TRANSFORMING CITIES

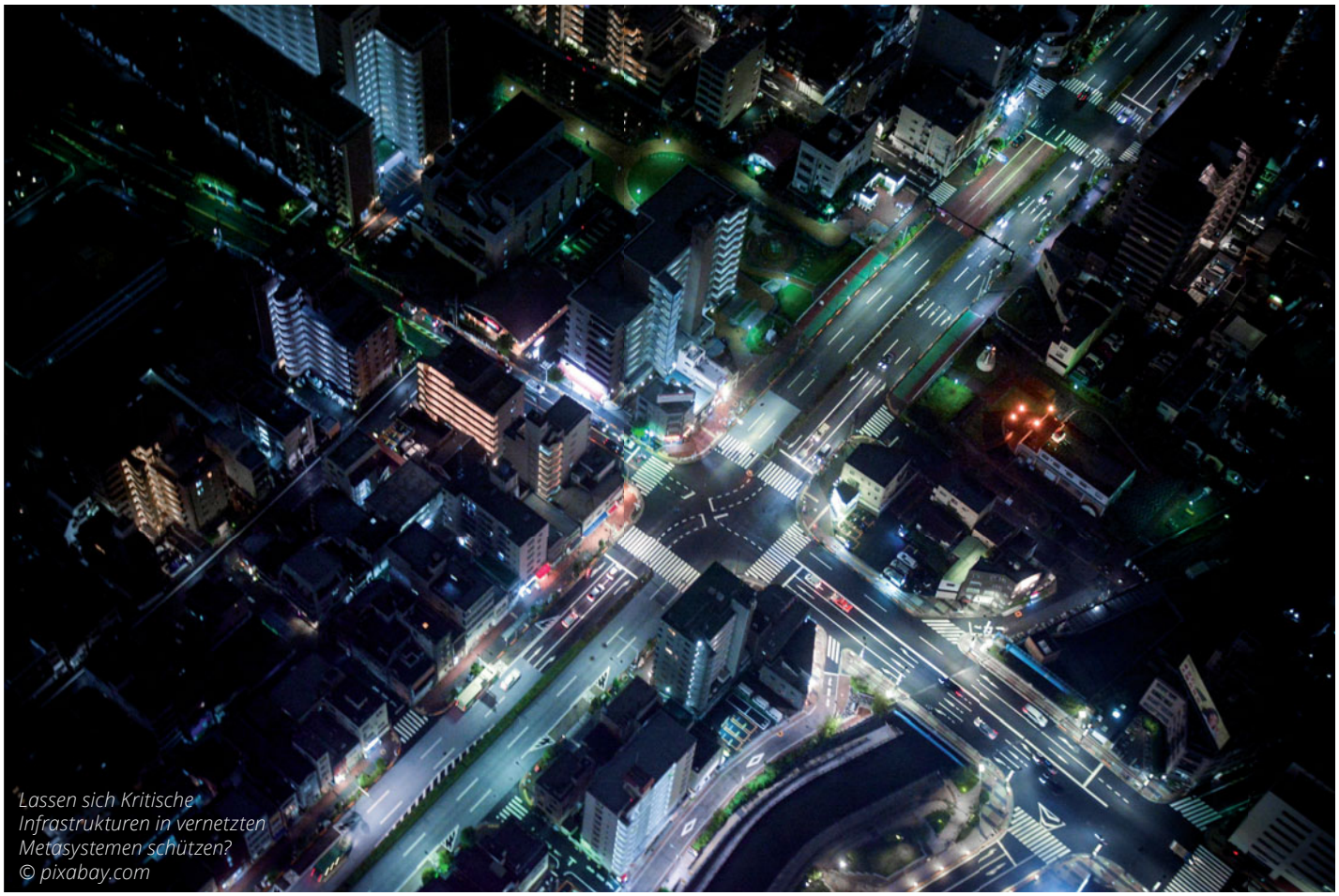
1 · 2016

URBANE SYSTEME IM WANDEL. DAS TECHNISCH-WISSENSCHAFTLICHE FACHMAGAZIN

Was macht Städte smart?

Digitalisierung versus Lebensqualität

Big Data | Green Digital Charter | Kritische Infrastrukturen | Privatheit | Sharing-Systeme



Lassen sich Kritische Infrastrukturen in vernetzten Metasystemen schützen?
© pixabay.com

Smart Cities im Kontext der Digitalisierung

Herausforderungen bei Überwachung und Schutz Kritischer Infrastruktur in Smart Cities

Digitalisierung, Big Data, Sensorik, Smart & Safe City, Kritische Infrastruktur, Metasysteme

Peter Fey

Die zunehmende Digitalisierung der verschiedenen Lebenswelten begünstigt den Trend zu Smart Cities. Die möglichst umfassende Vernetzung auf horizontaler und vertikaler Ebene ermöglicht das Erkennen und Verifizieren gefährdender Situationen, aber auch die zielorientierte und verzögerungsfreie Reaktion auf kritische Ereignisse. Zugleich stellt sie jedoch die größte Gefahrenquelle dar: Wie lässt sich Kritische Infrastruktur im Kontext von Smart Cities wirksam schützen, wenn aus bislang autarken Strukturen komplexe vernetzte Metasysteme werden? Gefordert sind übergreifende Ansätze – und ein Umdenken aller Beteiligten.

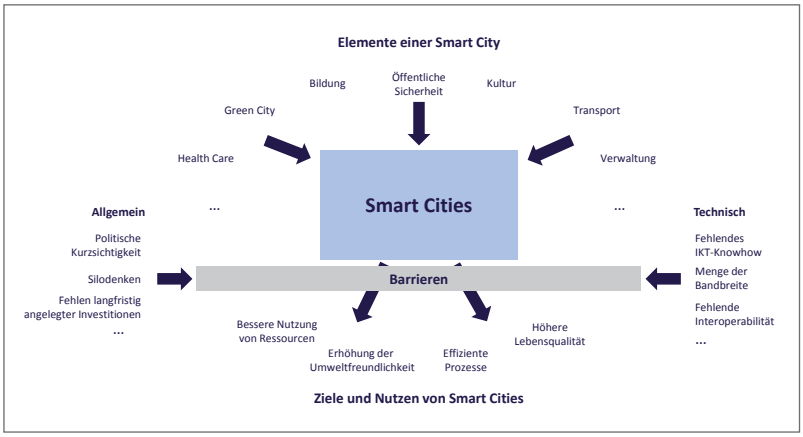


Bild 1: *Ziele und Barrieren zur Verwirklichung von Smart Cities. © Dr. Wieselhuber& Partner*

Der Trend zur Urbanisierung wird nicht nur in den asiatischen Regionen, sondern auch im so genannten Westen ungebremst voran schreiten. Im Jahr 2014 lebten laut der UN Population Division bereits 53,6 % der Weltbevölkerung in städtischen Regionen [1]. China ist in Sachen Urbanisierung sicherlich der Spitzenreiter, was Tempo und vor allem die Dimensionen der urbanen Ballungsgebiete anbelangt. Doch auch in Westeuropa schreitet die Verstädterung, wenn auch auf einem bereits hohen Niveau, weiter voran: Im Jahr 2000 betrug der Anteil der städtischen Bevölkerung bereits 75,3 %, bis 2020 soll er auf stolze 80,0 % anwachsen – womit auch Westeuropa im Hinblick auf die zunehmende Urbanisierung vor neuen, nicht unerheblichen Herausforderungen steht.

Der Trend zur Urbanisierung verlangt nach neuen Antworten auf die Frage, wie das gesellschaftliche, wirtschaftliche und verwaltungstechnische Miteinander in derartigen Ballungsgebieten zu organisieren ist. Bereits in den frühen 2000er Jahren wurde der Begriff Smart City geprägt. Richtet man den Blick auf die verschiedenen Definitionen, ist rasch zu erkennen, dass es keine einheitliche Nutzung dieses Begriffs gibt. Im Wesentlichen geht es um die intelligente Vernetzung bisher getrennt agierender Systeme (siehe **Bild 1**) wie das Smart City Council definiert:

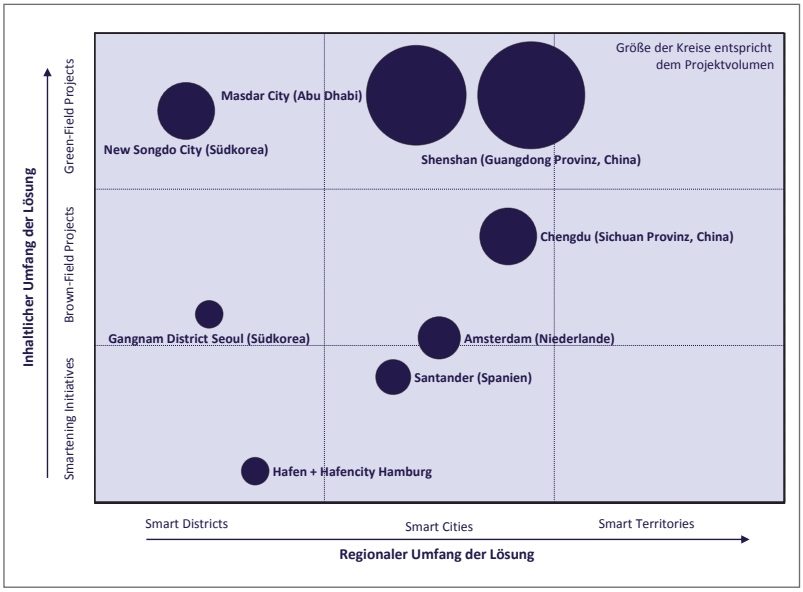
„Smart Cities have been defined as urban centers that integrate cyber-physical technologies and infrastructure to create environmental and economic efficiency while improving the overall quality of life." [2]

Der hinter dem Ansatz für Smart Cities stehende Kerngedanke ist geprägt von dem Umstand, dass auch Städte mehr und mehr im Wettbewerb stehen. Um langfristig zu überleben, sind die Ballungszentren auf eine prosperierende örtliche Wirtschaft, ein funktionierendes Gemeinwohl und motivierte und qualifizierte Bürger angewiesen. Der wirtschaftliche Gedanke des Wettbewerbs und das Ziel, möglichst attraktiv zu erscheinen, sind die Triebfedern für den Smart City-Ansatz. Die ISO-Norm 37120 [3] zeugt bereits heute davon, wohin die Reise gehen wird: Anhand von rund 100 Indikatoren wird die soziale, wirtschaftliche und umwelttechnische Performanz von bis heute ca. 250 Städten auf transparente Weise gemessen.

Getrieben durch den Megatrend Digitalisierung, soll die Qualität des öffentlichen und des privaten Lebens mit Hilfe von digitalen Technologien nachhaltig gesteigert werden. Intelligente Sensoren und Aktuatoren, Kommunikationsnetzwerke, Rechenzentren und die entsprechende Software werden die Bausteine sein, aus denen sich ein Smart City-Projekt physisch und mit Intelligenz versehen zusammensetzt. Ist die Smart City damit nichts anderes als ein spezifischer Teil des „Internet of Things" (IoT)? Vordergründig geht es im Kern um eine möglichst vollständige Vernetzung unterschiedlicher Partikular-Systeme oder auch Lebenswelten zu einem System der Systeme bzw. einem Metasystem.

Smart City-Projekte sind aktuell weltweit anzutreffen und stellen für viele Unternehmen auch wirtschaftlich ein interessantes Betätigungsfeld dar. Allein China möchte bis 2025 den stolzen Betrag von 320 Mrd. USD investieren, Saudi Arabien immerhin noch 70 Mrd. USD. Bereits bis 2020 sollen Schätzungen zufolge zwischen 100 Mrd. USD und 1000 Mrd. USD weltweit in Smart City-Projekte investiert werden. Dabei wird hinsichtlich des inhaltlichen Reifegrades zwischen sogenannten Smartening Initiatives (Implementierung von Teillösungen), Brown-Field-Projects (im Bestand) und Green-Field-Projects („Grüne Wiese") unterschieden. Während Green-Field-Projects vor allem in Asien und im Mittleren Osten zu finden sind, trifft man im europäi-

Bild 2: *Lösungsspektrum von Smart City-Projekten. © Dr. Wieselhuber& Partner*



schen Raum in erster Linie auf Smartening Initiatives und Brown-Field-Projects. Auf der anderen Seite spielt die räumliche Ausdehnung der Vorhaben eine Rolle: So wird zwischen Smart District, Smart Cities und Smart Territories unterschieden (siehe **Bild 2**).

Kritische Infrastruktur – zunehmend wichtig, zunehmend gefährdet

Der Begriff der „Kritischen Infrastruktur" nimmt im Kontext von Smart Cities, der Digitalisierung und des „Internet of Things" eine zentrale Rolle ein. Laut dem Bundesministerium des Inneren definiert sich dieser wie folgt:

„Kritische Infrastrukturen (KRITIS) sind Institutionen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Kritische Infrastrukturen sind häufig vernetzt und hängen voneinander ab, welches zu Risiken und Kaskadeneffekten führen kann." [4]

Sieht man sich die Elemente der Kritischen Infrastruktur im Einzelnen an, dann sind ähnliche Sektoren zu finden wie unter dem Begriff der Smart City: Energie- und Wasserversorgung, Transport und Verkehr, Finanz- und Versicherungswesen, das Gesundheitswesen, staatliche Behörden und Verwaltungsorgane, Informations- und Kommunikationstechnik sowie Medien und kulturelle Einrichtungen. Die Schnittmenge der zugehörigen Sektoren bzw. Subsysteme ist groß. In einem Smart City-Projekt werden alle Teilaspekte von Kritischen Infrastrukturen und darüber hinaus noch weiteren Bereichen des städtischen Lebens mit Hilfe digitaler Techniken zu einem „Smart City-Web" verknüpft, um so den größtmöglichen Nutzen für das gesellschaftliche, wirtschaftliche und verwaltungstechnische Miteinander der Bürger zu erzielen.

Die zunehmende Abhängigkeit von Kritischer Infrastruktur ist in städtischen Gebieten eine der Kernmotivationen für den vermehrten Einsatz von Sicherheitstechnik im oder außerhalb des Kontextes von Safe City-Projekten. Der weltweite Markt für derartige Projekte wird laut HSMR bis 2020 auf 226 Mrd. USD anwachsen. Auch hier zählt China, gefolgt von den USA und Indien, zu den Spitzenreitern. Viele der Safe City-Projekte weisen starke Merkmale von Smart City-Projekten auf: Der Einsatz des sicherheitstechnischen Equipments dient hierbei nicht mehr nur ausschließlich dem Kernziel Sicherheit. Je besser eine Volkswirtschaft entwickelt ist, desto mehr werden die Technologien der Sicherheitstechnik für Zwecke der Optimierung und Effizienzsteigerung z.B. von Verkehrs- oder Personenströmen eingesetzt. Die Ziele von Smart und Safe Cities sind also sehr ähnlich, wenngleich die von Smart Cities deutlich weiter gefasst sind.

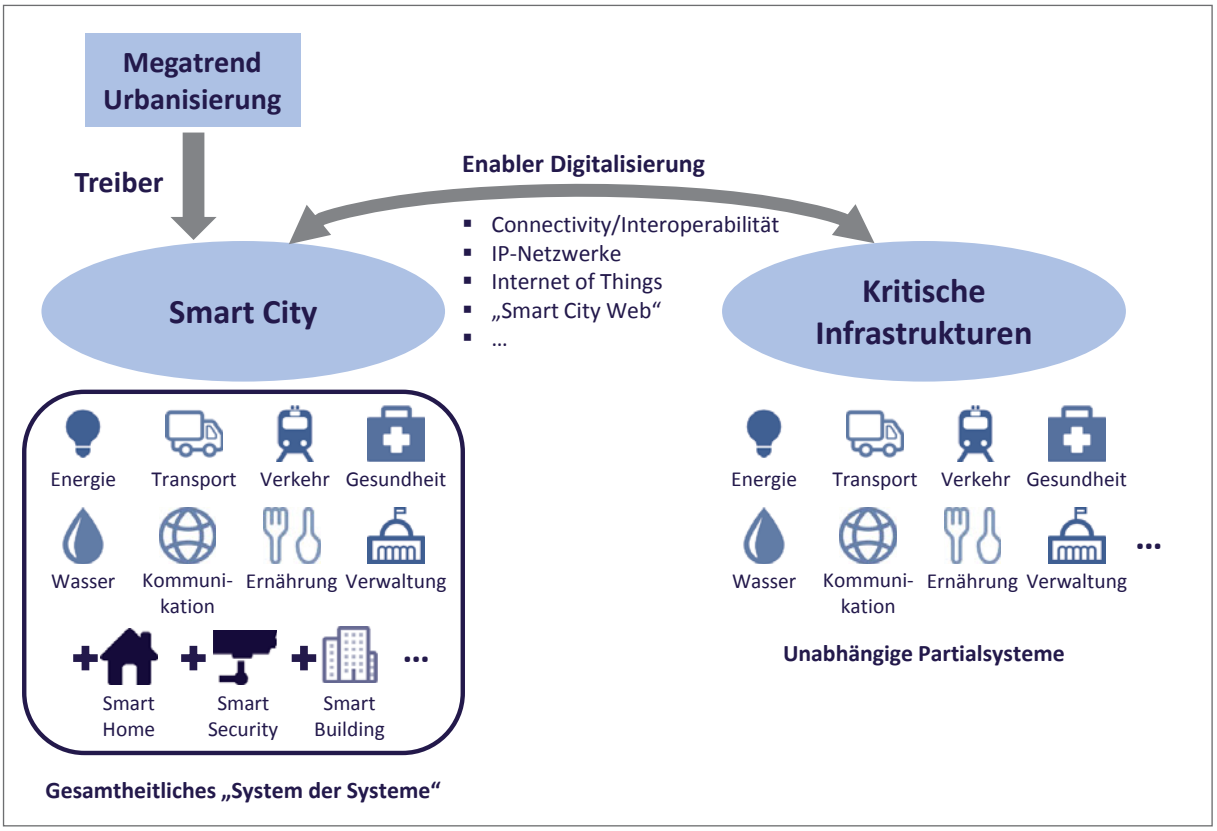


Bild 3:
Kritische Infrastrukturen im Kontext von Smart Cities.
© Dr. Wieselhuber& Partner

Systemische Sicherheit für Smart & Safe Cities

Die auf horizontaler und vertikaler Ebene miteinander vernetzten Teilsysteme einer Smart City umfassen zwingend den Schutz der Kritischen Infrastruktur – auch und gerade weil die Integration von Einzelsystemen ihr Kernmerkmal ist. Innerhalb derartiger Systeme ist der Begriff der Sicherheit einer entscheidenden inhaltlichen Veränderung unterworfen: Steht beim Schutz der Kritischen Infrastruktur im Sinne von Einzellösungen noch die physische Sicherheit im Vordergrund, wandelt sich der Sicherheitsbegriff im Kontext von Smart & Safe Cities mehr und mehr in Richtung der systemischen Sicherheit bzw. zu dem der Cyber Security. In diesem Zusammenhang wird häufig auch vom alten und neuen Sicherheitsbegriff gesprochen. Die Digitalisierung ist damit einerseits der Enabler für Smart Cities, auf der anderen Seite stellt sie damit aber auch die größte Gefahrenquelle für diese dar (siehe **Bild 3**).

Ganzheitliche Lösungen für Smart & Safe City-Projekte sind charakterisiert durch die folgenden Merkmale:

- Leistungsfähige und smarte Sensorik und Aktuatorik, die von einfachen RFIDs bis hin zu Embedded Systems mit einer dezentralen „Intelligence on the Edge“ ausgestattet sein können
- Hohe Konnektivität bzw. Interoperabilität der einzelnen Komponenten untereinander und mit der bestehenden Netzwerkinfrastruktur
- Performante Informations- und Kommunikationstechnologien zur Übertragung einer Flut von Daten an die verschiedenen Adressaten
- Leistungsfähige Rechencenter in Verbindung mit entsprechender Komprimierungstechnik zur Analyse und Aufbereitung der gewonnenen Daten – Smart Data ist das Ziel
- Integrierte Management-Systeme bzw. sicherheitstechnische Leitstände, die den Operatoren einen ganzheitlichen Überblick über die Situation gewähren und dabei wechselseitige Interdependenzen berücksichtigen
- „Collaboration Monitoring & Acting“, d.h. das Zusammenführen öffentlicher und privater Leistungen am Anfang und am Ende der relevanten Wertschöpfungskette
- Aktives Change Management und die Initiierung permanenter Lernprozesse zur Optimierung der bestehenden Produkte, Systeme und Dienstleistungen, denn komplexe Metasysteme werden nie fehlerfrei sein

Zusammenfassend kann festgehalten werden, dass die Systemintegration und die Beherrschung zentraler Schlüsseltechnologien wesentliche Voraussetzungen für die erfolgreiche Realisierung komplexer Smart & Safe City-Projekte sind. Damit ergeben sich für die beteiligten Akteure einerseits zahlreiche Geschäftschancen, andererseits werden sie dazu in die Lage versetzt, ihre Services gegenüber den Bewohnern und den Institutionen einer Smart & Safe City auf einem deutlich höheren Niveau zu erbringen.

Cyber Security als eine der Kernherausforderungen

Die genannten Voraussetzungen scheinen in einer zunehmend digitalisierten Welt auf den ersten Blick keine allzu hohen Hürden zu setzen. Es besteht jedoch eine Vielzahl von Hemmnissen bzw. Wachstumshürden, die einer raschen Erschließung der Chancen im Zusammenhang mit Smart City-Projekten gegenüber stehen. Hierzu zählen unter anderem:

- Mangelnde Professionalität hinsichtlich der Projektplanung und der dem Smart City-Projekt zugrundeliegenden Gesamtstrategie
- Unzureichendes technologisches Bewusstsein in Bezug auf die Möglichkeiten und Grenzen, die sich aus den neuen Technologien ergeben
- Politische Hemmschwellen können Smart & Safe City-Projekte in verschiedener Hinsicht einschränken: Feindliche Einstellung gegenüber Überwachungstechniken, unzureichendes Commitment gegenüber derartigen Projekten, etc.
- Silodenken der unterschiedlichen Institutionen und die Gefahr einer mangelnden Zusammenarbeit zwischen den öffentlichen und privaten Trägern der einzelnen Sektoren sowie ungeklärte Fragen nach den Entscheidungskompetenzen in einem derartig komplexen System
- Ungesicherte Finanzierung der Projekte insbesondere bei knappen Budgets der öffentlichen Hand und ein schwer greifbarer „Return on Investment“
- Auf der technischen Seite sind trotz der vielen Fortschritte die mangelnde Konnektivität der Einzelkomponenten sowie die unterschiedlichen Übertragungsprotokolle und Verschlüsselungsstandards eine Herausforderung
- Eine weitere Hürde ist in der teilweise unzureichenden Bandbreite der öffentlichen und privaten Netzwerke zu sehen

Diese Liste ließe sich noch um zahlreiche Punkte erweitern. Eine der größten Herausforderungen für die Realisierung von Smart & Safe City-Projekten ist zusammenfassend darin zu sehen, dass ein ganzheitlicher systemtechnischer Ansatz zwingend die Überwindung des Silodenkens voraus setzt. Die

einzelnen Sektoren einer Smart & Safe City haben in der Vergangenheit nie gefordert, an einer gemeinsamen, übergreifenden Problemlösung zu arbeiten. Im Gegenteil: Die Bereiche agieren in getrennten Systemen mit unterschiedlichen Standards und auf unterschiedlichen technischen Niveaus. Auch stehen Ansätzen, wie dem „Collaboration Monitoring & Acting"-Konzept, noch eine Reihe rechtlicher Probleme im Weg.

Eine der Kernherausforderungen oder besser Gefahren ist mit dem Schlagwort der Cyber Security am besten umrissen (siehe auch **Bild 4**): Folgt man der These, dass es sich bei einer Smart & Safe City um nichts anderes als ein spezifisches „Internet of Things" handelt, wird deutlich, warum die Cyber Security in diesem Kontext eine besonders herausragende Bedeutung zukommt. Der effektive Schutz der Kritischen Infrastruktur im Kontext einer Smart & Safe City ist elementare Voraussetzung für deren Verwirklichung. Die technischen Standards sind in den verschiedenen Bereichen unterschiedlich ausgeprägt, viele Komponenten waren nicht für einen vernetzten Einsatz geplant. Was also, wenn über die physische Schnittstelle einer veralteten, lediglich einem Upgrade unterworfenen Komponente ein Angriff auf das Gesamtnetzwerk erfolgt? Self-Awareness- und Self-Protecting-Systeme, die im Falle eines Fehlers oder Angriffs zu einem gesicherten Ausgangszustand zurückkehren können, müssen zu einem zwingenden Bestandteil derartig vernetzter Metasysteme werden.

Selbst wenn für diese Kernherausforderungen eine Lösung gefunden ist, bleibt immer noch ein weiteres Problem ungelöst: Wie ist der „Informational Overload" derartiger Metasysteme zu vermeiden?

Big Data ist ein vielzitiertes Schlagwort der Gegenwart. Um den Übergang von Big Data zu Smart Data zu erreichen, sind für eine Reihe spezifischer Aufgabenstellungen leistungsfähige Algorithmen programmiert worden. Doch reichen diese Lösungen, um dem Komplexitätsgrad eines Smart & Safe City-Projektes gerecht zu werden? Aktuell wohl kaum. Am Ende der Kette „von Big Data zu Smart Data" müssen letztendlich entscheidungsorientierte Erkenntnisse stehen, die den Entscheidungsträgern innerhalb einer hochkomplexen Smart & Safe City Handlungsorientierung geben. Hier ist noch ein weiter Weg zu gehen.

Fazit

Sind Smart Cities die adäquate Antwort auf den Trend der Urbanisierung? Im Grundsatz ist dem wohl zuzustimmen. Allerdings gilt es noch eine ganze Reihe von Hürden zu überwinden – technische ebenso wie solche, die in den unterschiedlichen Denkmodellen der verschiedenen beteiligten Akteure liegen. Aus diesem Grunde werden in den nächsten Jahren vor allem in Europa wohl primär Smartening Projects, die auf die Implementierung von Teilaspekten einer Smart City-Lösung abzielen, im Mittelpunkt stehen. Langfristig gesehen wird es aber nicht nur bei den asiatischen Green-Field-Projekten zu einer schrittweisen Integration von immer mehr Teilsystemen kommen – auch im europäischen Raum dürften Smart City-Projekte wohl bald Realität werden.

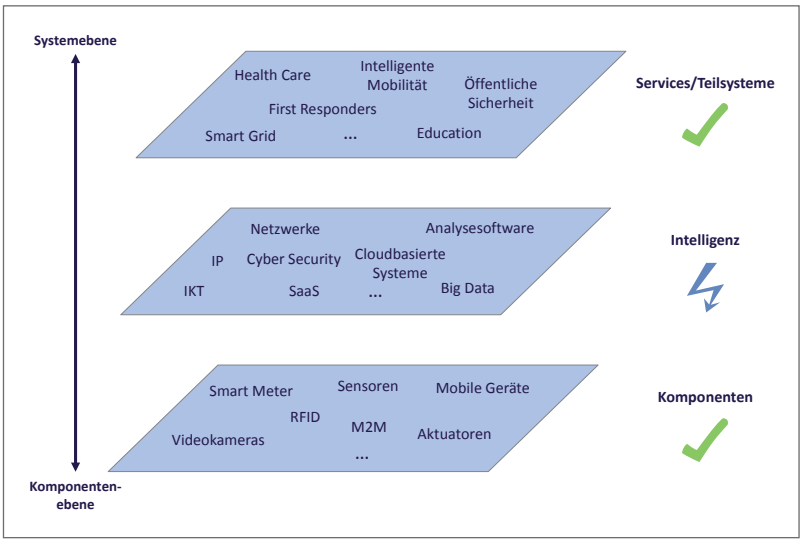


Bild 4: *Ebenen von Smart Cities © Dr. Wieselhuber& Partner*

LITERATUR

[1] United Nations Population Division: 2014 Revision of World Urbanization Prospects; http://esa.un.org/unpd/wup/ (Abruf am 22.12.2015)

[2] Smart Cities Council: "Vision"; http://smartcitiescouncil.com/smart-cities-information-center/definitions-and-overviews (Abruf am 22.12.2015)

[3] International Organization for Standardization: ISO 37120:2014 – Sustainable development of communities – Indicators for city services and quality of life; http://www.iso.org/iso/catalogue_detail?csnumber=62436 (Abruf am 22.12.2015)

[4] Bundesministerium des Innern: Nationale Strategie zum Schutz Kritischer Infrastrukturen; http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.html (Abruf am 22.12.2015)

AUTOR

Dr. **Peter Fey**,
Leiter Competence Center Sicherheitstechnik,

Dr. Wieselhuber & Partner, München
Kontakt: **fey@wieselhuber.de**