Herausforderung Logistik +++ Logistic challenges +++ Reform der Finanzarchitektur +++ Reform of the financial architecture

DOSSIER 42
Fluch & Segen der Globalisierung
Boon & bane of globalisation

INTERVIEW 28
Helmut Schmidt: Eine neue Weltordnung?
A new world order?

griephan global security

04 | 2008
www.griephan-globalsecurity.com

Thomas Straubhaar
Geht der Globalisierung der Sprit aus?
Is globalisation losing its juice?

Karl Engelhard
Gefährdung logistischer Ketten
Endangered supply chains

Wettbewerbsfaktor Sicherheit

STANDARDS MATTER

Competition factor security

PantherMedia/Sven T.

STANDARDS sind eine Grundvoraussetzung für funktionierende Sicherheitslösungen. Und wer Standards setzt, definiert Märkte.

Wettbewerbsfaktor Sicherheit

Competition factor security

Standards are a prerequisite for functioning security solutions. And those who set standards define markets.

A dynamic market is emerging around the topic of networked security. Its wide range of tasks comprises topics like the protection of critical infrastructures, border security, the security of public spaces and industrial counter-espionage. Many players offer a variety of products and solutions for this purpose.
In this complex environment standards serve to set uniform objectives for expectations and developments. Standards build a bridge between security and prosperity. They help ensure that the developed products and solutions provide answers to current or future security challenges and release the innovation potential of business and science. Therefore developing standards is an important tool of security, business and innovation policies that actively shape the future.

PLAYERS AND REQUIREMENTS Unlike the largely uniform defence market the market for networked security is more heterogeneous. On the state side it comprises authorities and organisations with security tasks, the armed forces and respective ministries on a national and federal state level. In the private sector it comprises businesses in general and above all the owners and operators of critical infrastructures (e.g. transport, energy, ICT providers, banks). And not to forget solution providers in the security and defence industry as well as builders who create critical infrastructures.
It is obvious that security products with a focus on the needs of these different customer groups need to meet a very wide range of requirements. They should
+++ Enable and simplify real-time networking of the players by encouraging a shared situational awareness/understanding and supporting decision-making with suitable tools.

Heiko Borchert

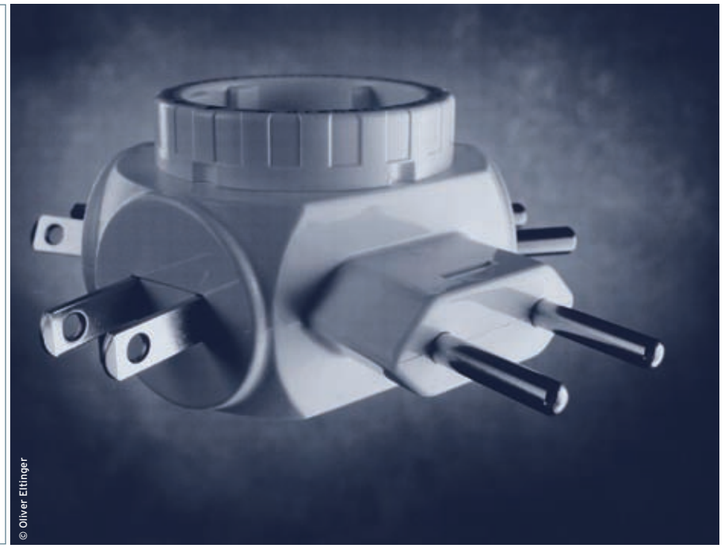
Rund um das Thema Vernetzte Sicherheit entsteht ein dynamischer Markt. Themen wie der Schutz der Kritischen Infrastrukturen, die Grenzsicherheit, die Sicherheit öffentlicher Räume oder die Abwehr der Wirtschaftsspionage beschreiben das breite Aufgabenspektrum. Zahlreiche Akteure bieten hierzu unterschiedliche Produkt- und Lösungsvorschläge an.
In diesem komplexen Umfeld dienen Standards dazu, die Erwartungen und Entwicklungen auf einheitliche Zielvorstellungen auszurichten. Standards sind das Bindeglied zwischen Sicherheit und Prosperität. Sie tragen dazu bei, dass Produkte und Lösungen entwickelt werden, die gleichzeitig Antworten auf die aktuellen bzw. künftigen Sicherheitsherausforderungen geben und das Innovationspotenzial von Wirtschaft und Wissenschaft freisetzen. Deshalb ist die Entwicklung von Standards ein wichtiges Instrument einer aktiv gestaltenden Sicherheits-, Wirtschafts- und Innovationspolitik.

AKTEURE UND ANFORDERUNGEN

Im Unterschied zu dem weitgehend homogenen Markt der Rüstungsgüter ist der Markt der Vernetzten Sicherheit heterogener. Auf der staatlichen Seite geht es um die Behörden und Organisationen mit Sicherheitsaufgaben, die Streitkräfte sowie die jeweiligen Ministerien auf Bundes- und Länderebene. Im privatwirtschaftlichen Bereich sind neben der Wirtschaft im Allgemeinen vor allem die Eigentümer und Betreiber der Kritischen Infrastrukturen (z. B. Transport, Energie, Informations- und Kommunikationsunternehmen, Banken) zu nennen. Hinzu kommen die Lösungsanbieter aus der Sicherheits- und Rüstungsindustrie sowie die Bauunternehmen, die Kritische Infrastrukturen erstellen.
Es ist naheliegend, dass Sicherheitsprodukte, die auf die Bedürfnisse dieser unterschiedlichen Kundengruppen ausgerichtet sind, ein sehr breites Anforderungsspektrum abdecken müssen. Sie sollten
+++ die Vernetzung der Akteure in Echtzeit ermöglichen und vereinfachen, indem sie beispielsweise das gemeinsame Lagebewusstsein/-verständnis fördern und die Entscheidungsfindung durch geeignete Instrumente unterstützen.
+++ flexibel und skalierbar sein, damit sie an die Anforderungen der staatlichen und privatwirtschaftlichen Kunden angepasst werden können. Das erfordert zum Teil eine von Grund auf anders konzipierte Architektur, die mit den Anforderungen der Kunden wachsen kann.

© Tom Hoenig/Westend61

Welcher Standard gilt?



© Oliver Eltinger

Which standard supply?

+++ die Interoperabilität fördern, damit staatliche und privatwirtschaftliche Akteure reibungslos zusammenarbeiten können. Gerade weil die Finanzlage im zivilen Sicherheitsbereich noch angespannter ist als im militärischen Umfeld, wollen die Kunden eingeführte Systeme möglichst lang nutzen. Neue Sicherheitsprodukte müssen also parallel zu den bereits betriebenen eingesetzt werden können. Das erhöht die Anforderungen an die Kompatibilität zwischen den Produkten.

»Standards schaffen Vertrauen in die Zuverlässigkeit von Lösungen, Produkten und Dienstleistungen.«

»Standards inspire trust in the reliability of solutions, products and services.«

STANDARDS: WAS IST DAMIT GEMEINT? Sprechen wir vor diesem Hintergrund von Standards für den Markt der Vernetzten Sicherheit, so sind damit zwei unterschiedliche Ausprägungen gemeint.

Zum einen ist eine Leistung, die Standards setzt, beispielgebend. Welche Akteure mit welchen Ansätzen welche Felder des Marktes der Vernetzten Sicherheit bedienen, ist im Moment noch offen. Bislang ist die Entwicklung des Marktes von Anwendungen geprägt, die aus dem militärischen Umfeld durch Adaption ins zivile Umfeld übertragen werden. Damit können erste Erfolge erzielt werden, doch langfristig wird dieser Ansatz nicht ausreichen.

Von entscheidender Bedeutung für adäquate Sicherheitslösungen im zivilen Umfeld ist eine umfassende Systemarchitektur, die auf offenen Standards basiert. Unternehmen, die sich gestützt darauf um neue Anwendungen bemühen, werden beispielgebend sein und Standards zur Erschließung neuer Marktfelder setzen. So wird beispielsweise im Rahmen des österreichischen Sicherheitsforschungsprogramms KIRAS daran gearbeitet, ein öffentlich-privates Lagebild in enger Zusammenarbeit zwischen Ministerien und Unternehmen zu erstellen. Es zeichnet sich ab, dass damit eine neue Fähigkeit der gemeinsamen öffentlich-privaten Führung auf der strategischen und allen nachgelagerten Ebenen geschaffen wird, die für die Sicherheitsvorsorge von zentraler Bedeutung ist.

Zum anderen bezeichnen Standards ganz bestimmte Anforderungen, die von Lösungen, Produkten und Dienstleistungen erfüllt werden müssen. Traditionellerweise fällt dabei der Blick auf die eigentlichen Sicherheitsstandards, die z. B. die Leistungsfähigkeit und die Ausfallsicherheit beschreiben. Im Markt der zivilen Sicherheitslösungen werden darüber hinaus weitere Kategorien von Standards von zunehmender Bedeutung sein, nämlich solche, die

+++ die kontinuierliche Entwicklung der relevanten Fähigkeiten an die Entwicklung der Sicherheitslage und den technischen Fortschritt sicherstellen (Transformation),

+++ es ermöglichen, Prozesse für eine offene Architektur unter Einschluss öffentlicher und privater Akteure zu definieren,

+++ die Vernetzung und den Daten- bzw. Informationsaustausch zwischen diesen Akteuren fördern und

+++ die organisationsübergreifende Führung in der normalen Lage und im krisenbezogenen Anlassfall gewährleisten.

Damit sind gleichzeitig auch jene Marktfelder beschrieben, die aus Anbietersicht ein attraktives Zukunftspotenzial versprechen. Neben den eigentlichen Produkten zeichnen sich zwei Segmente ab:

+++ Marktreife Betreiberlösungen, bei denen die Anbieter die Infrastruktur/Plattform unterhalten und betreiben, während die Kunden eine spezifische Anwendung wie z. B. die Bereitstellung von Kommunikations-, Transport- oder Überwachungskapazitäten erwerben. Gewisse zivile Leitstellen funktionieren bereits heute nach diesem Prinzip.

+++ Eng damit verbunden ist die Beratungsfunktion für öffentliche und privatwirtschaftliche Bedarfsträger im Hinblick auf die Konzipierung vernetzter Sicherheitslösungen. Dabei stehen das Architekturdesign und die Prozessmodellierung im Mittelpunkt.

Dabei erleichtern Standards den Austausch zwischen den öffentlichen und privatwirtschaftlichen Partnern, schaffen Zugang zu attraktiven Marktfeldern und können die Wirtschaftlichkeit von Lösungen fördern, indem anstelle von Neuentwicklungen auf Bewährtes zurückgegriffen werden kann. Neben diesen allgemeinen Wesensmerkmalen sind für den Markt der Vernetzten Sicherheit zwei weitere Aspekte wichtig:

+++ Standards schaffen Vertrauen in die Zuverlässigkeit von Lösungen, Produkten und Dienstleistungen. Das ist für die Akzeptanz von Sicherheitsanwendungen von vorrangiger Bedeutung. Daher ist es konsequent, wenn im europäischen Umfeld die Einführung eines Sicherheitslabels diskutiert wird, das den Kunden als Orientierungshilfe beim Erwerb von Sicherheitsanwendungen dienen soll.

+++ Standards differenzieren Wettbewerber voneinander. Sicherheitsansätze, die der unilateralen Ausweitung nationaler Sicherheitsvorschriften dienen, sind problematisch. So wird kritisiert, die US Container Security Initiative verzerre den Wettbewerb, weil Warenströme auf bestimmte, zur Einfuhr von Gütern in die USA zertifizierte Häfen umgelenkt werden. Die Häfen, die die Standards allerdings erfüllen, verschaffen sich einen Wettbewerbsvorteil gegenüber der Konkurrenz.

»Öffentlich-Private Sicherheitspartnerschaft dient der nationalen Sicherheitsvorsorge – und ist exportfähig.«

»Public private security partnership is at the service of national security management – and can be exported.«

BEGLEITMAßNAHMEN Die Entwicklung von Standards für die Vernetzte Sicherheit ist anspruchsvoll, denn es geht um mehr als die technische Normierung. Es erscheint daher sinnvoll, den Prozess der Standardisierung mit folgenden Begleitmaßnahmen zu unterstützen:

+++ Gemeinsame Risiko-, Aufgaben- und Fähigkeitsanalyse

Die Entwicklung von Standards sollte Hand in Hand mit der Beurteilung des nationalen und internationalen Risikobildes vorgenommen werden. Nur so kann gewährleistet werden, dass die angebotenen Lösungen den relevanten Sicherheitsherausforderungen entsprechen. Erforderlich ist daher ein regelmäßiger und systematischer Austausch zwischen Staat und Wirtschaft im Hinblick auf die erwarteten Sicherheitsherausforderungen, den gegenwärtigen Stand der staatlichen und unternehmerischen Sicherheitsvorsorge, die vorhandenen öffentlichen und unternehmerischen Sicherheitsfähigkeiten sowie den bestehenden Handlungsbedarf. Daraus können weitere Maßnahmen abgeleitet werden.

+++ Wissenschafts- und Technologiestrategie für Vernetzte Sicherheit

Im Verteidigungsbereich ist es üblich, sich über die rüstungstechnischen Kernfähigkeiten und die rüstungsindustrielle Technologiebasis Gedanken zu machen. Angesichts eines umfassenden Sicherheitsverständnisses reicht dieser Ansatz nicht länger aus. Er sollte ergänzt werden durch vergleichbare Überlegungen für die zivilen Sicherheitsanwendungen. Beide Perspektiven sollten in einer Wissenschafts- und Technologiestrategie sowie in entsprechenden Förderprogrammen für die Vernetzte Sicherheit zusammengeführt werden. In der Gesamtschau von Herausforderungen, Aufgaben, Fähigkeiten sowie vorhandenen Wissenschafts- und ▸

+++ Be flexible and scalable, so that they can be adapted to the needs of public and private customers. This partly requires an architecture with a radically different concept, which can grow with the customers' needs.

+++ Promote interoperability so that public and private players can work together smoothly. Especially because the financial situation in the civil security sector is even tighter than in the military environment, customers want to use introduced systems for as long as possible. New security products need to be usable side by side with existing systems. This heightens compatibility requirements for the products.

STANDARDS: WHAT DO WE MEAN? When speaking of standards for the networked security market in this context, we always mean two different manifestations.

Firstly, a service that sets standards acts as a role model. The future players, segments and approaches of the networked security market are still unclear. So far, the market's development is influenced by applications that have been transferred from the military segment to a civilian context by adaptation. Despite its initial success this approach will not suffice in the long run.

A comprehensive systems architecture based on open standards is essential for adequate security solutions in a civil environment. Companies who base their efforts to develop new applications on this will set an example and create standards for the development of new market segments. For example, the Austrian security research programme KIRAS is working on creating a public-private situation profile as a close co-operation between ministries and companies. There are signs that this will create a new capability of shared public-private leadership on the strategic and downstream levels that are of crucial importance for security management.

Secondly, standards always refer to certain requirements that solutions, products and services need to meet. Traditionally, the focus is on the actual security standards that describe e.g. efficiency and security against loss. In the market for civil security solutions new categories of standards will also come to play an important role, i.e. those that

+++ Ensure a continuous development of relevant capabilities adapted to the security situation and technical progress (transformation),

+++ Enable the definition of processes for an open architecture integrating public and private players,

+++ Promote the networking and exchange of data and information between these players, and ▸

Technologiekompetenzen könnte dann ein umfassender Standardisierungsansatz entwickelt werden.

+++ Anreize
Die staatliche Sicherheitsvorsorge ist untrennbar mit der unternehmerischen Sicherheitsvorsorge verbunden. Um Sicherheit und Prosperität zu fördern, ist daher zu überlegen, mit welchen Rahmenbedingungen Anreize für Investitionen in Sicherheitslösungen geschaffen werden könnten. Denkbar wären z. B. Anreize, die die Entwicklung von Sicherheitsprodukten steuerlich fördern. Ein anderer Anreiz ist die öffentlich-private Risikobeurteilung, die von den Unternehmen als neue Informationsquelle für gezielte Produktentwicklungen genutzt werden könnte.

AUSBLICK Durch die hier beschriebene Nutzung von Standards wird Sicherheit im doppelten Sinne des Wortes zu einem Wettbewerbsfaktor. Sicherheit und Prosperität können aber nur dann Hand in Hand entwickelt werden, wenn Staat und Wirtschaft enger als in der Vergangenheit zusammenarbeiten. Benötigt wird eine Öffentlich-Private Sicherheitspartnerschaft, in der gemeinsam Sicherheitsrisiken und -chancen analysiert sowie Maßnahmen definiert, umgesetzt und weiterentwickelt werden.
Die Öffentlich-Private Sicherheitspartnerschaft dient der nationalen Sicherheitsvorsorge – und sie ist exportfähig. In dem Maße, wie sich die Bundesregierung beispielsweise bei der Stabilisierung von Drittländern für den Aufbau des Sicherheitssektors einsetzt, kann sie der heimischen Wirtschaft und Wissenschaft neue Marktchancen erschließen. Standards sind dabei jenes Instrument, mit dem ein politischer Führungsanspruch in wirtschaftliches Potenzial übersetzt werden kann.

Dr. Heiko Borchert
führt sicherheitspolitische Beratungsunternehmen in der Schweiz und in Österreich und ist Mitglied des Beirates von IPA Network, Berlin
Directs security political consulting companies in Switzerland and Austria and is a member of the Advisory Council of IPA Network, Berlin
email_to_author@dvvmedia.com

+++ Guarantee cross-organisational leadership in normal situations and in crisis-based events.
This also describes market segments that promise an attractive future potential from the suppliers' point of view. Alongside the actual products two segments are anticipated:
+++ Marketable operator solutions with providers maintaining and operating the infrastructure/platform, while customers acquire a specific application such as communication, transport or surveillance capacities. Certain civil control centres already work on this basis.
+++ This is closely related to the consulting function for public and private buyers regarding the development of networked security solutions. The focus is on architectural design and process modelling.
Standards facilitate communication between den public and private partners, offer access to attractive market segments and can boost the profitability of solutions by enabling the use of proven resources instead of developing new ones. Apart from these general characteristics two further aspects are important for the networked security market:
+++ Standards inspire trust in the reliability of solutions, products and services. This is of overriding importance for the acceptance of security applications. So it's only logical that the introduction of a security label is being discussed in Europe in order to offer customers orientation for purchasing security applications.
+++ Standards create distinctions between competitors. Security approaches that unilaterally expand national security regulations are problematic. Hence, critics claim that the US Container Security Initiative distorts competition because goods flows are redirected to certain ports that are certified to import goods to the USA. However, the ports that meet these standards will have a competitive advantage over their competitors.

SUPPORTING MEASURES The development of standards for networked security is a demanding task, as it comprises more than just technical standardisation. It would therefore make sense to support the standardisation process with the following flanking measures:
+++ Common risk, responsibility and capability analysis
The development of standards should go hand in hand with the assessment of the national and international risk situation. This is the only way to guarantee that the offered solutions meet the relevant security challenges. Therefore a regular and systematic exchange between the state and industry is necessary in view of the expected security challenges, the current situation of public and corporate security management, existing public and private security capabilities and existing need for action. Further measures may be developed on this basis.
+++ Science and technology strategy for networked security
In the defence sector it is a common practice to think about defence-related core capabilities and the defence-industrial technology basis. In view of a broader definition of security this approach is no longer adequate. Similar considerations need to be added for civil security applications. Both perspectives should be combined in a science and technology strategy and corresponding programmes to promote networked security. Based on a combination of all these challenges, tasks, capabilities and existing scientific and technological expertise, one could then develop a comprehensive standardisation approach.
+++ Incentives
Public security management is indivisible from corporate security management. To boost security and prosperity one must consider what framework conditions are needed to create incentives for investments in security solutions. One thinkable option would be tax incentives to encourage the development of security products. Another incentive would a public-private risk assessment which the companies could use as a new source of information for targeted product developments.

OUTLOOK The utilisation of these standards will make security a competition factor in a double sense. But security and prosperity can only develop hand in hand, if the public and private sectors co-operate more closely than in the past. What we need is a public-private security partnership where security risks and opportunities can be jointly analysed followed by the definition, realisation and further development of measures.
This public private security partnership will be at the service of national security management – and can be exported. In the same measure that the German government commits to building a security sector through the stabilisation of third countries, it can open up new market opportunities for domestic industry and research. Standards are the tool we need to translate political leadership claims into economic potential.

intersec
trade fair and conference

The focal point of security and safety.
For the protection of life, property and assets, information and borders.

January 18 – 20, 2009
Dubai International Convention and Exhibition Centre, Dubai, UAE

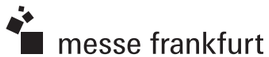
www.intersecexpo.com

Accompanying conference: "Fighting terrorism and serious organised crime"

Sunday, January 18, 2009: Intersec Conference Keynotes
Monday – Tuesday, January 19 – 20, 2009: Conference Tracks According to Intersec Trade Fair Sections

Topics

Commercial Security (14 Lectures)	Information Security (14 Lectures)	Homeland Security, Counter-Terrorism & Policing (14 Lectures)	Fire & Rescue (14 Lectures)	Safety & Health (IOSH Middle East Conference)
Chair: N.N. 21st Century security challenges CCTV / behavioural analysis IP and physical security Guards management Security by design and high-rise security concepts Latest trends in biometrics	Chair: Dr. Oliver Weissmann (TUV Rheinland), Co-editor of IS 27xxx Threat report Basics of information security Measuring and introducing information security Industrial espionage and social engineering Cryptography Information security in the oil and gas sector Information security in the finance / banking sector	Chair: Rita Cosby (author, news presenter and senior correspondent, formerly with MSNBC and FOX) Global supply chain security Critical infrastructure protection Serious organised crime and the link to terrorism (drugs, money laundering and human trafficking) Airport and port security The effect of terrorism on and business continuity management in the finance / banking sector Globalisation and the new economy of terrorism	Chair: Neil Wallington Editor of Fire Middle East Magazine Fire safety engineering in the Middle East Urban search and rescue (the aftermath of terrorist attacks) Fire and rescue challenges of new generation large aircrafts Building fire protection technology and high rise fire fighting Oil and gas fire fighting Command & control at major incidents Technical rescue (transport accidents, water and line rescue)	**First day: Conference "Practitioners in Practice"** Chairs: Nattasha Freeman President - IOSH Protecting your assets: Transition of health and safety from construction to facilities management Training and maintaining competence: ADCO graduate development programme **Second day: Panel Discussion and Networking Workshops** • Ask the lawyers • Communication business benefits • Updating your CPD and membership queries • Understanding and implementing CDM • Reporting incidents: requirements and best practice

Supported by:

Organised by: