vor allem über "Experten"-Urteile, die in der Regel weder in risikostrukturierter Form vorliegen noch die multi-dimensionalen Zielfunktionen der relevanten Akteure adäquat berücksichtigen. Doch in welche Richtung müssen wir nun unsere Systeme entwickeln und ausbauen?



SICHERHEITSPOLITIK ALS FRAGE OPTIMALER RESSOURCEN-VERTEILUNG

Grundsätzlich ist eine Systematisierung (i.e. Professionalisierung) der Risikomanagement-Systeme in den Sicherheitsapparaten notwendig. Dies bedeutet zuerst einmal, dass die Zielsetzungen sowohl auf Seite der Verteidiger als auch auf Seite der Gefährder bestmöglich strukturiert (erheben, beschreiben, bewerten bzw. quantifizieren) werden. Auf Basis ausentwickelter Zielsysteme können bereits zentrale Sicherheitsfragen geklärt werden, u.a. die relative Attraktivität von Targets oder die spezifischen Inhalte von relevanten Bedrohungsszenarien. Um jedoch die alles entscheidende Frage nach der Verteilung der (knappen) Ressourcen auf einzelne Bedrohungen beantworten zu können, muss allerdings noch ein weiteres Problem gelöst werden, das bisher in den etablierten Sicherheitssystemen nur unzureichend behandelt wurde – die Strukturierung und Bewertung des Risikos. Sie ist die Voraussetzung für die informierte Allokation von monetären und personellen Ressourcen.



RESSOURCEN-VERTEILUNG

RISIKOKENNZAHLEN ALS BASIS

Einfache Risiko-Kennzahlen

Im Rahmen von Sicherheitssystemen sind grundsätzlich zwei Ansätze denkbar bzw. in anderen Ländern auch etabliert. Da gibt es einmal den Lösungsversuch über einfache Risiko-Kennzahlen, die sich jeweils an mehreren Risiko-Treibern orientieren können. Weit verbreitet ist etwa, z.B. im Zusammenhang mit definierten strategischen Angriffszielen, die Deduktion des Risikos (Wahrscheinlichkeit des Eintritts des Bedrohungsfalles) aus Bevölkerungskennzahlen. Das Argument wäre hier, dass die Konsequenzen eines Sicherheitsfalles eng mit Einwohnerzahlen und der Bevölkerungsdichte korreliert sind, da die beiden Kennzahlen den Wert von Angriffszielen (u.a. urbane Räume) für einen potenziellen Gefährder gut beschreiben. Vorteile dieses Ansatzes sind in der Praxis die Verständlichkeit des Konzepts und die gute Messbarkeit (i.e. die gute Verfügbarkeit von Daten). Gleichzeitig ist er allerdings auch sehr limitiert in den Möglichkeiten. So gehen nur wenige Aspekte in die Konstruktion der Indices ein. Die Wechselbeziehungen zwischen Bedrohung, Verwundbarkeit und potenziellen Schäden können z.B. ebenso wenig erfasst werden wie die spezifischen Lösungen, die einem potenziellen Angreifer im Rahmen von Anschlägen auf ein bestimmtes Ziel zur Verfügung stehen.



RESSOURCEN-VERTEILUNG

RISIKOKENNZAHLEN ALS BASIS

Ereignis-basierte Indikatoren

Die Qualität von Risikomanagement-Systemen liegt in der Erfassung und der Behandlung der einzelnen Perspektiven und Dimensionen von Bedrohungen; sie liegt in Systemen von Ereignis-basierten Indikatoren ("Event Based Indicators"). Diese bauen auf einer detaillierten Analyse äußerst spezifizierter Szenarien auf, für die (im Idealfall) ein breites Set an Daten zur Verfügung steht. Dabei können auch gleichzeitig sich überlagernde Events und multiple Angriffsziele verarbeitet werden. Die große Herausforderung im Rahmen dieses RM-Ansatzes bildet allerdings die Schätzung der Parameter der Szenarien. Die großen Vorteile sind hingegen die größere Verlässlichkeit (Treffsicherheit) durch die relativ hohe Erklärungstiefe. Einige Modelltypen können über die Ereignis-basierten Indikatoren aufgebaut werden (z.B. das ursprünglich aus der Versicherungswirtschaft stammende "RMS Terrorism Risk Model"), wir wollen jedoch an dieser Stelle näher auf die modernen "Value Models" bzw. Nutzen-basierten Modelle eingehen.

Über "Value Models" können speziell auch Mehrfachzielsetzungen der Akteure (Freund und Feind) und Trade-Offs zwischen Konsequenzen einzelner Aktionen innerhalb von Szenarien abgebildet werden. Value Models sind letztlich mathematische Programme, deren Optimierungsobjekt der Nutzen aus alternativen Sets an Aktivitäten bzw. Entscheidungen der relevanten Akteure im Rahmen einer Bedrohungssituation ist. Dieser Nutzen kann sich (wie im Falle mehrerer Zielsetzungen) über mehrere Teilnutzen-bildende Terme aufbauen, die in additiven oder multiplikativen Nutzenfunktionen (Aggregation) zusammengefasst werden. In den Modellen werden zudem offengelegte Risikostrukturen (wir sprechen vom "erwarteten" bzw. "risikoangepassten" Nutzen) integriert. Ressourcen werden auf Basis dieser Modelle nach der Höhe des durch das jeweilige Handlungsset erzielbaren Nutzen verteilt.



RISIKOSTRUKTURIERUNG VON EREIGNISSEN

VALUE-MODELL EINER TERRORISTISCHEN BEDROHUNG

Die Perspektive des Feindes

In der Folge wollen wir über die Perspektive eines Feindes (z.B. ein Terrorist oder ein autoritär-regierender Präsident eines feindlichen Landes) die Funktionsweise und den Wert von Value Models darstellen. Nach einer Ableitung konkreter operationalisierbarer Ziele der Sicherheitspolitik in Bezug auf konkrete Szenarien und den Aufbau von Mittel-Zweck-Beziehungen (z.B. mehr Personenkontrollen führen zu einer höheren Wahrscheinlichkeit potenzielle Attentäter zu enttarnen) werden (aggregierte) Nutzenfunktionen formuliert, die realistischerweise auch Nutzenkonflikte berücksichtigen (können). Diese Nutzen- oder Wertkonflikte beschreiben dabei Situationen, in denen die Erreichung eines bestimmten Zieles nur dadurch verbessert werden kann, dass man in Kauf nimmt, dass sich der Zielerreichungsgrad in einem anderen Bereich verringert. Diese Trade-Offs zwischen Prozessergebnissen sind in der Regel komplex, aber gleichzeitig elementar für den Aufbau leistungsfähiger Entscheidungssysteme. Um sie zu definieren, müssen die verschiedenen isolierten Effekte explizit (Aufbau einer über alle Effekte hinweg einheitlichen Währung, z.B. Monetarisierung) oder implizit (qualitatives Experten-Urteil) in Relation zu einander gebracht bzw. (aus)tauschbar gemacht werden. Wir stellen die Logik im Rahmen des Nutzen-Assessments in der Folge anhand eines Value-Modells eines Terroristen (das Kalkül des Feindes ist für die Entscheidungen der Sicherheitsbehörden gleichermaßen wertvoll wie ihr eigener Zielekatalog) dar.



RISIKOSTRUKTURIERUNG VON EREIGNISSEN

VALUE-MODELL EINER TERRORISTISCHEN BEDROHUNG

Ziele und Entscheidungsmodell eines Terroristen

Ausgangspunkt ist in unserem Beispiel ein einzelner Terrorist, der plant, die Kontrolle über eine bestimmte Menge Plutonium zu erlangen, um damit z.B. eine "schmutzige" Bombe zu bauen. In diesem Zusammenhang steht der potenzielle Attentäter vor einer Reihe von Entscheidungen. Wie (Kauf oder Diebstahl) und wo (Institution, Vertriebskanal) bekommt er Zugriff auf das radioaktive Material? In welcher Form (fest oder gelöst, rein oder verunreinigt) soll das Plutonium bezogen werden? Wie viel des Transurans (Gewicht, Wirkung) soll gekauft werden? Wie kann er sich gegen die Strahlung schützen? ... usw. Das Entscheidungskalkül des Terroristen lässt sich nun als aggregierte Nutzenfunktion mit (z.B.) 3 Zielsetzungen beschreiben:

- (1) Maximierung der Menge des eingesetzten Plutoniums (Wirkungsradius)
- (2) Maximierung der Reinheit des eingesetzten Plutoniums (Effektivität)
- (3) Minimierung der persönlichen Gesundheitsschäden (eigene Verstrahlung)

Über das drei-dimensionale Kalkül lassen sich nun die Entscheidungsvariablen des mathematischen Programms beschreiben:

- x_1 ... einsetzbares Plutonium (in Gramm)
- x_2 ... Reinheit des ursprünglich verfügbaren radioaktiven Materials
(z.B. Gramm Uran pro Liter einer mit dem Transuran versetzten Flüssigkeit)
- x_3 ... im Rahmen der Anschlagvorbereitung einwirkende Strahlendosis (Gray/h)

RISIKOSTRUKTURIERUNG VON EREIGNISSEN

VALUE-MODELL EINER TERRORISTISCHEN BEDROHUNG



Zusätzlich muss für unsere Zwecke das Intervall festgelegt werden, in dem sich die Werte der Entscheidungsvariablen x_1 , x_2 und x_3 bewegen sollen (siehe dazu Abbildung 1). Dabei werden speziell auch die möglichen Einsatzszenarien mitberücksichtigt.

Attribut	Maßeinheit	Untere Grenze	Obere Grenze
x_1 = Plutonium	g.Pu	10	2.500
x_2 = Reinheit	g.U/L	333	0
x_3 = Verstrahlung	Gy/h	100	0

Abb.1: Spannweite der Entscheidungsvariablen

Die Ableitung der aggregierten Nutzenfunktion $u(x_1, x_2, x_3)$ erfolgt in unserem Beispiel auf Basis von bestimmten (getesteten) Annahmen, u.a. ob der Trade-Off zwischen 2 Variablen durch den Wert der dritten beeinflusst wird oder nicht.

$$u(x_1, x_2, x_3) = \sum_{i=1}^3 k_i u_i(x_i) \quad \text{Additive Nutzenfunktion}$$

$$1 + ku(x_1, x_2, x_3) = \prod_{i=1}^3 \{1 + k_i u_i(x_i)\} \quad k \neq 0 \quad \text{Multiplikative Nutzenfunktion}$$

$u(x_1, x_2, x_3)$... Nutzenfunktion des Terroristen

x_1 ... Entscheidungsvariablen des Terroristen

$u_i(x_i)$... Teilnutzenfunktion des Terroristen in Bezug auf die einzelnen Variablen

k bzw. k_i ... Konstante (Skalierungsfaktor)

Die erste angeführte Gleichung beschreibt eine additive Nutzenfunktion (Spezial- bzw. Grenzfall der rechtsstehende multiplikativen Nutzenfunktion).

RISIKOSTRUKTURIERUNG VON EREIGNISSEN

VALUE-MODELL EINER TERRORISTISCHEN BEDROHUNG

Über die Teilnutzen-Funktionen zum Gesamt-Assessment der Bedrohung

Die möglichen Teilnutzen-Werte bewegen sich in unserem Beispiel für alle Entscheidungsvariablen im Intervall von 0 bis 1. Für die erste Variable "Plutonium-Menge" (x_1) (siehe oben) lässt sich dies wie folgt abbilden: $u_1(x_1)=[0,1]$; d.h. $u_1(10)=0$ und $u_1(2.500)=1$. Die große Herausforderung ist nun jedoch, den Verlauf der Nutzenfunktion zwischen den gesetzten Grenzen abzubilden. Keeney, ein Berater des DHS in den USA, setzt dafür Expertenurteile ein, die fiktive Lotterieregebnisse in die Nutzenwertgenerierung miteinbeziehen. So wird z.B. abgeschätzt, dass der Terrorist zwischen einer sicheren Verfügbarkeit von 800g Plutonium und einer Lotterieteilnahme, die mit 50%-Wahrscheinlichkeit entweder 10 oder 2.500g des Materials bringt, indifferent ist. Daraus folgt: $u_1(800)=0,5$ bzw. $u_1(800) = 0,5u_1(10) + 0,5u_1(2.500)$. Weitere Punkte können auf diesem Wege ermittelt und die Kurven entwickelt (gefittet) werden. In Bezug auf die zwei weiteren Teilnutzenfunktionen wird ähnlich vorgegangen. Abbildung 2 zeigt die über diesen Weg aufgebauten Verläufe der einzelnen mit den drei Entscheidungsvariablen verbundenen (Teil-)Nutzenfunktionen.

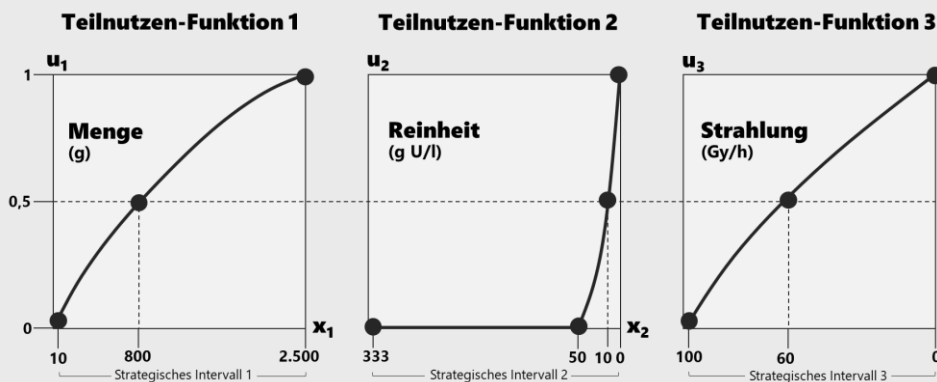


Abb.2: Entwickelte Verläufe der Teilnutzen-Funktionen des Terroristen

Keeney, Ralph.L. (2007) "Modeling Values for Anti-Terrorism Analysis". Risk Analysis 27 (3)

RISIKOSTRUKTURIERUNG VON EREIGNISSEN

VALUE-MODELL EINER TERRORISTISCHEN BEDROHUNG

Abgrenzung der Trade-Offs

Die Bestimmung der Trade-offs zwischen den einzelnen im Auge des Terroristen Nutzen-treibenden Aspekten (Teilnutzen) eines Anschlages ist die Voraussetzung, um unser Entscheidungsmodell (aggregierte Nutzenfunktion) vollständig beschreiben zu können. In diesem Zusammenhang werden die einzelnen strategischen Aspekte der Tat paarweise miteinander verglichen. So kann einmal analysiert werden, zwischen welchen Kombinationen von x_1 (Gewicht) und x_3 (Strahlung) der potenzielle Attentäter (ceteris paribus) indifferent wäre, oder zwischen welchen Kombinationen von x_2 (Reinheit des Kampfstoffes) und x_3 (Strahlung). Siehe dazu Möglichkeitsräume des Terroristen in Abbildung 3.

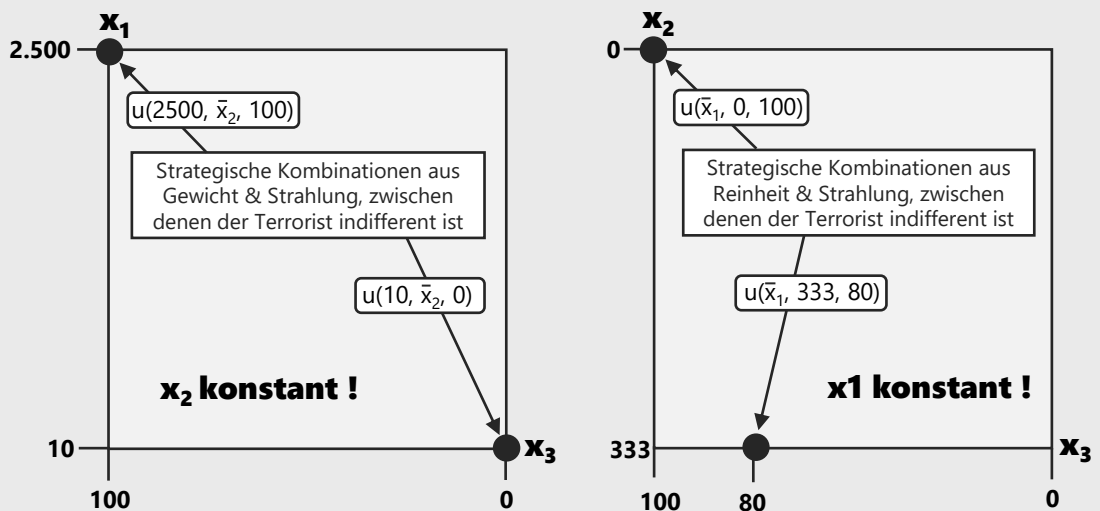


Abb.3: Möglichkeitsräume des Terroristen (in \mathbb{R}_2) - Beispiele

RISIKOSTRUKTURIERUNG VON EREIGNISSEN

VALUE-MODELL EINER TERRORISTISCHEN BEDROHUNG



Abgrenzung der Trade-Offs

In der Praxis werden beliebige Kombinationen von Merkmalen des Anschlags (Gewicht des radioaktiven Material, seine Reinheit und Strahlung) analysiert und schrittweise selektiv entlang der 3 Dimensionen angepasst, bis gleichwertige Setups des Anschlags (natürlich nicht durch Informationen aus der Terrorszene) gefunden werden. Im oben dargestellten ersten Fall können wir z.B. festhalten, dass folgendes gilt:

$$u(2500, x_2, 100) = u(10, x_2, 0) \quad u \dots \text{Nutzen}$$

Durch Einsatz der über Bewertungen abgeleiteten mathematischen Gleichungen der in Abbildung 2 dargestellten Nutzenfunktionen und der nun etablierten Indifferenzkonstellationen (in unserem Fall der Merkmalskombinationen x_1x_2 , x_1x_3 und x_2x_3) können die Koeffizienten k und k_i in den Teilnutzenfunktionen bzw. der aggregierten Nutzenfunktion (Value Model) ermittelt werden. Die Aggregation der einzelnen ausformulierten Teilnutzenfunktionen erfolgt hier im Rahmen einer multiplikativen Nutzenfunktion (unter Berücksichtigung der Interdependenzen zwischen den Entscheidungsvariablen des Terroristen). Diese kann nun genutzt werden, um die potenziellen Angriffsszenarien des Terroristen (von seiner Perspektive aus) eindeutig zu reihen.

Ergebnis des skizzierten Analyseprozesses ist die Identifikation des zentralen (wahrscheinlichsten) Set-Ups eines möglichen Anschlags mit einer schmutzigen Bombe (Nutzenoptimum des Terroristen). Auf der Basis, dass der Feind zumindest in Bezug auf die Anschlagsplanung (und hier könnten wir weitere Variablen x_n , wie z.B. spezifische Charakteristika potenzieller Ziele, einführen) rational handelt, können so Sicherheitsmaßnahmen (und die dahinter liegenden Ressourcen) in der Praxis optimal, d.h. zielgenau und detailliert, angeleitet werden.

RISIKOSTRUKTURIERUNG VON EREIGNISSEN

DIE BEDEUTUNG VON VALUE-MODELLEN

Fazit

Der Einsatz moderner Value-Modelle bringt viele Vorteile für Sicherheitsbehörden bzw. für all jene Stellen, die sich mit Risikomanagement im Rahmen sozialer, wirtschaftlicher und politischer Prozesse beschäftigen.

- Sie ermöglichen ein besseres Verständnis des Verhaltens, der Strategien und Handlungen, von Gefährdern bzw. Gruppen von Gefährdern
- Sie liefern die Grundlage für eine zielgerichtete Priorisierung potenzieller Angriffsziele (z.B. aus dem Blickwinkel der Gefährder)
- Sie ermöglichen die Abgrenzung potenzieller Angriffsschäden und liefern gleichzeitig Ansätze zur Schadensreduktion
- Die Ergebnisse von Value-Modellen im Bereich Sicherheit können genutzt werden, um Gegenmaßnahmen der Behörden zu bewerten und zu priorisieren.
- Die Entwicklung von spezifischen Value-Modellen stellt einen wichtigen Lernprozess für beteiligte Organisationen dar.
- Sicherheitspolitische Entscheidungen können über Value-Modelle erklärt, begründet und kommuniziert werden.

Es ist an der Zeit, moderne ökonomische Modellierungen und Verfahren auch in die heimische Sicherheitsinfrastruktur zu integrieren. Mainland Labs-Experten bringen dabei die notwendige Erfahrung und quantitative Expertise in den Aufbau moderner leistungsfähiger Value-Modelle ein. Kommen wir ins Gespräch. Wir freuen uns auf die Diskussion.





Our Platform for Ground-Breaking
Economic Thinking and Consulting.

Mainland Economic Consultants GmbH
Office Vienna | Büro Wien
Klagbaumgasse 9, A-1050 Vienna | Wien

T +43 (0)1 7109036 E office@mainland.at
F +43 (0)1 7109036-36 W mainland-labs.com