Die dunkle Seite neuer Technologien – Projektbericht FESTOS

Roman Peperhove

Zusammenfassung

Das FESTOS-Projekt wurde im 7. Forschungsrahmenprogramm der EU-Sicherheitsforschung durchgeführt. Aufgabe des Projektes war eine Identifizierung zukünftiger Technologien, die von Terroristen oder Kriminellen missbraucht werden könnten. Der Schwerpunkt lag hierbei auf geringer Wahrscheinlichkeit, aber großen Auswirkungen (*Low Likelihood – High Impact*). Die Ergebnisse flossen in die Erstellung narrativer Szenarien, die zum einen eine Wirkungsanalyse darstellen und zum anderen geeignet sind, das Bewusstsein für einen Technologiemissbrauch zu erhöhen. Die Diskussion forschungsrelevanter und politischer Implikationen bildet den Abschluss des Artikels.

Abstract

The FESTOS project was conducted within the 7th Framework Programme of the EU "Security" strategy. Scope of the project had been the identification of future technologies which might have the potential to be misused by terrorists or criminals. Focus was laid on events with low likelihood but high impact. Based on the technology assessment, the project developed narrative scenarios for impact analysis and as a tool to raise awareness for technology misuse. Political and research relevance implications are discussed in the end of the article.

1 Einleitung

Zukünftige technische und soziale Entwicklungen zu bewerten stellt Wissenschaft und Forschung immer wieder vor große Herausforderungen. Je weiter die Vorausschau in die Zukunft verweist, desto schwieriger ist es, neue technische und soziale Entwicklungen, aber auch politische, natürliche und menschengemachte Einflüsse einzubeziehen.

Dennoch sind Zukunftsstudien, sowohl mit relativ kurzen als auch mit mittleren und großen Zeithorizonten von großer strategischer Wichtigkeit. Ziel ist es, sich frühzeitig mit unterschiedlichen Eventualitäten zu beschäftigen, bestehende Formen der politischen und wirtschaftlichen Realitäten zu prüfen und gegebenenfalls neue Instrumentarien zu entwickeln. Gerade im Bereich der Sicherheitsforschung ist in den vergangenen Jahren ein Schwerpunkt auf die Früherkennung von Gefahren gelegt worden. Die europäischen, aber auch deutschen Forschungsprogramme machen dies deutlich (Bundesministerium für Bildung und Forschung 2012; Europäische Kommission 2012). Ziel ist eine rechtzeitige, kritische Überprüfung relevanter nationaler und internationaler Sicherheitsstrukturen. Die Innovationsfähigkeit terroristischer Gruppen ist durch die Anschläge vom 11.09.2001, aber auch durch die versuchten Anschläge mit bisher undetektierbarem Plastiksprengstoff 2010[1] eindrucksvoll unter Beweis gestellt worden. Seither bemühen sich deutsche und europäische Sicherheitsinstitutionen sich auf neue, unbekannte Gefahren einzustellen.

[1] Geplant wurden die Anschläge höchstwahrscheinlich durch den al- Qaida-Ableger auf der arabischen Halbinsel (al-Qaeda in the Arabian Peninsula [AQAP]).

Es gilt zu beachten, dass die Affinität zu neuen Technologien bei Terroristen und Kriminellen differiert. Sind kriminelle Organisationen oftmals auf einem hohen technischen Stand,[2] ist bei terroristischen Gruppierungen der Drang zu technologischen Neuerungen sehr unterschiedlich ausgeprägt (vgl. Dolnik 2007; Cragin 2007). Auch wenn die meisten Anschläge in der Vergangenheit mit Lowtech durchgeführt wurden, gibt es doch auch einige Beispiele, in denen Hightech bereits zum Einsatz gekommen ist (z. B. bei den Saringas-Anschlägen der japanischen Gruppierung Ōmu Shinrikyō 1995 oder durch die Verwendung von Google Maps zur Planung und Durchführung der Anschläge in Mumbai 2008).

In diesem Kontext ist auch das Projekt FESTOS (Foresight of Evolving Security Threats Posed by Emerging Technologies) zu sehen.[3] Durchgeführt im 7. Forschungsrahmenprogramm der EU widmete sich das Projekt dem Ziel, mögliche zukünftige Technologien der kommenden 20 Jahre zu identifizieren und deren Missbrauchspotenzial durch Terroristen oder organisierte Kriminalität zu bestimmen.[4]

Im Folgenden wird ein Überblick über die Zielsetzungen, die angewandten Methoden und einige Ergebnisse des Projektes skizziert. Der Schwerpunkt wird hierbei sowohl auf der Technologievorausschau als auch der Entwicklung narrativer Szenarien liegen. Eine grundlegende Diskussion der im Projekt genutzten Termini und Theorieansätze kann in diesem Rahmen nicht erfolgen.

2 Neue Technologien – neue Gefahren?

Oftmals erleichtern neue Technologien das tägliche Leben und ermöglichen soziale, gesundheitliche und wirtschaftliche Impulse. Zugleich wird auch immer wieder vor mit ihnen verbundenen Risiken gewarnt. Während die freiwillige Nutzung neuer Technologien Risiken birgt, besteht zudem die Gefahr des absichtsvollen und gezielten Missbrauchs neuer, friedlicher und positiv intendierter Technologien durch Kriminelle und Terroristen. Was passiert, wenn neue Technologien durch Kriminelle oder Terroristen missbraucht werden? Welche Auswirkung hat die intendierte Zweckentfremdung einer Technologie in einer zukünftigen Gesellschaft? Was können neue Nanotechnologien in den Händen von Attentätern tatsächlich anrichten?

Solche Fragen umreißen die Ausgangssituation des FESTOS-Projektes. Die Zukunftsaussage, dass die Welt in 20 Jahren noch stärker durch Technologien geprägt sein wird als heute, bedarf keiner großen Fantasie. Auch ist anzunehmen, dass es zu einer neuen Qualität von Symbiosen zwischen neuen Technologien, Systemen und Lebenswirklichkeiten kommen wird. Der Missbrauch neuer Technologien in einer zukünftigen, hoch technologieorientierteren Gesellschaft erscheint vor diesem Hintergrund als eine unbehagliche Vorstellung. Die direkten und indirekten Auswirkungen des Missbrauchs neuer Technologien sind kaum abzuschätzen.

Die Besonderheit des FESTOS-Projektes liegt darin, nicht auf die wahrscheinlichsten Gefahren, die aus der Entwicklung neuer Technologien erwachsen, sondern auf Gefahren mit einer geringen Eintrittswahrscheinlichkeit, aber – im Falle eines Eintretens – großen Auswirkung (*Low Likelihood* –

[2] Vor allem im Bereich „Cybercrime“ wird dies sehr deutlich. Das BKA hebt im „Cybercrime. Bundeslagebild 2010“ die Anpassungs- und Innovationsfähigkeit der Täter in diesem Bereich hervor und betont die zunehmende internationale Zusammenarbeit der Kriminellen (vgl. BKA 2010).

[3] Das Konsortium des FESTOS-Projektes bestand aus den folgenden Partnern: Interdisciplinary Centre for Technology Analysis and Forecasting (ICTAF), Tel Aviv University, Israel; Finland Futures Research Centre (FFRC), University of Turku, Finnland
Zentrum Technik und Gesellschaft (ZTG), Technische Universität Berlin (TUB), Deutschland
Institute of Sociology (IS), University of Lodz (ULOD), Polen; EFP Consulting Ltd, Israel und Vereinigtes Königreich von Großbritannien und Nordirland

[4] www.festos.org

High Impact) zu fokussieren. Diese unwahrscheinlichen Ereignisse, auch als *Wild Cards* (vgl. Steinmüller & Steinmüller 2004) bezeichnet, werden in der üblichen Priorisierungspraxis in der Regel vernachlässigt. Ein Vorteil der Analyse von Wild Cards ist es, dass anhand neuer und oftmals kaum beachteter Bedrohungsereignisse neue Perspektiven sichtbar werden. Diese Art der Bewertung technologischer Gefahren ermöglicht eine neue und innovative Neubewertung existierender Reaktions- und Abwehrmaßnahmen.

Eine rechtzeitige Beschäftigung mit potenziellen zukünftigen Veränderungen, sei es im wirtschaftlichen, sozialen oder politischen Rahmen, ermöglicht die Chance, sich auf veränderte Bedingungen einzustellen und adäquat zu reagieren – im Falle von FESTOS auf den intendierten Missbrauch ziviler Technologien.[5]

Das Projekt verfolgte vornehmlich drei konkrete Zielsetzungen:

1. Identifikation zukünftiger Technologien und deren Missbrauchspotenziale
2. Entwicklung umfassender Szenarien und Indikatoren
3. Diskussion von Richtlinien und Maßnahmen zur Minimierung eines Missbrauchspotenzials

Nun ist es kaum möglich, alle Technologiefelder nach zukünftigen Technologien zu beforschen. Eine umfassende Technikvorausschau scheitert schnell an der Komplexität technologischer Entwicklungen. Um bessere Ergebnisse zu erzielen, wurde in FESTOS der Schwerpunkt bereits in der Konzeption auf sechs Technologiefelder gelegt. Es standen die Nanotechnologie, Biotechnologie, Informations- und Kommunikationstechnologie (IuK), Robotik, Neue Materialien und Konvergierende Technologien[6] im Zentrum des Interesses.

Wie sieht die technisierte Welt im Jahr 2030 aus? Welche Technologien werden durch die Menschen tagtäglich genutzt oder dienen in Industrie und Wirtschaft? Welche Interdependenzen zwischen Technologien sind denkbar? Welche sozio-politische Sprengkraft könnte ein Missbrauch entwickeln? Auf welche Weise lässt sich die Dimension eines Missbrauchs bemessen und wie kann diese anschaulich dargestellt werden?

Ebenso stellen sich Fragen bezüglich der Reaktion sowohl aufseiten der Forschung und Entwicklung als auch in der politischen Arena. Muss die Forschung auf mögliche Missbrauchspotenziale reagieren? Wie könnte eine solche Reaktion aussehen? Welche politischen Einwirkungen erscheinen sinnvoll und gewinnbringend, um das Missbrauchspotenzial neuer Technologien zu verringern?

2.1 Technologievorausschau

Üblicherweise wird bei einer Technologievorausschau eine Sichtung relevanter Technologien durchgeführt, die unterschiedliche Methoden beinhaltet. Im FESTOS-Projekt wurden umfangreiche Recherchen der einzelnen Partner durchgeführt, wozu qualitative Interviews mit führenden Wissenschaftlern und Experten der unterschiedlichen Technologiefelder gehörten. Anschließend wurden die Ergebnisse intern aufbereitet und einer Evaluierung im Rahmen einer internationalen und interdisziplinären Umfrage unterzogen. Zentrale Ziele waren hierbei die Einschätzung, wann die vorgestellten Technologien die Marktreife erreichen und wie groß das jeweilige Missbrauchspotenzial sein könnte.

[5] Es ist wichtig zu betonen, dass Technologien, die für militärische Anwendungen entwickelt werden, explizit vom FESTOS-Projekt ausgeschlossen wurden.
[6] Dieser Überbegriff bezeichnet in der Regel Querschnittstechnologien aus dem Bereich der Nanotechnologie, der Biotechnologie wie der Informationstechnologie und der Neurowissenschaften.

Thematisch war die Umfrage in zwei Blöcke unterteilt. Im ersten Frageblock wurden die einzelnen Technologien präsentiert und um eine Bewertung durch die Teilnehmer gebeten. Die 256 Teilnehmer der Umfrage stammten überwiegend aus Europa. Ihre fachliche Expertise verteilte sich relativ gleichbleibend über die sechs Technologiefelder, wobei die Experten aus dem Bereich IuK die größte Gruppe bildeten. Im zweiten Block wurden Fragen zur Bewertung und öffentlichen Diskussion technologischer Gefahren gestellt.

Die zur Diskussion gestellte Liste umfasste insgesamt 35 Technologien. Alle Teilnehmer waren aufgerufen, die Technologien ihrer Fachgebiete anhand von fünf Fragen zu bewerten:

1. When will this technology be sufficiently mature to be used in practice?
2. How easy will it be to use it for malicious purposes?[7]
3. How severe is the potential security threat posed by this technology?[8]
4. The likelihood that it will actually come to pose a security threat, in different time frames?[9]
5. To which societal spheres it will pose a security threat?[10]

Auf diese Weise wurde sowohl eine umfassende Analyse der vorgestellten Technologien hinsichtlich ihrer wahrscheinlichen Marktreife vorgenommen als auch eine detaillierte Gefahrenanalyse erreicht.

Die Dimensionen, die durch einen Missbrauch der vorgestellten Technologien betroffen sein könnten, wurden durch eine erweiterte STEEP-Analyse repräsentiert (Dimensionen: *Social Trends*, *Technology Trends*, *Economic Trends*, *Ecological Trends*, *Political Trends*). Da eine zunehmend technologisch ausgerichtete Gesellschaft auch mit ethisch-moralischen Fragen konfrontiert ist, legte das Projekt auf diesen Bereich ein besonderes Augenmerk. Die STEEP Analyse wurde daher um die Dimension *Value* (V) ergänzt.

Die Analyse der Ergebnisse geschah nach ausgewählten Gesichtspunkten. Eines der Kriterien war das Potenzial eines Missbrauchs der einzelnen Technologien. Hierfür wurden die Ergebnisse hinsichtlich der *Einfachheit eines Missbrauchs* mit dem *Grad der Auswirkungen* in Beziehung gesetzt: Welche Technologien sind besonders leicht zu manipulieren und haben zugleich im Falle eines Missbrauchs massive Auswirkungen?

Die Darstellung zeigt die Auswahl der Technologien und die Bewertung hinsichtlich der Intensität der Gefahr und der Einfachheit eines Missbrauchs durch die Teilnehmer der Studie.[11] Neben weiteren Analysen wurde ebenso nach der Wahrscheinlichkeit eines Missbrauchs gefragt. Tabelle 2 listet exemplarisch die Technologien mit der höchsten Missbrauchswahrscheinlichkeit für den Zeitraum 2026-2035 auf.

[7] Likert-Skala von 1 bis 5 (1 = *not easy at all*, 5 = *very easy*)
[8] Likert-Skala von 1 bis 5 (1 = *very low severity*, 5 = *very high severity)*
[9] Likert-Skala von 1 bis 5 (1 = *very unlikely*, 5 = *very likely*)
[10] STEEPV-Analyse
[11] y-Achse: Likert-Skala von 1 bis 5 (5 = *most severe*), x-Achse: Likert-Skala von 1 bis 5 (1 = *not easy at all*, 5 = *very easy*)

Tabelle 1 Easiness of malicious use vs. severity of threat[12]

Technology	A: How easy will it be to use this technology for malicious purposes that might pose security threats?	B: How severe is the potential security threat posed by this technology?	C: Multiplication of A and B: Potential of abuse
Smart mobile	3.69	3.49	12.88
Internet of things	3.61	3.49	12.60
Cloud computing	3.29	3.53	11.61
Gene transfer	3.52	3.22	11.33
Artificial intelligence	3.21	3.43	11.01
Synthetic biology	3.16	3.40	10.74
Cyborg insects	3.33	3.08	10.26
Energetic nanomaterials	3.00	3.33	9.99
RFID	3.14	3.03	9.51
Autonomous robots	3.36	2.83	9.51

Quelle: ICTAF, FESTOS-Projekt

Tabelle 2 Likelihood of posing a threat in different time intervals[13]

Technology	Now-2015	2016-2020	2021-2025	2026-2035	After 2035	Never	N
Energetic nanomaterials	2.2	2.91	3.3	3.9	3.78	1.17	11
Synthetic biology	1.91	2.59	3.14	3.64	4.15	2.13	22
Crystalline polymers	2.12	2.40	2.99	3.54	3.38	1.18	17
3-D printing	2.13	2.68	3.18	3.53	3.56	1.49	20
Internet of things	2.57	3.11	3.6	3.51	3.23	1.46	54
Artificial intelligence	2.07	2.56	3.13	3.43	3.71	1.71	46
Gene transfer	2.23	2.94	3.41	3.41	3.47	2.38	22
Future fuels	1.47	2.07	2.78	3.38	3.71	1.76	17
Metamaterials	1.21	1.99	2.56	3.33	3.82	1.39	19
Smart mobile	3.06	3.33	3.44	3.15	2.96	2.08	31

Quelle: ICTAF, FESTOS-Projekt

Die Einbeziehung der Wahrscheinlichkeit eines Missbrauchs – nach der Einschätzung der Teilnehmer der Umfrage – eröffnet eine wichtige neue Bewertungsebene. Technologien, deren Missbrauchswahrscheinlichkeit als unwahrscheinlich eingestuft wurde, deren mögliche Auswirkungen im Falle

[12] Auswahl derjenigen Technologien, die als einfach zu missbrauchen eingeschätzt wurden und deren Potential in Kombination mit der Schwere eines möglichen Missbrauchs daher als besonders hoch eingeschätzt wurden.
[13] Die Anzahl der abgegebenen Antworten N variiert, da die Technologien von Experten gemäß ihrer Expertise bewertet wurden.

eines solchen aber als hoch bewertet wurden, können daher durchaus als Wild Card beschrieben werden. In diesem Fall etwa ein Missbrauch von Metamaterials[14] oder auch Gene transfers[15].

Die Teilnehmer der Studie waren neben der Bewertung der einzelnen Technologien auch aufgerufen, ihre Bewertung hinsichtlich des öffentlichen Bewusstseins für Technologiemissbrauch abzugeben.

Zwei zentrale Fragen lauteten:

1. How well informed is the public about the potential dangers that might stem from new technologies?

69 % (155 von 226 Teilnehmern) der beteiligten Experten schätzten die Bevölkerung hinsichtlich potenzieller Gefahren durch neue Technologien als eher schlecht informiert ein. Nur 9 % hielten die Bevölkerung für eher gut informiert.

2. Are the estimated dangers that might be posed by new technologies overestimated or underestimated?

Um ein möglichst differenziertes Bild zu erhalten, wurde diese Frage dreigeteilt. Die Teilnehmer waren aufgefordert, eine Einschätzung hinsichtlich der Bewertung neuer Technologien abzugeben für 1) die Bevölkerung generell, 2) die Regierung und 3) ihre Kollegen aus Technik und Forschung.

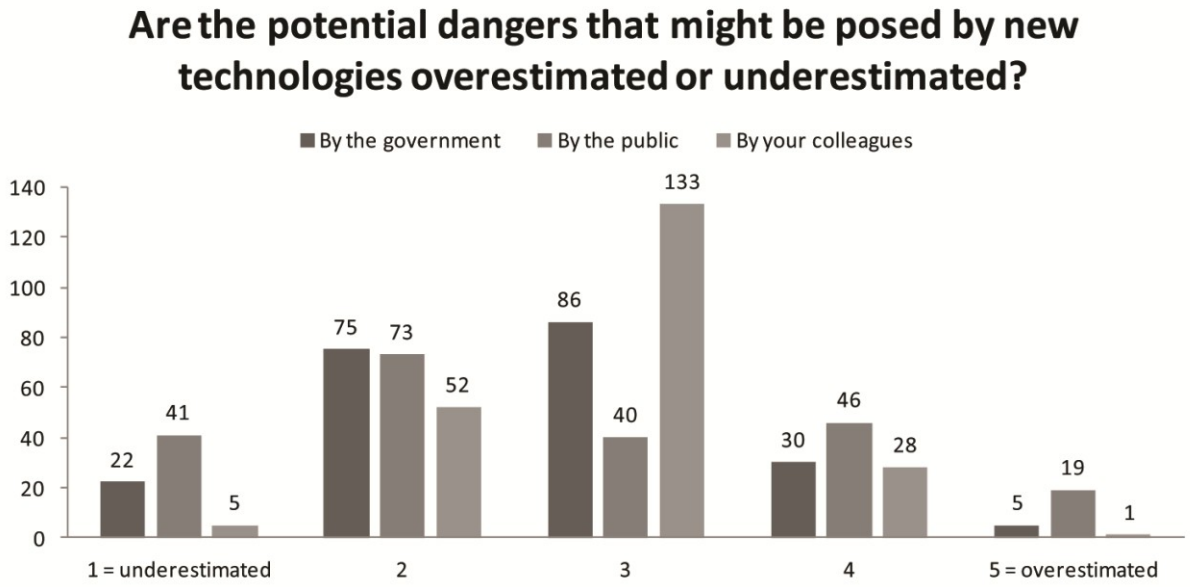

Abb. 1: Antworten der Teilnehmer in absoluten Zahlen (N ≈ 250)[16]*. Quelle: Eigene Darstellung*

Die Antworten der Teilnehmer der Umfrage zeigen vor allem zwei wichtige Erkenntnisse auf:

1. Die Bevölkerung ist sich laut Aussage der Teilnehmer der möglichen Gefahren nicht in einem angemessenen Umfang bewusst.

[14] Beschreibung im FESTOS-Survey: „Such specially engineered metamaterials could enable optical "cloaking", and creation of "super-lenses" with a spatial resolution below that of the wavelength. It has been shown that cloaking devices made out of metamaterials can hide objects from sight in certain wavelengths, or make them appear as other objects." (Interner FESTOS Projektbericht)

[15] Beschreibung im FESTOS-Survey: „New devices and methods are being developed for transferring genes from one living organism to another. Such devices could be increasingly available (and affordable) in the future." (Interner FESTOS Projektbericht)

[16] Nicht alle Teilnehmer haben die Frage beantwortet: *By the government* (N = 218), *By the public* (N = 219); *By the colleagues* (N = 219).

2. Hinsichtlich einer korrekten Einschätzung technologischer Gefahren vertrauten die Experten am wenigsten der Bevölkerung, mäßig den Regierungen und am meisten ihren Fachkollegen.

2.2 Szenarienentwicklung in FESTOS

Auf Basis der empirischen Ergebnisse wurden Szenarien entwickelt. Der FESTOS-Ansatz beinhaltete hierbei zwei Besonderheiten. Zum einen wurden explizit Szenarien mit geringen Eintrittswahrscheinlichkeiten und gleichzeitig großen Auswirkungen behandelt. Zum anderen wurden die FESTOS-Szenarien in Form von Kurzgeschichten narrativ dargestellt (Gaßner & Steinmüller 2006).

Mithilfe von Charakteren wird die Möglichkeit eröffnet, die Folgen und Auswirkungen technologischen Missbrauchs, beispielsweise durch Terroristen, aus der Perspektive betroffener Personen zu sehen. Da die Akteure in ihrer täglichen Umgebung agieren, besteht der Vorteil, dass viele Details in den Handlungsablauf integriert werden können, um auf diese Weise eine detaillierte Beschreibung zu ermöglichen.[17] Zudem bieten narrative Szenarien eine neue Zugangsweise zu möglichen zukünftigen Ereignissen:

> Stories are about meaning; they help explain *why* things could happen in a certain way. They give order and meaning to events – a crucial aspect of understanding future possibilities. (Schwartz 1996, S. 38)

Die Entwicklung der FESTOS-Szenarien basiert auf drei Teilschritten:

1. der Erarbeitung von Rahmenbedingungen zukünftiger Gesellschaften,
2. der Identifikation von möglichen, aber unwahrscheinlichen Gefahrenquellen und deren Auswirkungen im Falle eines Missbrauchs,
3. des Verfassens der narrativen Szenarien.

Die Grundlage für die FESTOS-Szenarien wurde während eines zweitägigen Szenarienworkshops im Sommer 2010 gelegt, an dem 35 Teilnehmer aus Forschung, Wissenschaft, Sicherheitsinstitutionen und der Verwaltung teilnahmen.

Als Rahmenbedingungen für die zukünftigen Gesellschaften wurden unterschiedliche Kenngrößen benutzt, um einerseits eine detaillierte Analyse zu forcieren und andererseits die Kreativität der Teilnehmer zu stimulieren. Zu diesen Kenngrößen gehörten u. a.: Größe des Landes, wirtschaftliche Situation, Zustand der Infrastruktur oder auch politisches System. Insgesamt wurden vier Hintergrundgesellschaften skizziert, analog zu den zu entwickelnden vier Szenarien.

Diese sogenannten *Security Climates* wurden erstellt, um der Tatsache Rechnung zu tragen, dass historische Erfahrungen, regionale Besonderheiten, Bevölkerungsstruktur und politische Zustände Einfluss auf die Wahrnehmung und die Bewertung von Gefahren nehmen (vgl. Jacobs & Worthley 1999; Douglas & Wildavsky 1983), wodurch auch die Reaktion einer Bevölkerung beeinflusst wird (vgl. Spilerman & Stecklov 2009).

Angestrebt wurde die Erarbeitung von vier Wild Cards, entsprechend der vier Szenarien. Jede Wild Card bildete den Ursprung eines Szenarios und wurde an eine zukünftige Gesellschaft gekoppelt. Auf diese Weise entstand eine Kombination von Wechselwirkungen zwischen der ausgewählten technologischen Bedrohung und den Besonderheiten der zukünftigen Gesellschaft.

[17] Eine Veröffentlichung der detaillierten Szenarienentwicklung inklusive der vollständigen Szenarien ist in Bearbeitung.

Basierend auf den Ergebnissen der Technologievorausschau wurden die folgenden Wild Cards entwickelt:

1. Schwärme von Cyber-Insekten attackieren Menschen und Tiere.
2. Individuelle DNA wird zur Erpressung missbraucht.
3. Intelligente, alltägliche, auf Nanotechnologie basierende Produkte können durch ein Funksignal zur Selbstauflösung gebracht werden.
4. Eine terroristische Gruppe benutzt einen Virus, um das Verhalten eines Teils der Bevölkerung für eine bestimmte Periode zu ändern.

Diese sehr unterschiedlichen technologischen Bedrohungen bildeten den Nukleus der Szenarien. In kleinen Gruppen erarbeiteten die Teilnehmer des Workshops mögliche Auswirkungen eines solchen technologischen Missbrauchs und diskutierten Kaskadeneffekte. Hierfür wurden in mehreren Sessions die Teilnehmer zu den unterschiedlichen Szenarien geleitet, an denen sie die Ergebnisse der Vorgängergruppe überprüfen, weiterentwickeln sowie neue Wechselwirkungen und Folgeeffekte identifizieren konnten.

Methodisch orientierte sich das Projektteam an der World-Café-Methode (Brown & Isaacs 2005). Diese partizipative und kreative Methode stimuliert eine spontane und dennoch strukturierte Aufnahme und Bewertung. Um die Komplexität einer gesamtgesellschaftlichen Bedrohung möglichst umfassend wiederzugeben und gleichzeitig dennoch eine stufenweise Bewertung zu ermöglichen, wurden zwei wichtige Ergänzungen vorgenommen. Zum einen sollten fünf gesellschaftliche Dimensionen als Anhaltspunkte für die Analyse dienen und zum anderen wurde zwischen drei Ebenen von Auswirkungen unterschieden. Die sechs Dimensionen lauteten in leichter Abwandlung zu denen der STEEPV-Analyse: *People/Society*, *Infrastructure*, *Political System*, *Economy*, *Environment* und *Value*. Die Ebenen der Auswirkungsanalyse wurden kreisförmig über die Dimensionen gelegt und galten: 1) den direkten und unmittelbaren Auswirkungen, 2) den indirekten Auswirkungen und 3) den Kaskadeneffekten. Als direkte Auswirkungen sind Tote oder Verletzte anzusehen, eine indirekte Auswirkung könnte ein Zusammenbruch von Kommunikationsmitteln sein und ein Kaskadeneffekt ein Rückgang von Investitionen im betroffenen Technologiefeld bzw. der betroffenen Region.

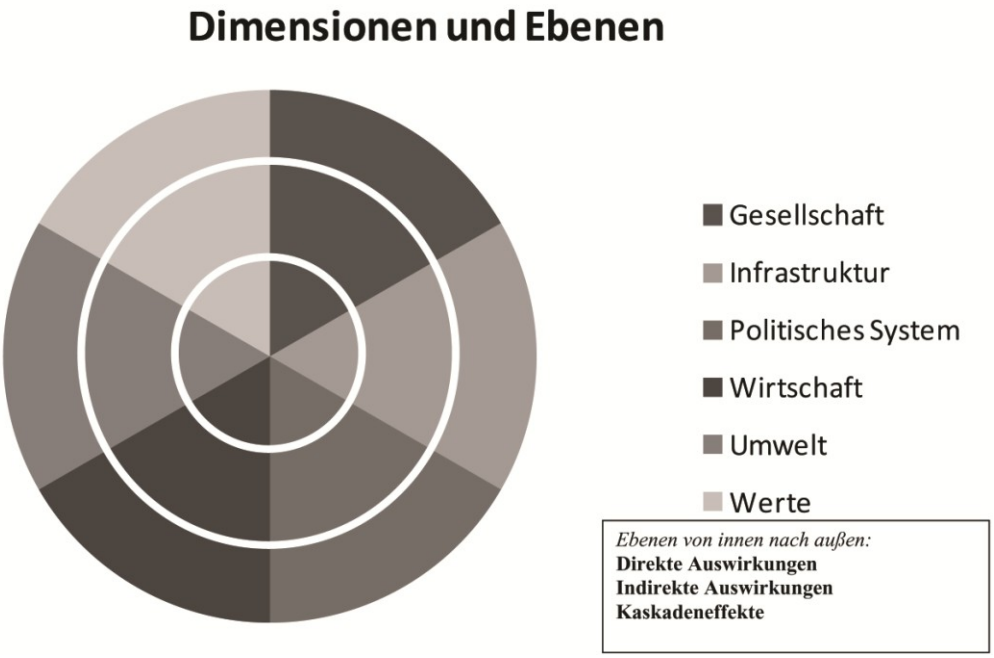

Abb.2: Dimensionen und Ebenen in der Wirkungsanalyse. Quelle: Eigene Darstellung

Abbildung 2 zeigt die unterschiedlichen Dimensionen im Zusammenspiel der Wirkungsebenen. Auf diese Weise wurde bereits während der Analyse die Möglichkeit eröffnet, sowohl die Breite als auch die Tiefe möglicher Auswirkungen intuitiv in die Analyse einzubeziehen.

In Geschichten umgesetzt wurden die Szenarien von Dr. Karlheinz Steinmüller[18]. Basierend auf den Ergebnissen des ersten Tages präsentierte Steinmüller den Teilnehmern bereits am zweiten Tag grobe Szenarienskizzen. Auf diese Weise konnten schon die Eckpunkte der narrativen Szenarien vor Ort diskutiert werden. Zudem wurden die Entwürfe um weitere Aspekte der jeweiligen Bedrohungen erweitert.

Die aufbereiteten Daten der Workshop-Sessions lieferten die Rahmenbedingungen für die Szenarien. Steinmüller erarbeitete detaillierte Entwürfe, die anschließend durch Reviews und Feedbacks erweitert wurden. Hierzu dienten vor allem eine interaktive Online-Befragung, Workshops und teaminterne Diskussionen. Anschließend wurden die Szenarien finalisiert.

Wie kann man sich nun die FESTOS-Szenarien vorstellen und welchen Nutzen kann man aus ihnen ziehen? Die Szenarien umfassen jeweils etwa vier bis fünf Seiten und beschreiben die Auswirkungen in der täglichen Umgebung der handelnden Personen aus deren Perspektive.

Um einen Eindruck über die Art der Szenarien zu geben, hier nun ein kurzer Auszug aus dem Szenario „Cyber-Insects attack!“:

> “Mommy, Daddy, the synsects stung me!” Julie ran into the house in a fluster. Martin, who just sat down to deal with the administrative stuff for his organic farm, looked over at his eleven-year-old daughter. On her face and all over her arms were red marks that looked like mosquito bites. “What happened?” Julie had just been inspecting the rabbit hutches. Apparently, a swarm of these synsects had flown at her and attacked her [...] Years ago, the bee populations had collapsed. A strange, almost unaccountable disease had devastated them. [...]
>
> They were powered by solar energy, navigated with a micro-GPS and, in good weather, could reach almost half as many flowers as a bee. The current, third-generation synsects were smaller, faster and more versatile, they even communicated with each other. [...]
>
> By the afternoon, the marauding synsects had taken over the number one spot in the national news. Apparently, the bees had nearly blanketed some regions. Martin turned on the TV while he searched the Internet. “Synsects inciting stampedes.“ “Do cyberbees carry diseases?” “Farmer loses control of his tractor.” “Minister of Agriculture fears crop shortages.” Also, a swarm had already been spotted in a city. There were various warnings being issued not to go outdoors unless it was absolutely necessary. [...]
>
> A few days later, Martin went out to inspect his land, protected by a kind of hand-made beekeeper’s mask. The effects of the synsect plague were everywhere. Whoever could was staying inside. In the cities, entrances to the underground trains were being covered with fine-mesh metallic screens, street cafés were closed, open-air events and football games were cancelled. Air travel was suspended in large portions of Central Europe for safety reasons. Several sources reported that the Assassins, a fundamentalist bioterrorist group, were being arrested. There was a lot of false information going around, however. [...]
>
> Carlson, a man in his mid-thirties, seemed overworked. “You’re really lucky here,” he said. “The synnis don’t like damp areas. In other places, people have made huge plots, entire square kilometers, into no-go zones. A swarm attacks every couple of minutes in those places. The birds have all left already and the army is trying to set up wireless signal blocks all around the area.”

[18] Karlheinz Steinmüller ist Wissenschaftlicher Direktor der Z_punkt GmbH und Partner im FESTOS-Projekt.

Das Szenario erscheint auf den ersten Blick als unterhaltsame Kurzgeschichte, doch bei näherer Betrachtung eröffnet es eine ganze Palette politischer, sozialer und wirtschaftlicher Aspekte, die im Falle eines Technologiemissbrauchs tangiert wären.

Intuitiv fallen den meisten Rezipienten weitere potenzielle Auswirkungen und Wirkungsweisen ein, die sich aus den unterschiedlichen Ebenen und Dimensionen ergeben. Gerade dieser Effekt war in FESTOS aus zwei Gründen intendiert: 1) Durch die interaktive Feedback-Schleife wurden die Szenarien strategisch überprüft und erweitert. 2) Die Identifikation mit den Akteuren bewirkt bei den Rezipienten den Impuls, eigene, individuelle und institutionelle Arbeitsweisen mit den Beispielen abzugleichen und auf diese Weise über den Zusammenhang zwischen Sicherheit und neuen Technologien zu reflektieren.

Es ist zu beachten, dass die im Projekt erarbeiteten Szenarien nur beispielhaft mögliche Auswirkungen eines Technologiemissbrauchs darstellen – natürlich sind auch andere Szenarien denkbar und möglich.

2.3 Indikatoren

In FESTOS dienten die Szenarien neben der Bewertung und Darstellung von möglichen Auswirkungen eines Missbrauchs einem weiteren Zweck. Die Szenarien wurden als ein wichtiger Ansatz genutzt, um Indikatoren zu identifizieren, die möglicherweise geeignet sind, bereits frühzeitig ein erhöhtes Missbrauchspotenzial zu detektieren.

Die Herausforderung bestand vor allem in der Entwicklung umfassender Indikatoren, die die Bandbreite möglicher Einflussfaktoren widerspiegeln und dennoch handhabbar sind.

Zu diesem Zweck hat das FESTOS-Team drei Indikatorencluster konstruiert, um unterschiedliche Bereiche einzubinden: 1) *Technology*, 2) *Background* und 3) *Perpetrator*.

An einigen Beispielen soll der Hintergrund für die Auswahl beschrieben werden.

Der Cluster *Technology* umfasst Aspekte, die direkt mit der Technologie verbunden sind. Hierzu gehören die *Entwicklung einzelner Komponenten* als Voraussetzung für eine Marktreife ebenso wie *(nicht) implementierte Sicherheitsmerkmale*. Die Entwicklung einzelner technologischer Komponenten muss nicht zwangsläufig eine bestimmte Technologie hervorbringen, macht es allerdings wesentlich wahrscheinlicher. Die Implementierung von Sicherheitsmerkmalen in eine Technologie dagegen hat direkten Einfluss auf einen Missbrauch. Je ausgefeilter die Schutzvorrichtung ist, desto schwieriger wird ein Missbrauch.

Der zweite Cluster, *Background*, beinhaltet vor allem sozio-kulturelle und ökonomische Indikatoren, etwa einen *sinkenden Preis* für ein Produkt, da dies in der Regel die Verbreitung und somit auch die Anfälligkeit steigert, oder auch eine *steigende Akzeptanz* für eine Technologie in der Bevölkerung, die eine Durchsetzung am Markt wahrscheinlicher macht. Ein sinkender Preis ist in der Regel ein deutliches Anzeichen für eine steigende Verbreitung neuer Technologien, da hierdurch breite Bevölkerungsschichten, Organisationen und Unternehmen Nutzer werden können. Es ist anzunehmen, dass die Auswirkungen im Falle eines Missbrauchs dementsprechend größer sind, je weiter eine Technologie verbreitet ist – wodurch ein Missbrauch für Täter wiederum attraktiver wird. Ähnlich verhält es sich mit einer steigenden Akzeptanz. Eine weite und arglose Nutzung durch eine hohe Akzeptanz neuer Technologien kann zu einer höheren Vulnerabilität führen, da die Sensibilität für mögliche Risiken nachlassen könnte.

Der dritte Cluster, *Perpetrator*, umfasst neben den technischen und den sozio-kulturellen Voraussetzungen eine weitere wichtige Vorbedingung: das Vorhandensein von potenziellen Tätern. Es

gibt unzählige Technologien, aber nur wenige von ihnen werden intendiert von Terroristen oder Kriminellen missbraucht. Daher tauchen in diesem Cluster Indikatoren wie etwa *passende ideologische Ausrichtung* oder auch *ausreichende Ressourcen* auf. Basierend auf dem offensichtlichen Zusammenhang zwischen der Wahl einer Technologie und der Ausrichtung eines Täters oder einer Gruppierung bedarf es eines Abgleichs zwischen einer möglichen Technologie und dem oder den möglichen Täter(n).[19] Ausreichende Ressourcen werden vor allem dann zu einem wichtigen Indikator, wenn eine bestimmte Technologie sehr aufwendig zu produzieren oder sehr kostenintensiv ist. Die Entwicklung und Herstellung des Saringases durch die japanische Endzeitsekte Ōmu Shinrikyō hat die Gruppierung nach Schätzungen etwa 30 Millionen US-Dollar gekostet – eine Investition, die sich nur die wenigsten potenziellen Attentäter würden leisten können (vgl. Dolnik 2007, S. 76).

Durch eine Kombination dieser Indikatoren und deren zukünftiger Erweiterung und Evaluation durch Praxis und Forschung könnte den zuständigen Behörden die Chance eröffnet werden, die steigende Wahrscheinlichkeit eines potenziellen Missbrauchs frühzeitig zu erkennen und mögliche Gegenmaßnahmen zu entwickeln. Hierbei ist zu beachten, dass keineswegs alle Indikatoren gleichzeitig zutreffen müssen. Eine Zunahme von übereinstimmenden Indikatoren kann jedoch eine steigende Missbrauchsgefahr signalisieren.

Basierend auf diesen Annahmen und den Szenarien ist festzuhalten, dass die Wahrscheinlichkeit eines Missbrauchs zukünftiger Technologien maßgeblich durch drei Faktoren beeinflusst wird:

1. Die Verfügbarkeit und die Nützlichkeit einer Technologie für einen Täter
2. Die Auswirkungen durch einen Missbrauch der Technologie
3. Die Vulnerabilität des Zielsystems (z. B. Gesellschaft, Institution, Infrastruktur)

3 Gefahrenminimierung

Die Einschätzung der Technologie- und Sicherheitsexperten hat gezeigt, dass es zukünftige Technologien mit einem deutlichen Missbrauchspotenzial geben könnte. Die Komplexität der Auswirkungen eines solchen Missbrauchs wurde durch die Szenarien detailliert beschrieben. Nun stellte sich die Frage, wie Forschung und Entwicklung, aber auch die Politik mit diesen Erkenntnissen umgehen. Ebenso wurde der Frage nachgegangen, ob bzw. wie Forscher und Entwickler auf einen möglichen Missbrauch ihrer Technologien reagieren könnten. Daher untersuchte das FESTOS-Projekt die Bereitschaft in Forschung und Entwicklung, Maßnahmen in Betracht zu ziehen, die möglicherweise geeignet sind, einen Missbrauch von Technologien oder relevanten Informationen zu verringern.

In einer internationalen Umfrage wurden aktuelle Regelungen und die Einstellung gegenüber neuen Praktiken zur Gefahrenminimierung ermittelt. Insgesamt nahmen 192 Teilnehmer teil, von denen 92 % aus europäischen Ländern und Israel stammten.

[19] Gewaltbereite Umweltaktivisten werden beispielsweise den Einsatz von Technologien, die sich (nachhaltig) negativ auf die Umwelt auswirken, vermutlich ablehnen.

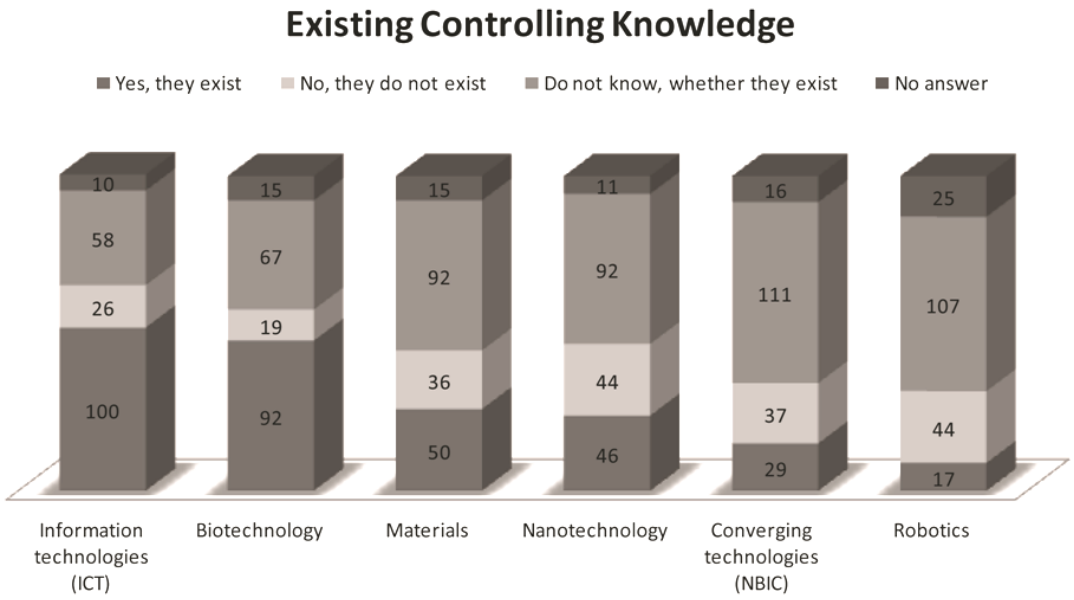

Abb. 3: Kenntnis über existierende Kontrollmechanismen in absoluten Zahlen (N ≈ 192)[20]*. Quelle: ULOD, FESTOS-Projekt*

Es stellte sich heraus, dass ein Großteil der befragten Forscher und Entwickler nur bedingt wusste, ob bereits Kontrollmechanismen in ihren Institutionen implementiert sind (Abbildung 3). Aus dem Bereich der Robotik gaben 68,4 % der Befragten an, dass sie nicht wüssten, ob es Richtlinien gebe, weitere 22,8 % glaubten, dass solche Regelungen nicht existierten. Lediglich 8,8 % waren sicher, dass es Regelungen gebe.

Im Gegensatz hierzu gaben 51,8 % der befragten Forscher und Entwickler aus dem Bereich IuK an, dass sie von solchen Regelungen Kenntnis hätten. 34,7 % wussten nicht, ob Regelungen existierten und weitere 13,5 % waren sich sicher, dass es keine Regelungen gebe.

Diese beiden Teilergebnisse deuten bereits an, wie unterschiedlich die Kenntnisse über bereits existierende Regelungen sind. Nun ist nicht eindeutig zu bestimmen, ob Forscher und Entwickler aus dem Bereich IuK sich existierender Regelungen am ehesten bewusst sind oder ob in diesem Bereich tatsächlich öfter Reglungen existieren. Es scheint jedoch Realität zu sein, dass bei den Experten und/oder den jeweiligen Institutionen lediglich ein relativ geringes Gefahrenbewusstsein besteht – zumindest hinsichtlich der existierenden Regelungen. Daher ist es von großem Interesse, zu erforschen, ob Forscher und Entwickler überhaupt bereit sind, sich auf Kontrollmechanismen hinsichtlich potenziell sensiblen Wissens einzulassen, und wie diese Regelungen aussehen könnten.

Regeln im Kontext von Wissenschaft und Forschung steht schnell im Verdacht der Zensur. Dieses Spannungsfeld zwischen der Reglementierung von Wissen und dessen Kontrolle wurde im FESTOS-Projekt mit dem Terminus *Knowledge Control Dilemma* beschrieben.

In demokratischen und offenen Gesellschaften ist es gute wissenschaftliche Praxis, sich offen über Forschungen auszutauschen. Forschung ist ein hohes Gut der Wissenschaft und darf nur in besonderen Fällen zur Disposition stehen. Die Weitergabe von sicherheitsrelevantem Wissen mag in Ausnahmen jedoch ein solch besonderer Fall sein. Bereits heute sind einige Forschungsergebnisse für

[20] Hier fehlende Antworten: ICT – 10 (N = 183), Biotechnology – 15 (N = 178), Materials – 15 (N = 178), Nanotechnology – 11 (N = 182), NBIC – 16 (N = 177), Robotics – 25 (N = 169)

die Öffentlichkeit nicht zugänglich, etwa in der Nuklearforschung.[21] In anderen Fällen führt die Publizierung sensibler Forschungsergebnisse zu hitzigen Diskussion in der Forschungsgemeinde und der Öffentlichkeit, wie das aktuelle Beispiel der H5N1-Mutationsstudien aus den Niederlanden und den USA gezeigt hat (vgl. Nordqvist 2012). Die Regulierung von potenziell missbräuchlich zu nutzenden Informationen ist de facto bereits Bestandteil von Wissenschaft und Politik.

In der FESTOS-Umfrage sprachen sich mit 56,6 % die meisten Teilnehmer der Umfrage deutlich gegen eine Kontrolle der Publikation von Forschungsergebnissen aus (*strongly disagree* und *rather disagree*). Lediglich 26,9 % sahen eine solche Maßnahme als akzeptabel an (*rather accept* und *strongly accept*). Eine deutliche Skepsis zeigte sich auch gegenüber anderen Kontrollmechanismen. 40,9 % lehnten eine Überprüfung von Forschungsanträgen hinsichtlich sensibler Informationen ebenso ab wie 32,1 % eine Kontrolle während der industriellen Anwendungsphase.

Hierbei wird bereits eine Tendenz sichtbar, die durch weitere Ergebnisse der Umfrage bestätigt wurde: Die Teilnehmer favorisierten eher Bottom-up- als Top-down-Methoden. Zu den erfolgversprechendsten Ansätzen zählten:

1. (Aus-)Bildungscurricula einschließlich Programmen, die auf eine Stärkung des Bewusstseins für mögliche Gefahren abzielen,
2. Maßnahmen, die von den jeweiligen Forschern und Entwicklern selbst eingeführt werden,
3. Maßnahmen, die in Zusammenarbeit mit Medien entwickelt werden und die Publikation potenziell sensibler Informationen behandeln.

Diese Aussagen deuten an, dass Forscher und Entwickler einer externen Evaluation ihrer Arbeit und der hierbei entstehenden Informationen kritisch gegenüber stehen. Diese Skepsis könnte durchaus berechtigt sein, da die Komplexität technologischer Forschung bisweilen nur einem kleinen Expertenkreis zugänglich ist. Eine geforderte, angemessene Einzelfallprüfung erscheint vor diesem Hintergrund nur durch die jeweiligen Fachkollegen möglich zu sein. Gleichzeitig ist das Bewusstsein für einen möglichen Missbrauch zukünftiger Technologien unter Forschern und Entwicklern bisher nur rudimentär vorhanden, wie die FESTOS-Ergebnisse gezeigt haben. Daher ist der notwendige erste Schritt eine Stärkung des Bewusstseins für einen Technologiemissbrauch durch Kriminelle und Terroristen, um Forscher und Entwickler für diese Thematik zu sensibilisieren. Eine Bereitschaft hierzu wurde sowohl durch Rückmeldungen zur Umfrage als auch in den Einzelinterviews deutlich.

Sind Entwickler und Forscher sensibilisiert für eine Zweckentfremdung ihrer positiv intendierten Technologien, so können schon während des Entwicklungs- und Produktionsprozesses Sicherheitsmaßnahmen implementiert werden. Das Konzept heißt hier: *Security by design*[22].

Deutlich wurde bei allen Gesprächen und der Auswertung der Umfrage, dass eine internationale Zusammenarbeit bei der Bewertung von Informationen und Wissen vonnöten ist. Die Komplexität und Bandbreite technologischer Forschung erfordern gemeinsame internationale Anstrengungen bei der Bewertung zukünftiger Technologien hinsichtlich aus ihnen hervorgehender neuer Bedrohungslagen. FESTOS stellt hierfür einen ersten Schritt dar.

[21] In Projekten, die unter Beteiligung von Wirtschaftsunternehmen durchgeführt werden, ist eine Vielzahl von Ergebnissen nicht öffentlich. Dies ist in der Regel allerdings eher der Gewinnung von Wettbewerbsvorteilen geschuldet als sicherheitsrelevanten Überlegungen. Dennoch ist es eine Regulierung von Wissen und Informationen.

[22] Ursprünglich entwickelt in der Informatik, bezeichnet „Security by design“ das Konzept, Sicherheitsmechanismen bereits während der Planung und Entwicklungsphase in neue Technologien und Produkte zu implementieren.

Jedoch stehen alle Anstrengungen vor einem Zwiespalt: die Freiheit der Forschung zu schützen und gleichzeitig das Potenzial für einen Missbrauch neuer Technologien zu minimieren. Es wurde deutlich, dass sich die große Mehrheit der befragten Forscher und Entwickler gegen externe Kontrollmechanismen ausspricht. Lediglich interne Regularien und Codes of Conduct wurden von den Teilnehmern als akzeptabel angesehen. Eine ethische und rechtliche Überprüfung einer möglichen Kontrolle erscheint zudem essenziell.

Die entwickelten narrativen Szenarien des Projektes sind für einen Bewusstseinswandel ein probates Mittel. Sie zeigen nicht nur sehr detailliert die sozialen, politischen und wirtschaftlichen Auswirkungen technologischer Gefahren auf, sondern initiieren auch ein intuitives Nachdenken über Strategien zu Gefahrenminimierung.

4 Zusammenfassung und Ausblick

Eine perspektivische Bewertung zukünftiger Technologien durchzuführen, ist eine komplexe Aufgabe und bedarf der Zusammenarbeit von nationalen und internationalen Experten. Das FESTOS-Projekt hat aufgezeigt, dass es Strategien und Ansätze gibt, die eine Bewertung ermöglichen.

Eine zentrale Einsicht aus dem Projekt ist, dass die Möglichkeit eines gezielten Missbrauchs zukünftiger Technologien bisher kaum reflektiert wird – weder aufseiten von Forschung und Entwicklung noch auf politischer und administrativer Ebene. Die im Projekt entwickelten Szenarien sind konstruiert, um die Folgen eines möglichen Missbrauchs zu kontextualisieren. Es erscheint ratsam, bereits frühzeitig technologische Gefahren zu kommunizieren und zu reagieren.

Das Konzept „Security by design" ist ein vielversprechender Ansatz. Allerdings bedarf es nicht nur im technischen Bereich weiterer Forschung. Vor allem erscheint es wichtig, das Verhältnis zwischen Technik und Gesellschaft vor einem sicherheitspolitischen Hintergrund weiter zu diskutieren. Die FESTOS-Szenarien sind explizit als dunkle Szenarien konstruiert. Neue Technologien ermöglichen in der Regel eine Erleichterung und Verbesserung des individuellen und gesellschaftlichen Lebens. Dennoch wird die Frage, wie Gesellschaften und ihre Infrastruktur in einer zunehmend technologisierten Welt vor technologischen Sicherheitsrisiken geschützt werden können, eine zunehmende Bedeutung erhalten. Kommende technologische Gefahren offen zu kommunizieren, ohne sie zu dramatisieren, ist Aufgabe von Politik und Wissenschaft. Hierbei erscheint es notwendig, sich zukünftig vor allem auch den gesellschaftlichen Dimensionen von Technik und Sicherheit zu widmen.

Um jedoch nicht von neuen Technologien und deren möglichem Missbrauch überrascht zu werden, erscheinen technologisch-soziale Gefahrenabschätzungen als ein vielversprechender Weg.

Literaturverzeichnis

Bundesministerium für Bildung und Forschung (2012). *Forschung für die zivile Sicherheit 2012–2017. Rahmenprogramm der Bundesregierung*. Verfügbar unter: http://www.bmbf.de/pub/rahmenprogramm_sicherheitsforschung_2012.pdf [12. September 2012]

Bundeskriminalamt (2010). *Cybercrime. Bundeslagebild 2010*. Verfügbar unter: www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf [28. August 2012]

Brown, J. & Isaacs, D. (2005). *The World Café: Shaping our futures through conversations that matter*. San Francisco: Berrett-Koehler.

Cragin, K. (2007). *Sharing the dragon's teeth: terrorist groups and the exchange of new technologies*. Santa Monica: Rand Corp.

Dolnik, A. (2007). *Understanding terrorist innovation: Technology, tactics and global trends*. Abingdon: Psychology Press.

Douglas, M. & Wildavsky, A. (1983). *Risk and culture: An essay on the selection of technical and environmental dangers*. Berkeley: University of California Press.

Europäische Kommission (2012). Work *Programme 2013. Cooperation. Theme 10. Security*. Verfügbar unter: http://ec.europa.eu/research/participants/portalplus/static/docs/calls/fp7/common/32768-annex_13_to_the_decision_security_for_cap_en.pdf [12.09.2012]

Gaßner, R. & Steinmüller, K. (2006). Narrative normative Szenarien in der Praxis. In F. E. P. Wilms (Hrsg.). *Szenariotechnik: Vom Umgang mit der Zukunft* (S. 133–144). Bern: Haupt Verlag.

Jacobs, L. & Worthley, R. (1999). A comparative study of risk appraisal: A new look at risk assessment in different countries. *Environmental monitoring and assessment*, 59 (2), 225–247.

Nordqvist, C. (2012). Mutated H5N1 Virus Research To Remain Under Wraps For Now, Says WHO. *Medical News Today*. Verfügbar unter: http://www.medicalnewstoday.com/articles/241872.php [22.06.2012]

Schwartz, P. (1996). *The art of the long view: paths to strategic insight for yourself and your company*. New York: Crown Business.

Spilerman, S. & Stecklov, G. (2009). Societal Responses to Terrorist Attacks. *Annual Review of Sociology*, 35, 167–189.

Steinmüller, A. & Steinmüller, K. (2004). *Wild Cards: Wenn das Unwahrscheinliche eintritt*. Hamburg: Murmann Verlag.

Roman Peperhove: Studium der Neueren Geschichte und Islamwissenschaft. Er arbeitet vorwiegend zu Sicherheitsthemen wie Terrorismus, (De-)Radikalisierung und Extremismus. Hierbei interessiert er sich vor allem für Wechselwirkungen zwischen Sicherheit und Gesellschaft. Er ist unter anderem Mitglied des „European Expert Network on Terrorism Issues – EENeT" und der „Deutschen Arbeitsgemeinschaft Vorderer Orient für gegenwartsbezogene Forschung und Dokumentation e. V. – DAVO"

Nexus Institut für Kooperationsmanagement und interdisziplinäre Forschung, Otto-Suhr-Allee 59, 10585 Berlin, Tel.: +49 (0) 30-31805485, E-Mail: peperhove@nexusinstitut.de, www.nexusinstitut.de

Lizenz

Empfohlene Zitierweise

Peperhove R (2012). Die dunkle Seite neuer Technologien – Projektbericht FESTOS. Zeitschrift für Zukunftsforschung, Vol. 1. (urn:nbn:de:0009-32-34144)

Bitte geben Sie beim Zitieren dieses Artikels die exakte URL und das Datum Ihres letzten Besuchs bei dieser Online-Adresse an.