Forum KI am 23./24. Mai 2006 in Wiesbaden

Begrüßung

Carl-Ernst Brisach, BKA Wiesbaden, KI

Sehr geehrte Damen und Herren,

wir bei KI haben uns in diesem Jahr dazu entschlossen, das KI 1 - Forum zu einem KI-Forum auszuweiten. Ich möchte einige Gedanken darlegen, warum wir glaubten dies tun zu sollen:

(1)
Gemäss seinem Selbstverständnis sieht sich das Kriminalistische Institut des BKA als polizeiliche Institution,
die innovativ und zukunftsorientiert

- neue oder noch unbeantwortete (kriminal)polizeiliche Fragestellungen und Problemlagen im nationalen/internationalen Kontext aufgreift, dokumentiert und analysiert,
- Lösungswege und -methoden erforscht und entwickelt,
- diese in Form von Beratungs- und Serviceleistungen Bedarfsträgern zur Verfügung stellt und
- die (Forschungs-)Ergebnisse in die kriminalpolizeiliche Aus- und Fortbildung einbringt.

Wir betreiben also überwiegend anwenderorientierte Polizeiforschung, d.h. **Forschung und Entwicklung für die Polizei** in den Bereichen

- Kriminalistik (Methodenwissen)/Kriminologie (Ursachen- und Erscheinungsformen der Kriminalität)
- Technologie (zentral sind Neue Technologien, hier: Technikfolgenabschätzung für die Kriminalitätsentwicklung und Methodenentwicklung für die operative Einsatztechnik der Polizei)

in internationaler polizeilicher Kooperation mit verschiedenen Forschungs- und Entwicklungsdienststellen in Europa den USA sowie in Kooperation mit deutschen Technologieunternehmen.

(2)
Um dem im Selbstverständnis des Kriminalistischen Instituts formulierten Anspruch gerecht zu werden, ist eine enge Verzahnung der drei Bereiche „Forschung“, „Beratung/Umsetzung“ und „Lehre“ erforderlich.
Diese Verzahnung soll durch eine enge, ganzheitlich orientierte Kooperation über die organisatorischen Gruppengrenzen des Instituts hinaus erzielt werden.
Hierbei bieten sich insbesondere die Felder der derzeit im BKA priorisierten Deliktsbereiche an, in denen sowohl unter verhaltensorientierten als auch unter technischen Aspekten **ganzheitliche** Lösungen für die Kriminalitätsbekämpfung erarbeitet werden sollen.

(3)
Eine sich abzeichnende Neuorientierung der Sicherheitspolitik, die mit der Definition eines erweiterten Sicherheitsbegriff einhergeht, fordert diese **ganzheitliche** Sichtweise ein.
Im Rahmen der Erörterungen zu einem neuen Sicherheitsbegriff tritt zu den Dimensionen des klassischen Sicherheitsbegriffs in der Innen- und Außenpolitik die Dimension **technischer Sicherheit** hinzu.
Ein Problem, das zwar allgemein als gelöst gilt, wie Harrisburg oder Tschernobyl gezeigt haben aber eben immer noch ein „Restrisiko“ birgt. Zudem scheint der Aspekt der technischen Sicherheit im Zeitalter asymmetrischer Kriege insbesondere im Zusammenhang mit "kritischen Infrastrukturen" wieder in den Mittelpunkt von Sicherheitsüberlegungen gerückt.

(4)
Die Erweiterung des Sicherheitsbegriffs und der damit verknüpfte Wandel in den Sicherheitskonzepten zeigt sich am deutlichsten auf europäischer Ebene. Unter der ebenso klaren wie zutreffenden Zielsetzung, dass nichts geeigneter ist, den EU-Bürgern die Relevanz der Union zu demonstrieren als im Kampf gegen die Kriminalität und dort vor allem denjenigen Bereichen, in denen dem Nationalstaat Grenzen seiner Einflussnahme gesetzt sind, ist das Sicherheitskonzept der EU entwickelt worden.
Hier sind drei Aspekte von Sicherheit benannt, die alle im deutschen Begriff Sicherheit enthalten sind: safty, security und certainty.

Safety deckt dabei den technisch-funktionalen Bereich ab. Im Deutschen entspricht dem vielleicht am ehesten „Zuverlässigkeit", d.h. die Wahrscheinlichkeit, dass ein technisches Gerät bzw. ein System ohne innere Störungen wie vorgesehen funktioniert. Moderne Sicherungstechnik lässt gleichzeitig aber auch das Spannungsfeld zwischen *safty* und *security* erkennen. Die vollautomatisierte Fabrik erfordert hoch komplizierte und damit anfällige Steuerungsmechanismen. Unter dem Gesichtspunkt innerbetrieblicher Sicherheit ist es erwünscht, diese Kontrollsysteme möglichst weit zu vernetzen, damit Steuerungsexperten, die mit Störsituationen umgehen können, jederzeit Zugriff haben. Eine solche Vernetzung eröffnet aber gleichzeitig den Zugang für unautorisierte Eingriffe von außen. Je vernetzter ein System ist, um so größer wird die Wahrscheinlichkeit, dass an irgendeiner Stelle des Netzwerkes störende Einflüsse ins System gelangen.
So kommt es immer wieder vor, dass Hackern durch Tüftelei oder Zufall der Zugang zu lebenswichtigen Kontroll- und Steuerungszentren gelingt. Aufwendige Sicherungssysteme nützen nur etwas, wenn sie mit absoluter Konsequenz durchgehalten werden.

Security bedeutet Sicherheit gegenüber Gefahren und Risiken, die ihren Ursprung außerhalb der technischen Sphäre haben und in der Regel entweder durch Menschen oder durch Naturkatastrophen verursacht werden sowie die Absicherung von Wirtschaftsbeziehungen und von strategischen Versorgungsgütern, der Rechtssicherheit

von Wirtschaftssubjekten gegenüber Erpressung und staatlicher Willkür bis hin zur Absicherung der Finanzmärkte und des internationalen Zahlungsverkehrs.

Sicherheit ist somit künftig umfassend und global zu denken, weil die einzelnen Lebensbereiche und die Kontinente ineinander verwoben sind. Es kommt heute nicht nur darauf an Sicherheit innerhalb der Grenzen Deutschlands oder Europas zu gewährleisten, sondern auch Deutsche und deutsches Eigentum im Ausland wirksam zu verteidigen.

Im Weltmaßstab ringen wir derzeit um eine neue Art von Sicherheit: Interdependente, umfassende, präventive Sicherheit. Im Zeitalter der Globalisierung wird Sicherheit nur mehr im internationalen Maßstab vorstellbar. Auch Sicherheit globalisiert sich. Deshalb ist es wichtig, dass sich die Staatengemeinschaft bereit hält, dort zu intervenieren, wo Prinzipien einer solchen neuen weltweiten Sicherheitsordnung bedroht sind.
Was heißt das für unsere Sicherheitsstrategien? Wir müssen weg von der reaktiven Bekämpfungsstrategie, die gleichsam einem Reparaturtross hinter den Ereignissen hertrottet, hin zu einer aktiven Prävention. Das bedeutet nichts anderes, als weit vorausschauend Risiken mitzudenken und rechtzeitig eine Gegenstrategie zu entwickeln.
Die Abteilung KI ist diesem umfassenden Verständnis von Sicherheit verpflichtet.

Carl-Ernst Brisach
BKA Wiesbaden, KI
ki@bka.wiesbaden.de