

GEFÖRDERT VOM



**Bundesministerium
für Bildung
und Forschung**

Im Zuge der Förderrichtlinien
„Neue ökonomische Aspekte“ des BMBF
im Rahmen des Programms „Forschung für
die zivile Sicherheit“ der Bundesregierung.
www.sicherheitsforschungsprogramm.de

Ökonomische Bewertungs- verfahren zur Evaluierung von Sicherheitsmanagement: Ein einleitender Überblick

August 2017

Dr. Alexander Schulan, schulan@wiwi.uni-frankfurt.de
Prof. Dr. Horst Entorf, entorf@wiwi.uni-frankfurt.de
Lehrstuhl für Ökonometrie, Goethe-Universität

www.4d-sicherheit.de

Projektkoordinator: Technische Universität Berlin,
Zentrum für Technik und Gesellschaft (ZTG)

Projektpartner:

antwortING Beratende Ingenieure PartGmbH
European Aviation Security Center e.V. (EASC)

Goethe-Universität, Fachbereich

Wirtschaftswissenschaften



4D-SICHERHEIT
EFFIZIENZ
RECHT
VERTRAUEN

Zusammenfassung:

Die Ökonomie der Sicherheit zeigt, dass fehlende Sicherheit Kosten verursacht. Materialisiert sich die Unsicherheit in Form von potenziellen Schäden an Personen und Gegenständen, so verursacht dies zu erwartende Kosten. In den Wirtschaftswissenschaften gibt es zahlreiche Methoden, wie z. B. die Kosten-Nutzen Analyse, die Kosten-Effektivitäts Analyse, die Multi-Kriterien Analyse und den Return on Security Investment, um den Nutzen eines effektiven oder effizienten Sicherheitsmanagements zu erfassen, zu messen und zu bewerten. Der durch eine Sicherheitsmaßnahme erreichte Sicherheitsgewinn kann anhand von statistischen Testverfahren ermittelt werden. Hierfür gibt es eine Reihe von statistischen Kennzahlen für verschiedene Bereiche der Sicherheit, z. B. False Match Rate und False Non-Match Rate für biometrische Anwendungen, Reaktionszeit für den Rettungsdienst oder erwartete Unfallhäufigkeit für die Straßenverkehrssicherheit.

Inhaltsverzeichnis:

1. Sicherheit ist auch ein ökonomisches Thema.....	4
2. Ökonomische Bewertungsverfahren für Sicherheitsmaßnahmen	5
2.1 Kosten-Nutzen Analyse	6
2.2 Kosten-Effektivitäts Analyse.....	8
2.3 Multi-Kriterien Analyse	10
2.4 Return on Security Investment	11
3. Statistische Testverfahren	11
3.1 Grundlagen statistischer Tests	12
3.2 Biometrische Testverfahren.....	13
3.3 Bilderkennung	15
3.4 Rettungsdienst	16
3.5 Verkehrssicherheit	16
4. Bewertung von Sicherheitsmaßnahmen durch SERV-Dimensionen	17
Literatur.....	19

1. Sicherheit ist auch ein ökonomisches Thema

Der Wunsch nach Sicherheit führt zu einem Spannungsfeld zwischen ethischen und ökonomischen Aspekten. Es gilt aber: „Sicherheit ist teuer, aber *fehlende* Sicherheit kann noch deutlich teurer werden.“ (Entorf 2015).

Fehlende Sicherheit wird von Individuen als Bedrohung des Status Quo, als Beeinträchtigung der Lebenszufriedenheit und als unerwünschte „Unsicherheit“ wahrgenommenen, so dass Maßnahmen unternommen werden, um die Unsicherheit zu vermeiden oder zumindest zu reduzieren. Dadurch entstehen Kosten durch Ausgaben für die jeweilige Sicherheitsmaßnahme oder Kosten in Form von unerwünschten Verhaltensänderungen.

Die Frage, warum es sinnvoll ist, Sicherheitsmaßnahmen ökonomisch zu bewerten, lässt sich mit der statistischen Unsicherheit von Ereignissen und einer zukunftsorientierten Entscheidungsfindung begründen. Folgeschwere Ereignisse wie Unfälle, kriminelle Akte oder Naturkatastrophen können mit einer gewissen Wahrscheinlichkeit eintreten, was z.B. Unternehmensgewinne oder privates Wohlergehen im Falle des Falles nachhaltig schmälern oder gar zerstören kann. Investitionen in Sicherheit können das zukünftige Risiko mindern, aber gleichzeitig den erwarteten Nutzen aufgrund der entstehenden Kosten verringern. Wie sehr potentielle negative Ereignisse Entscheidungen beeinflussen, ist von Person zu Person unterschiedlich und hängt vom Grad der so genannten Risikoaversion ab. Die meisten Menschen empfinden es aber eher als unangenehm, möglicherweise in der Zukunft von einem negativen Ereignis betroffen zu sein, d.h. sie sind risikoscheu. Die Sorge vor negativen Ereignissen und den dadurch verursachten materiellen und immateriellen Kosten begründen in Personen den Wunsch, die bestehende Unsicherheit ganz oder teilweise zu reduzieren.

Der Rückgang der Unsicherheit sollte mit effizientem Einsatz der vorhandenen finanziellen Mittel erreicht werden. Um das Verhältnis von finanziellem Aufwand und Nutzen möglichst optimal zu gestalten, kann die Ökonomik mit Theorien und Methoden hilfreich zur Seite stehen. Dies gilt für eine einzelne Person, die z.B. den „sicheren Verlust“ einer Versicherungsprämie in Kauf nimmt, um im Schadensfall das Ausmaß des „unsicheren Schadens“ reduzieren zu können. Dies gilt auch für die Allgemeinheit, wo auf politischer Ebene die drohenden Kosten eines negativen Ereignisses und die Zahlungsbereitschaft der Allgemeinheit

für eine Sicherheitsmaßnahme zur Abwendung oder Eingrenzung des Risikos berücksichtigt werden.

Die Bewertung von Sicherheitslösungen im Rahmen eines ökonomischen Bewertungsverfahrens kann den Zielkonflikt zwischen begrenzten finanziellen Mitteln und dem Wunsch nach einem möglichst hohen Sicherheitsniveau abbilden. Der folgende Abschnitt gibt einen Überblick über gängige ökonomische Bewertungsverfahren, die Entscheidern eine fundierte Auswahl zwischen konkurrierenden Sicherheitsprojekten ermöglichen.

2. Ökonomische Bewertungsverfahren für Sicherheitsmaßnahmen

Da sowohl der drohende Schaden als auch die Vermeidung von Unsicherheit mit Kosten behaftet ist, wird das Thema Sicherheit also sowohl zu einem ökonomischen als auch mathematisch-statistischen Thema (Entorf 2015). Jede sicherheitsrelevante Entscheidung basiert auf dem Abwägen des Sicherheitsgewinns, d.h. der Wert der vermiedenen Kosten und des vermiedenen Leids, mit den hierfür aufzubringenden Kosten. Hierbei können wichtige Aspekte wie die Wahrscheinlichkeit des Eintreffens eines negativen Ereignisses mit Methoden der Statistik beleuchtet und die Zahlungsbereitschaft und -fähigkeit der betroffenen Personen mit Methoden der Ökonomik analysiert werden.

Eine neue Sicherheitsmaßnahme soll zu einem Mehr an Sicherheit führen und die empfundene Unsicherheit reduzieren. Der Sicherheitsgewinn entspricht der Differenz zwischen dem dann erwarteten und dem aktuellen Sicherheitsniveau. Mit statistischen Kennzahlen kann der Sicherheitsgewinn operationalisiert und mit empirischer Evidenz unterlegt werden. Darüber hinaus ist eine ökonomische Betrachtung einer möglichen Sicherheitsmaßnahme hilfreich, um die knappen finanziellen Ressourcen effizient für neue Sicherheitslösungen einzusetzen. Dabei quantifiziert die ökonomische Analyse die Kosten in Geldeinheiten und den Nutzen entweder auch in Geldeinheiten oder in einer anderweitig definierten Einheit, wie z.B. die Zahl der Verkehrsunfälle.

Das aus ökonomischen Aspekten „optimale“ Sicherheitsniveau hängt von Grenzkosten und Grenznutzen der Sicherheitslösung ab. Im Optimum entspricht der Grenznutzen den Grenzkosten. Die Kosten einer neu zu installierenden Sicherheitsmaßnahme entstehen in erster Linie kurzfristig, der Nutzen hingegen stellt sich aber langfristig ein (Brück 2004).

Bezieht sich die Kosten-Nutzen Analyse auf einen mehrjährigen Zeitraum, sollte daher der Nutzen mit einer dem Risiko adäquaten Rate diskontiert werden, um heutige Werte von Kosten und Nutzen miteinander vergleichen zu können.

Auch wenn bei jedem Investitionsprojekt der Entscheider Kosten und Nutzen gegeneinander abwägt, sind aufgrund der signifikant unterschiedlichen Charakteristika denkbarer Investitionsprojekte unterschiedliche ökonomische Bewertungsverfahren etabliert, um auf die Besonderheiten des Projekts eingehen zu können. Sind Kosten und Nutzen gut zu erfassen, ist die Kosten-Nutzen Analyse (Abschnitt 2.1) hilfreich. Ist der Nutzen nicht in Geldeinheiten messbar, so wird eine aussagekräftige Hilfsgröße konstruiert, um den Nutzen in der ökonomischen Effizienzanalyse berücksichtigen zu können. Dies wird in Abschnitt 2.2 anhand des Quality Adjusted Life Year (QALY) im Gesundheitsbereich dargestellt. Optimiert die ökonomische Analyse nicht nur die Zielerreichung einer Größe, z.B. Nutzenmaximierung, sondern optimiert mehrere Ziele simultan, z.B. Umweltschutz und eine gerechte Vermögensverteilung, so ist eine Multi-Kriterien Analyse (Abschnitt 2.3) geeignet.

2.1 Kosten-Nutzen Analyse

Die Kosten-Nutzen Analyse ermöglicht dem Entscheider eine fundierte Entscheidung für oder gegen ein Investitionsprojekt, da sie die Kosten und den erwarteten Nutzen miteinander vergleicht. Übersteigt der erwartete Nutzen die Kosten, so sollte die Sicherheitsmaßnahme durchgeführt werden. Übersteigen hingegen die Kosten den erwarteten Nutzen, sollte die Sicherheitsmaßnahme nicht durchgeführt werden. Diese Entscheidungsregel trifft für alle in diesem Text vorgestellten ökonomischen Bewertungsverfahren zu.

Bei einer ökonomischen Kosten-Nutzen Analyse ist wichtig, dass sowohl die Kosten als auch der Nutzen mit ausreichender Genauigkeit erfasst werden können. Nur so kann sichergestellt werden, dass Fehlallokationen in Sicherheitslösungen vermieden werden. Bei einer Fehlallokation würde entweder zu wenig in Sicherheit investiert, so dass eine gesellschaftlich erwünschte Reduzierung der Unsicherheit unterbleiben würde, bzw. zu viel in Sicherheit investiert, so dass die begrenzten finanziellen Ressourcen bei der Durchführung eines alternativen (Sicherheits-) Projekts gesellschaftlich optimaler investiert wären.

In der ökonomischen Literatur wird zwischen materiellen und immateriellen Kosten der Unsicherheit unterschieden, wobei materielle Kosten sowohl direkt als auch indirekt sein kön-

nen (Entorf 2015). Direkte materielle Kosten sind z.B. medizinische Versorgung, materielle Schäden, Verlust an Eigentum, Lohnfortzahlung, Kosten von Polizei und Justiz und Produktivitätseinschränkungen durch Ausfall oder Pflege. Für die direkten Kosten bestehen Marktpreise, so dass sie gut in Geldeinheiten quantifizierbar sind. Indirekte materielle Kosten sind z.B. Auswirkungen der Produktivitätsverluste, Lohneinbußen des Opfers, niedrigere Steuereinnahmen, negative Effekte für Unternehmen, Effizienzverluste, Friktionsverluste, evtl. Neueinstellungen mit Turnover-Kosten, geringere Teamleistung, geringere Netzwerkeffekte und Präventionskosten bei Polizei, Feuerwehr und Justiz. Immaterielle Kosten der Unsicherheit sind z.B. Schmerz, Einschränkung der Lebensqualität, Behinderung, Kriminalitätsfurcht, Traumata und Reputationsverlust für Unternehmen oder Kommunen.

Die verschiedenen indirekten Kosten sind facettenreich, so dass die Bezifferung der genauen Höhe schwierig ist. Weiter kann es bei einer Sicherheitsmaßnahme immaterielle Kosten geben. Ein Beispiel hierfür sind Verhaltensänderungen oder Einschränkungen aufgrund einer Sicherheitsmaßnahme wie z.B. der Vorratsdatenspeicherung. Als Folge der mangelnden Privatsphäre können sich Personen entscheiden, bei unverschlüsselter Kommunikation private Sachverhalte nicht mehr oder in anderer Form zu kommunizieren, so dass diese Einschränkungen Kosten darstellen. Da die Schätzung immaterieller Kosten auf subjektiven Annahmen und Wertvorstellungen beruht, können individuelle Schätzungen der immateriellen Kosten voneinander abweichen.

Der Nutzen einer Sicherheitsmaßnahme ist die Reduzierung der Kosten der Unsicherheit und somit die vermiedenen „Kosten“ im weitesten Sinne, also finanzielle Kosten, aber auch die Vermeidung von Schmerz und Leid (Entorf 2015). Die oben dargestellte Aufschlüsselung nach direkten materiellen, indirekten materiellen und immateriellen Kosten und deren Beschreibung trifft daher ebenso auf die vermiedenen Kosten zu.

Obwohl das Konzept des Nutzens durch den Utilitarismus und die Mikroökonomik theoretisch gut fundiert ist, ist die Quantifizierung des Nutzens einer Sicherheitslösung in Form von vermiedenen Kosten in der Regel anspruchsvoller als die Quantifizierung der Kosten. Sicher ist aber, dass eine effektive Sicherheitslösung die Höhe des Schadens oder dessen Eintrittswahrscheinlichkeit reduziert. Nicht nur moralisch schwierig ist die Bezifferung der vermie-

denen Kosten in Geldeinheiten bei Verletzungen oder sogar Todesfällen (siehe Abschnitt 2.3 für ein Maß, das Gesundheitseinbußen quantifiziert).

Tritt der erwartete Nutzen der Sicherheitslösung erst nach einigen Jahren ein, ist es zweckmäßig im Rahmen einer Zeitwertberücksichtigung des Nutzens diesen unter Berücksichtigung seiner Unsicherheit zu diskontieren, um den heutigen Zeitwert des Nutzens mit heute anfallenden Kosten vergleichen zu können.

Weiter muss bei der ökonomischen Bewertung einer Sicherheitsmaßnahme auch die Anreizstruktur überprüft werden (Entorf 2015). Ein möglicher negativer Anreiz eines gestiegenen Sicherheitsniveaus kann sein, dass Personen dadurch zu riskanterem Handeln neigen („Moral Hazard“). Zum Beispiel hat bei einem gesellschaftlich erwünschten Rückgang von ansteckenden Krankheiten durch Impfungen der Einzelne – aufgrund der reduzierten Ansteckungsgefahr – einen Anreiz auf die Impfung zu verzichten, und sich somit nicht dem Risiko der Nebenwirkungen einer Impfung auszusetzen.

Im Rahmen einer ökonomischen Kosten-Nutzen-Analyse bestimmen individuelle Präferenzen das konkrete jeweilige Nutzenniveau eines Individuums (Brück 2004). Daher kann eine Kosten-Nutzen Analyse zu einem ökonomisch nicht optimalen Sicherheitsniveau führen, wenn z.B. starke Emotionen zu einer verzerrten Wahrnehmung und dadurch zu einer Überschätzung des Risikos führen. In diesem Fall würden private und öffentliche Sicherheitsmaßnahmen in zu starkem Maße durchgeführt werden, so dass die Kosten den Nutzen übersteigen würden. So besteht die Gefahr, dass die heutige Sicherheitsgesellschaft dazu neigt, eher Unschuldige zu inhaftieren als Schuldige nicht zu belangen (siehe Abschnitt 3.1 für eine Erläuterung zu Fehler 1. und 2. Art).

2.2 Kosten-Effektivitäts Analyse

Die Kosten-Effektivitäts Analyse ist gut anwendbar für Projekte, deren Nutzen nur schwer abschätzbar ist, die Kosten aber gut zu bestimmen sind, z.B. bei Maßnahmen im Gesundheitssektor, Bildung oder Umweltschutz (European Commission 2014). Die Kosten-Effektivitäts Analyse vergleicht alternative Projekte, die alle den gleichen Effekt bewirken. Für gegebene Kosten maximiert die Kosten-Effektivitäts Analyse den Output und für einen gegebenen Output minimiert die Kosten-Effektivitäts Analyse die Kosten. Die Kosten werden bei einer Kosten-Effektivitäts Analyse in der gleichen Einheit erfasst wie bei einer Kosten-

Nutzen Analyse. Die Effektivität der in Frage stehenden Maßnahme wird jedoch in Abhängigkeit des Outputs nicht in Geldeinheiten gemessen. Vielmehr kann die Effektivität in Einheiten wie gewonnenen Lebensjahren oder Testwerten gemessen werden.

Die Kosten-Effektivitäts Analyse vergleicht konkurrierende Projekte anhand deren Verhältnis von Kosten und Nutzen. Durch eine inkrementelle Analyse werden an Hand des Incremental Cost-Effectiveness Ratio (ICER) die zusätzlichen Kosten für eine weitere Einheit Output ermittelt. Diese Kosten können z. B. Kosten pro QALY oder Kosten pro erfolgreichem Rettungseinsatz innerhalb der Hilfsfrist sein:

$$ICER = \frac{\Delta C}{\Delta E} = \frac{(C_a - C_b)}{(E_a - E_b)}$$

Wenn die Kosten von Projekt A (C_a) geringer sind als von Projekt B (C_b) und die Effektivität von Projekt A (E_a) größer ist als bei Projekt B (E_b), dann dominiert Projekt A Projekt B sowohl durch niedrigere Kosten als auch durch eine höhere Effektivität. In der Realität kann es aber gut sein, dass ein Projekt günstigere Kosten hat, das andere Projekt aber eine größere Effektivität. In diesem Fall gilt $C_a - C_b > 0$ und $E_a - E_b > 0$ oder $C_a - C_b < 0$ und $E_a - E_b < 0$, so dass eine erweiterte Dominanz vorliegt. In diesem Fall zeigt die Kosten-Effektivitäts Analyse durch das niedrigste Kosten-Nutzen Verhältnis (C_x/E_x) das kosteneffizienteste Projekt an. Daher ist es ökonomisch optimal, das vorhandene Budget beginnend mit der Investition in das Projekt mit dem niedrigsten Kosten-Nutzen Verhältnis zu belasten (man beachte, dass man bei gleicher Effektivität von A und B einfacherweise das kostengünstigste auswählt, da das ICER sonst auf einem Nenner von 0 basiert; analog ist das effektivere Projekt zu wählen, wenn $ICER=0$ wegen $C_a - C_b = 0$).

Ein Beispiel für die Kosten-Effektivitäts Analyse im Gesundheitsbereich ist das Quality-Adjusted Life Year (QALY). Diese Kenngröße berücksichtigt sowohl die Quantität als auch die Qualität eines Lebensjahres. Daher kann ein QALY als Maßeinheit für den Nutzen in einer ökonomischen Bewertung einer Sicherheitsmaßnahme einfließen. Zum Beispiel kann zur Beurteilung der Effizienz einer Sicherheitsmaßnahme in einer Kosten-Nutzen Analyse der QALY je Geldeinheit als Maß für die Effizienz verwendet werden. Dies ermöglicht auch einen Vergleich von konkurrierenden Projekten, da Gesundheit wünschenswert und wertvoll ist und daher maximiert werden soll.

Ein QALY quantifiziert den Nutzen von Gesundheit, indem die gesundheitsrelevante Qualität des Lebens gewichtet über den Zeitraum von einem Jahr berücksichtigt wird (Whitehead und Ali 2010). Die individuelle Gesundheit einer Person wird mit einem Wert von 1=perfekte Gesundheit bis 0=Tod auf einer Intervallskala beschrieben, d. h. eine Veränderung von 0,8 auf 0,9 hat den gleichen Wert wie eine Veränderung von 0,2 auf 0,3. Um die Präferenzen von Personen für bestimmte Gesundheitszustände zu ermitteln, können Umfragen erhoben werden, um verschiedenen Gesundheitszuständen einen Wert zwischen 0 und 1 zuzuordnen. Die Intervallskala des QALYs erlaubt auch eine Aggregation einzelner QALYs. Multipliziert man den Wert der individuellen Gesundheit mit der Anzahl der Jahre, in denen dieser individuelle Wert der Gesundheit zutrifft, erhält man den QALY als quantitatives Maß für den Nutzen der Gesundheit über den entsprechenden Zeitraum.

Die Konstruktion des konventionellen QALYs beruht u.a. auf den nicht unumstrittenen Annahmen, dass die Einheit eines QALYs über die Zeit hinweg für eine Person den gleichen Nutzen stiftet, als auch, dass die Einheit eines QALYs für alle Personen den gleichen Nutzen stiftet (Weinstein et al. 2009). Ein weiterer zu hinterfragender Punkt ist, mit welchem Zinssatz ein in der Zukunft erwarteter Nutzen von Gesundheit diskontiert werden soll, um den heutigen Nutzen davon zu ermitteln (Whitehead und Ali 2010).

2.3 Multi-Kriterien Analyse

Die Multi-Kriterien Analyse ist geeignet, um Investitionsprogramme zu bewerten, die gleichzeitig mehrere Ziele verfolgen (European Commission 2014). Die Multi-Kriterien Analyse optimiert im Hinblick auf verschiedene Kriterien, wobei die Ziele in messbaren Größen angegeben werden. Eine relative Gewichtung der verschiedenen Kriterien erfolgt durch die Entscheider. Das Ergebnis der Multi-Kriterien Analyse ist eine Reihenfolge der in Frage stehenden Investitionsprogramme. In jedem Fall sollte eine Multi-Kriterien Analyse auch durch eine Kosten-Nutzen Analyse für finanzielle und ökonomische Ziele ergänzt werden. Falls der Nutzen der Projekte nicht nur nicht-monetär bewertet werden kann, sondern auch nicht durch eine physische Einheit gemessen werden kann, sollte trotzdem eine quantitative Analyse durchgeführt werden. Gewichtet man den Einfluss der verschiedenen Maßnahmen auf die Kriterien und gewichtet die Kriterien, so liefert die Summe der Produkte von Gewicht und Einfluss eine Reihenfolge der Gesamtauswirkung der einzelnen Projekte. Wird von den Entscheidern z.B. Kriterium 1 mit 0,7 und Kriterium 2 mit 0,3 gewichtet und hat das Investi-

tionsprojekt A einen positiven Einfluss auf Kriterium 1 von 0,8 und auf Kriterium 2 von 0,5, so hat das Investitionsprojekt A eine Gesamtauswirkung von $0,8 \cdot 0,7 + 0,5 \cdot 0,3 = 0,71$.

2.4 Return on Security Investment

Ein weiteres Maß um die Effizienz einer Investition in eine Sicherheitsmaßnahme beurteilen zu können ist der „Return on Security Investment“ (ROSI). Somit ist auch der Return on Security Investment geeignet, um gemäß dem Kriterium der Effizienz unter verschiedenen zur Auswahl stehenden Sicherheitsmaßnahmen auszuwählen. Ähnlich einer Kosten-Nutzen Analyse setzt der Return on Security Investment den inkrementellen Anstieg des Sicherheitsniveaus, d. h. den Sicherheitsgewinn, zu den dafür notwendigen Kosten ins Verhältnis. Im Falle des Returns on Security Investment entspricht der Ertrag der Sicherheitslösung den vermiedenen Schäden. UcedaVelez (2008) definiert den Return on Security Investment als:

$$ROSI = \frac{ALE(\$) \times \% \text{ Mitigated by Control} - \text{Control cost} (\$)}{\text{Control Cost}(\$)},$$

wobei ALE = jährlich erwarteter Schaden (Annual Loss Expectancy),

% Mitigated by Control = Vermiedener Schaden in % und

Control Cost = Kosten der Sicherheitsmaßnahme entsprechen.

Return on Security Investment ist der erwartete Ertrag, den eine Sicherheitsmaßnahme im nächsten Jahr erzielen wird. Im Gegensatz zu einem klassischen positiven Ertrag in Finance, der einem tatsächlichen Cashflow entspricht, ist der Ertrag des Return on Security Investment ein vermiedener Schaden aufgrund der durchgeführten Sicherheitsmaßnahme.

Return on Security Investment wird oftmals im Bereich der IT-Sicherheit verwendet. Um das Konzept des Return on Security Investment in der Praxis anwenden zu können, müssen sowohl die Kosten als auch der vermiedene Schaden in Geldeinheiten quantifizierbar sein. So kann z. B. der Nutzen der Sicherheitsmaßnahme anhand von Ausfallsicherheit für Systeme oder Anlagen in Form von vermiedenen Betriebsunterbrechungen in Geldeinheiten quantifiziert werden.

3. Statistische Testverfahren

Die oben dargestellten ökonomischen Bewertungsverfahren für Sicherheitsmaßnahmen anhand ihrer Effizienz vergleichen Kosten und Nutzen einer Sicherheitsmaßnahme. Die Kos-

ten einer Sicherheitsmaßnahme können gewöhnlich relativ gut in Geldeinheiten angegeben werden (mit Ausnahme von immateriellen Kosten). Der Nutzen kann unter Umständen nur schwer in Geldeinheiten angegeben werden. Als Alternative können aber möglicherweise statistische Kennzahlen und Testverfahren die Effektivität einer Sicherheitsmaßnahme, d. h. das Ausmaß des Sicherheitsgewinns, quantifizieren. In diesem Fall können statistische Kennzahlen und Testverfahren helfen, den Nutzen für eine Bewertung der Sicherheitslösung anhand der Dimension Sicherheit zu quantifizieren. Daher können im 4D-Projekt statistische Kennzahlen und Testverfahren sowohl bei der Bewertung anhand der Dimension Sicherheit einen wertvollen Beitrag leisten, als auch darauf aufbauend bei der Bewertung anhand der Dimension Effizienz, bei der der quantifizierte Sicherheitsgewinn zu den Kosten ins Verhältnis gesetzt wird. Darüber hinaus kann ein statistisch erkennbarer Sicherheitsgewinn auch in die Bewertung einer Sicherheitsmaßnahme anhand der Dimension Vertrauen einfließen.

Die zu erwartende Verbesserung des Sicherheitsniveaus basiert auf der durch die Sicherheitsmaßnahme zusätzlich erzielte Sicherheit, d. h. den Sicherheitsgewinn. Das Ausmaß des Sicherheitsgewinns kann durch statistische Tests quantifiziert werden. Damit ein statistischer Test eine starke Aussagekraft hat, ist eine Voraussetzung, dass eine ausreichend große Anzahl an Beobachtungen vorliegt, damit der Test Aussagen mit hoher statistischer Sicherheit treffen kann. Daher haben statistische Analysen für z. B. die Qualität automatischer Gesichtserkennung durch einen Algorithmus anhand einer Datenbank mit 10.000 Gesichtern eine größere Aussagekraft als bei seltenen Ereignissen wie etwa Feuerkatastrophen in einem bestimmten Tunnel.

Im folgenden Absatz 3.1 werden kurz die Grundlagen statistischer Testverfahren wie z. B. Nullhypothese, Signifikanzniveau und Testergebnis vorgestellt, bevor daran anschließend statistische Testverfahren und Kennzahlen für ausgewählte Bereiche ziviler Sicherheit vorgestellt werden (Abschnitte 3.2 – 3.5).

3.1 Grundlagen statistischer Tests

Tests sind ein Eckpfeiler induktiver Statistik, da statistische Tests aufgestellte Hypothese temporär verifizieren oder endgültig falsifizieren. Beispiele für aufgestellte Hypothesen sind z.B. dass Zinsanstiege einen negativen Einfluss auf das BIP haben oder dass Kinder mit mehr

als acht Geschwistern ein um zehn Prozentpunkte unterdurchschnittliches Lebenseinkommen haben.

Ob eine aufgestellte Hypothese akzeptiert oder verworfen wird, hängt auch von dem gewählten Signifikanzniveau α ab, das in der Regel mit 1% oder 5% angenommen wird. Das Signifikanzniveau bestimmt, mit welcher Wahrscheinlichkeit die Nullhypothese höchstens fälschlicherweise abgelehnt werden soll. Übertragen auf das Beispiel einer Gerichtsverhandlung ist die Nullhypothese $H(0)$, dass der Angeklagte unschuldig ist (Unschuldsvermutung). Die Alternativhypothese wäre dementsprechend, dass der Angeklagte schuldig ist. In der Regel möchte der Staatsanwalt bzw. der Wissenschaftler die Nullhypothese verwerfen. Ziel ist es daher bei einem Gerichtsprozess zu vermeiden, dass eine unschuldige Person verurteilt wird (Fehler 1. Art).

Entscheidung	Wahrheitswert: $H(0)$ ist wahr	Wahrheitswert: $H(0)$ ist falsch
	$H(0)$ akzeptiert	richtige Entscheidung
$H(0)$ verworfen	falsche Entscheidung Fehler 1. Art Signifikanzniveau α $\alpha = P(\text{Fehler 1. Art})$	richtige Entscheidung „Power“ des Tests $= 1 - \beta$

3.2 Biometrische Testverfahren

Das erste hier aufgeführte Beispiel für die Anwendung statistischer Testverfahren in der zivilen Sicherheit sind Testverfahren, um die Qualität von biometrischen Anwendungen beurteilen zu können.

Ein biometrisches Erkennungsverfahren muss zwei Anforderungen erfüllen (Jain et al. 2016): Die Ähnlichkeit zwischen unterschiedlichen Beobachtungen eines biometrischen Merkmals einer gleichen Person muss sehr hoch sein („intra-subject similarity“) und die Ähnlichkeit zwischen unterschiedlichen Beobachtungen eines biometrischen Merkmals bei verschiedenen Personen muss sehr gering sein („inter-subject similarity“). Biometrische Verfahren arbeiten daher mit einer eindeutigen und unveränderbaren Beschreibung einer Person (Didier 2004).

Bei der Interpretation der Qualität von biometrischen Verfahren muss berücksichtigt werden, dass bei Anwendung für eine große Zahl von Nutzern, möglicherweise mehrere Millionen Personen, bereits kleine Fehlerraten zu erheblichen manuellen Nachbearbeitungen und entsprechenden Kosten führen können.

Biometrische Verfahren können für verschiedene Zwecke eingesetzt werden. Ein System zur Verifikation bestätigt die Identität einer Person. Das System überprüft, ob eine Person auch tatsächlich diejenige Person ist, die sie vorzugeben scheint. Die Überprüfung findet anhand des Abgleichs von in der Datenbank gespeicherten biometrischen Merkmalen dieser Person mit den ursprünglich erhobenen biometrischen Merkmalen statt. Dieser „1-zu-1“ Abgleich funktioniert relativ schnell und akkurat.

Ein System zur Identifikation stellt die Identität einer Person fest. Beim Versuch, die Identität einer Person herauszufinden, vergleicht das System die erhobenen biometrischen Merkmale der Person mit allen in der Datenbank gespeicherten biometrischen Merkmalen. Dieser „1-zu-n“ Abgleich ist im Vergleich zum „1-zu-1“ Abgleich langsamer und mit einer größeren Fehleranfälligkeit behaftet.

Ob das in Frage stehende biometrische Testverfahren prinzipiell geeignet ist, kann durch den „Failure to Enrol (FTE)“ festgestellt werden (Didier 2004). Der FTE gibt den Anteil der Population wieder, der nicht an dem biometrischen Testverfahren teilnehmen kann. So kann z.B. die Fingerabdruckerkennung bei händisch Arbeitenden problematisch sein.

Die „False Match Rate (FMR)“ bezeichnet den Anteil der Population, bei der fälschlicherweise eine Übereinstimmung angegeben wird (Didier 2004). Bei Zugangskontrollen bestimmt die FMR, wie viele unberechtigte Personen Zugang erhalten (falsche Akzeptanz). Bei einem Hausverbot bestimmt die FMR, wie vielen berechtigten Personen der Zugang fälschlicherweise verweigert wird (falsche Zurückweisung). Die Anteile für falsche Akzeptanz und falsche Zurückweisung sind korreliert. Sollen z.B. alle Betrüger erkannt werden, werden folglich mehr Personen irrtümlich abgewiesen.

Die „False Non-Match Rate (FNMR)“ gibt den Anteil der Population wieder, der fälschlicherweise bei einem Abgleich des biometrisches Merkmals mit der Beschreibung in der Datenbank als unterschiedlich klassifiziert wird (Didier 2004). Der Trade-Off zwischen FMR und

FNMR wird graphisch in Form der so genannten ROC-Kurve (ROC = Receiver-Operating Characteristic) dargestellt. Sie dient auch zur Identifikation der Equal Error Rate (EER), also jenes Punktes, in dem FNMR und FMR identisch sind (Jain und Ross 2008).

Nach Jain et al. (2016) beziehen sich FMR und FNMR auf die Fehlerraten in einem System zur Verifikation. Analog bestimmen „false positive identification rate (FPIR)“ und „false negative identification rate (FNIR)“ die entsprechenden Fehlerraten in einem System zur Identifikation.

Die Qualität der Fingerabdruckerkennung kann z.B. anhand der „true acceptance rate (TAR)“ und der „false acceptance rate (FAR)“ beurteilt werden. Jain et al. 2016 nennen für aktuelle Systeme zur Fingerabdruckerkennung z.B. eine TAR von 99,4%, bei einer FAR von 0,01%, wobei die FAR ähnlich dem Signifikanzniveau (α) bei einem statistischen Test interpretiert werden kann. Das „rank-1“ Kriterium liefert bei der Erkennung durch Fingerabdrücke den Anteil der gewonnenen Fingerabdrücke, zu denen ein System zur Identifikation mit der korrekten Identität aus der Datenbank bei dem 1-zu-n Abgleich die größte Übereinstimmung feststellt (Jain et al. 2016).

Generell ist bei der Bewertung von biometrischen Verfahren durch empirische Fehlerraten zu berücksichtigen, dass die ermittelten Fehlerraten von der analysierten Datenbank abhängen. Bei stark anwachsender Population oder sich verändernden Charakteristika in der Population kann die Fehlerrate möglicherweise ansteigen (Jain et al. 2016). Beurteilt man den erzielten Sicherheitsgewinn von biometrischen Verfahren, so ist wichtig, dass bei dem Vergleich von neuem mit altem Sicherheitsniveau die Referenzgröße für das alte Sicherheitsniveau auch tatsächlich aussagekräftig ist (Jain et al. 2016).

3.3 Bilderkennung

Ein weiteres mögliches Anwendungsfeld von statistischen Testverfahren im 4D-Projekt ist die softwaregestützte Bilderkennung. Das automatische Erkennen von Objekten, Personen und deren Tätigkeiten auf Bildern kann ebenfalls bei der Schaffung von Sicherheit eingesetzt werden. Obwohl das Beschreiben von Bildern am besten von Menschen übernommen wird (bei Vinyals et al. (2015) durch ein Amazon Mechanical Turk Experiment), kann diese Aufgabe auch von einem Algorithmus übernommen werden. Voraussetzung hierfür ist jedoch, dass auch eine von Menschen formulierte Beschreibung des Inhalts der Bilder aus der Da-

tenbank vorhanden ist. Nur dann kann ein statistisches Testverfahren die Qualität der Übereinstimmung der von einem Menschen formulierten Beschreibung mit der Beschreibung des Algorithmus vergleichen. Hierfür ist die am meisten in der Literatur verwendete statistische Kennzahl der „BLEU score“ (Bilingual Evaluation Understudy) (Vinyals et al. 2015). Der BLEU-score beurteilt die Qualität der Übereinstimmung der menschlichen Bildbeschreibung mit der Bildbeschreibung des Algorithmus.

3.4 Rettungsdienst

Im Rettungsdienst gibt es ebenfalls Kenngrößen um die tatsächliche Sicherheit bzw. einen erzielten Sicherheitsgewinn zu quantifizieren. Eine Messzahl für die Qualität des Rettungsdienstes ist die Reaktionszeit, d.h. die Zeit zwischen Absetzen des Notrufs bis zur Ankunft des Rettungsteams vor Ort (Jaldell et al. 2014). Eine weitere Kenngröße in diesem Zusammenhang ist die Zeitspanne vom Notruf bis zu dem Zeitpunkt, bis der Patient das Krankenhaus erreicht (operational time). Ebenso gibt die Anzahl der bearbeiteten Notrufe in einer bestimmten Periode Aufschluss über die Leistungsfähigkeit eines Rettungswesens. Um die Qualität des Rettungsdienstes zu beurteilen bzw. zu verbessern, können noch statistische Erhebungen über die Arte der Hilfe, z.B. Krankenwagen oder Notarzt, Ort des Unfalls bzw. Notrufs, Informationen über die Art des Unfalls oder das Ausmaß der Gefährdung für Gesundheit und Leben, angewendet werden. Weiter kann die Analyse verfeinert werden durch Berücksichtigung von Zeitintervallen, wie z.B. vom Notruf bis zum Einsatzbefehl, bis zum Ausrücken der Rettungsfahrzeuge, bis zur Ankunft beim Patienten, Abfahrt zum und Ankunft im Krankenhaus.

Um zusätzlich zu den oben genannten Kennzahlen im Rahmen der Bewertung anhand der Sicherheit auch die Effizienz einer Maßnahme im Rettungsdienst beurteilen zu können, sind Kennzahlen wie die Zeitspanne vom Krankenhaus bis zur Rückkehr des Einsatzfahrzeugs an seinen Standort, die gesamte Zeitdauer des Einsatzes und die zurückgelegten Kilometer – je nach Typ des Rettungsdienstes – aufschlussreich (Jaldell et al. 2014).

3.5 Verkehrssicherheit

Auch in der Verkehrssicherheit gibt es Kennzahlen, die eine Entscheidungshilfe für mögliche Sicherheitsinvestitionen sind, um Streckenabschnitte mit großer Unfallhäufigkeit oder besonders schweren Unfällen sicherer zu machen. Einzelne Kennzahlen können bei Bedarf im

Rahmen einer Sicherheitsstudie in ein Scoring Modell für Verkehrssicherheit integriert werden. Eine Messgröße für Verkehrssicherheit ist die erwartete Unfallhäufigkeit, gegeben den baulichen Voraussetzungen der Straße bzw. Kreuzung und dem Verkehrsaufkommen (Ohio Department of Transportation and Management 2014). Weiter kann das Verhältnis von Unfällen mit tödlichen und schweren Verletzungen im Vergleich zu allen Unfällen in die Analyse mit einbezogen werden.

Aufschluss über den Sicherheitsgewinn einer Sicherheitsmaßnahme gibt das Verhältnis von erwarteter Unfallhäufigkeit zu langfristiger Unfallhäufigkeit. Um die Effizienz einer Sicherheitsmaßnahme zu beurteilen, können die durchschnittlichen Kosten je Unfall herangezogen werden. Ebenfalls zur Beurteilung der Effizienz kann ein Index konstruiert werden, der die Summe aus dem Produkt von erwarteter Unfallhäufigkeit mit unterschiedlicher Schwere und einem entsprechendem Gewichtungsfaktor zu der gesamten erwarteten Unfallhäufigkeit ins Verhältnis setzt. Diese Kennzahl liefert Informationen über die langfristig erwartete Schwere der Unfälle an der Straße oder Kreuzung, die durch das Sicherheitsprojekt sicherer gemacht werden soll. Weitere Kenngrößen sind der Anteil von LKWs am gesamten Verkehrsaufkommen und das tatsächliche Verkehrsaufkommen im Verhältnis zu dem Verkehrsaufkommen, das für diesen Streckenabschnitt geplant war, als Maß für Verkehrsbehinderungen durch Stau.

Im Rahmen von Verkehrsprojekten wird zur Beurteilung der Effizienz auch das Verhältnis von Barwert des Nutzens des Sicherheitsgewinns und Barwert der Kosten des Projekts genannt (Ohio Department of Transportation and Management 2014). Um als übergeordnete Stelle, z.B. Bund oder Land, einen Eindruck von der Notwendigkeit der Sicherheitsmaßnahme zu bekommen, können auch die lokal übernommenen Kosten durch das Verhältnis von angefragtem Fördervolumen zu Gesamtkosten des Projekts in die Analyse mit einbezogen werden.

4. Bewertung von Sicherheitsmaßnahmen durch SERV-Dimensionen

Die vorangegangenen Abschnitte haben erläutert, wie ökonomische Bewertungsverfahren für Investitionsprojekte im Kontext ziviler Sicherheitsmaßnahmen eingesetzt werden können. Die allgemeine Grundlage von ökonomischen Bewertungsverfahren ist der Vergleich von erwarteten Kosten und Nutzen. Für die konkrete Analyse der Effizienz einer einzelnen

Sicherheitsmaßnahme können die ökonomischen Bewertungsverfahren entsprechend angepasst werden, um die Besonderheiten der Sicherheitsmaßnahme und deren Kosten und Nutzen zu berücksichtigen.

Im Rahmen des Forschungsprojekts 4D-Sicherheit erfolgt die Bewertung einer Sicherheitsmaßnahme nicht nur anhand von Sicherheitsgewinn und ökonomischer Effizienz, sondern umfassend anhand der vier Dimensionen Sicherheit, Effizienz, Recht und Vertrauen (SERV-Dimensionen). Hierbei steht die S-Dimension für die Verbesserung des Sicherheitsniveaus und die E-Dimension für ökonomische Effizienz. In dem ganzheitlichen Ansatz von 4D-Sicherheit spielt auch die R-Dimension, d. h. die Freiheit und die Rechte einer Person sowie die Rechtmäßigkeit der zu bewertenden Sicherheitslösung eine Rolle. Nicht zuletzt wird auch das „Vertrauen“ bzw. die Akzeptanz der Sicherheitslösungen seitens der Akteure einbezogen (V-Dimension). Die ökonomische Bewertung von Sicherheitslösungen soll im Rahmen des 4D-Projektes – unter Berücksichtigung der genannten SERV-Dimensionen – in generalisierender Weise die Vielfalt der heterogenen Anwendungsfelder ziviler Sicherheit berücksichtigen.

Literatur

- Brück, T. (2004): Assessing the Economic Trade-offs of the Security Economy. The Security Economy, OECD, 101–125.
- Didier, B. (2004): Biometrics. The Security Economy, OECD, 35–54.
- Entorf, H. (2015): Der Wert der Sicherheit: Anmerkungen zur Ökonomie der Sicherheit. Zöche, P., Kaufmann, S. und Arnold, H. (Ed.): Sichere Zeiten? Gesellschaftliche Dimensionen der Sicherheitsforschung. Lit Verlag, 375–391.
- European Commission (2014): Guide to Cost-Benefit Analysis of Investment Projects Economic Appraisal Tool for Cohesion Policy 2014-2020, Directorate-General for Regional and Urban policy.
- Jain, A. K. und A. Ross (2008): Introduction to Biometrics. In: Jain, AK, P. Flynn und A. Ross. Handbook of Biometrics. Springer, 1–22.
- Jain, A. K., Nandakumar, K., und Ross, A. (2016): 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, 79:80–105.
- Jaldell, H., Lebnak, P., und Amornpetsathaporn, A. (2014): Time Is Money, But How Much? The Monetary Value of Response Time for Thai Ambulance Emergency Services. Value in Health, 17:555–560.
- Ohio Department of Transportation (2014): Safety Study Guidelines. Working paper.
- UcedaVelez, T. (2008): What's the Return on Your Security Investment? The Journal of Corporate Accounting & Finance, July/August 2008, 19(5):61-67.
- Vinyals, O., Toshev, A., Bengio, S., und Erhan, D. (2015): Show and Tell: A Neural Image Caption Generator. arXiv:1411.4555v2.
- Weinstein, M. C., Torrance, G. und McGuire, A. (2009): QALYs: The Basics. Value in Health, 12: Supplement 1:5-9
- Whitehead, S. und Ali, S. (2010): Health outcomes in economic valuation: the QALY and utilities. British Medical Bulletin, 96:5–21.