Sicherheit und Risiken vernetzter Gesellschaften

Moderne Gesellschaften sind unter anderem gekennzeichnet durch eine große Zahl von Phänomenen, die sich immer schneller entwickeln und die per se, aber auch durch ihre Entwicklungsgeschwindigkeit zunehmende Risiken mit sich bringen.
In diesem Beitrag soll vorwiegend auf die Risiken eingegangen werden, die sich aus den nationalen und internationalen Vernetzungen von Infrastrukturen ergeben.
Hierzu wird vor allem auf Trends in der Bedrohung, bei Verwundbarkeiten und deren Wahrnehmung eingegangen. Am Beispiel der so genannten Kritischen Infrastrukturen wird aufgezeigt, welche neuen Herausforderungen auf uns zukommen und welche Maßnahmen Politik, Gesellschaft, Wirtschaft und Forschung vorbereiten und ergreifen sollten.
Erforderlich wird ein Gesamt-Sicherheitssystem, bei dem sich Einzelmaßnahmen in eine übergeordnete Strategie international einreihen und welche im Ernstfall effizient zusammenwirken müssen.

Bedrohungen, Verwundbarkeiten, Risiken

Während der Periode des kalten Krieges haben sich die Bedrohungsbetrachtungen primär auf eine massive militärische Ost-West Konfrontation konzentriert. Seit deren Ende sind die Ursachen, Quellen, Mittel der Bedrohung und deren Weiterentwicklung ungleich vielseitiger und schwerer vorherzusagen. Ursachen bzw. Quellen, mit denen wir uns heute verstärkt auseinandersetzen müssen sind u.a.

- Katastrophen
  - Natürliche wie Umwelt; Klima
  - Künstliche aus Industrien; Anlagen; Infrastrukturen
- Pandemien
- Organisierte Kriminalität
- Terrorismus
- Instabile Staaten
- Proliferation
- Kriege.

Naturkatastrophen hat es schon immer gegeben. Dennoch werden und müssen sie heute anders betrachtet und behandelt werden als vor 100 Jahren und zwar aus folgenden Gründen: Die Auswirkungen von Katastrophen sind aufgrund der in den letzten 200 Jahren verdreifachten Bevölkerungsdichte entsprechend gravierender. Hinzu kommen erhöhte Verwundbarkeiten durch die Abhängigkeit der Gesellschaft von hoch technisierten Infrastrukturen – Energie, Wasserversorgung, Verkehrssysteme, das Gesundheitswesens u.v.m. Darüber hinaus hat sich die Zahl der Naturkatastrophen aus welchen Gründen auch immer, exponentiell entwickelt und in den letzten 100 Jahren auf das 100-fache gesteigert [1]. Selbst wenn man Veränderungen in der Datenerhebung und der Zählweise herausnimmt, ist der Trend immer noch erschreckend.

Über Bedrohungen durch internationalen Terrorismus und organisierte Kriminalität gibt es Bände. Neuartig ist nicht nur die Entwicklung des technischen und intellektuellen Potenzials, sondern auch die veränderte Wahrnehmung in Politik und Gesellschaft und die sich daraus ergebenden Verpflichtungen: **Globalisierung** heißt auch globale Verantwortung zu helfen. **Demokratisierung** bedeutet auch, dass der Bürger an den Staat zunehmend hohe Erwartungen an Sicherheitsstandards entwickelt. **Hochtechnisierung** heißt auch, dass es eine erhöhte Verantwortung gibt, moderne Technologien einerseits zu schützen,

[1] The OFDA/CRED International Desaster Data Base

andererseits sie intensiv auch für Sicherheitsaufgaben einzusetzen und entsprechende Forschungs- und Entwicklungsinvestitionen zu leisten.
Zu den so verschiedenen **Bedrohungsquellen** gesellen sich die verschiedenartigsten **Bedrohungsmittel**. Im Falle kriegerischer oder terroristischer Bedrohungen reichen sie vom konventionellen Sprengstoff über chemische, biologische und radiologische Substanzen bis zur Bedrohung mit Nuklearwaffen als Folge zunehmend schwieriger zu kontrollierender Proliferation, welche in Fachkreisen immer ernster genommen wird.

Eine heute noch eher zweitrangige Rolle spielt die Informationstechnik (IT) im Rahmen aggressiver Bedrohungsszenarien: Aber in hoch zivilisierten Gesellschaften sind etwa 95% aller Vorgänge, Handlungen, Planungs- und Steuerungsprozesse, die Versorgung der Bevölkerung, Geräte, Waren usw. in irgendeiner Weise von Informationstechnik abhängig. Mit der Verdopplung von Leistung, Kapazität und Vernetzung alle 1 ½ bis 2 Jahre setzt sich dieser Trend ungleich schneller fort als die Durchdringung der Gesellschaft mit anderen Technologien. (Das Automobil z.B. ist heute im Durchschnitt doppelt so schnell und achtmal so sicher wie vor vierzig Jahren ein großer, aber im Vergleich zur IT sehr bescheidener Fortschritt). Neben den unumstrittenen Segnungen durch die IT haben sich aber auch ganz neue Angriffsflächen, Verwundbarkeiten und Risiken entwickelt: Die Zahl der Sicherheitsvorfälle im Internet hat sich in den letzten 5 Jahren jährlich verdoppelt[2]. Wichtige Systeme unserer Gesellschaft wie Energieversorgung oder Flugverkehr reagieren immer empfindlicher bis katastrophal auf Störungen, u.a. weil sie hochgradig vernetzt sind und von hoch entwickelten elektronischen Überwachungs-, Steuerungs- und Kontrollsystemen abhängen. Jüngere Ereignisse haben das nur allzu drastisch verdeutlicht (Stromausfälle, Zusammenbruch von Buchungssystemen etc.).

Auch wenn diese bisher eher zufällig entstehen, kann man sich vorstellen, welche Folgen ein gut vorbereiteter und konzentrierter Angriff auf kritische IT- abhängige Infrastrukturen, ein so genannten „Cyber"- Angriff haben kann. Man kann es auch anders ausdrücken: Solche Vorfälle, die vor den Augen der Welt passieren sind geradezu eine Einladung an terroristische Organisationen, sich mit neuen, auch auf Informationstechnik abzielenden Angriffsoptionen zu beschäftigen. Es gibt genügend Hinweise darauf, dass sie es tun. Aber der Terrorismus ist nicht die einzige Art von „Cyber"- Bedrohungen: Sie reichen vom Amateur-Hacker (und der kann bekanntlich bereits Schäden in Milliardenhöhe produzieren) über verärgerte oder infiltrierte Mitarbeiter in sensiblen Unternehmen, Industriespionage, elektronische Geldwäsche, Verbreitung von verbotenen Informationen und illegalen Darstellungen. Und natürlich hat auch das Militär für Auseinandersetzungen auf staatlicher Ebene längst den „Cyber War", oder harmloser ausgedrückt, die so genannten „Informationsoperationen" entdeckt und ihre technischen und operativen Fähigkeiten entsprechend weiter entwickelt.

Wodurch ist dieser Trend und die zu erwartende Verschärfung im IT-Sektor begründet? Weltweite Vernetzung generell und empfindliche Wirtschaftszweige wie das Finanzwesen oder die Gasversorgung und die Verbreitung des Internets machen Wirkungen unvorhersehbar und Täter meistens nicht verfolgbar. Heutige Systeme sind in ihrer Komplexität in kritischen Situationen kaum noch beherrschbar: Das fängt schon beim „einfachen" im Wirklichkeit hoch- und viel zu komplizierten Betriebssystem am PC an und endet bei massiven Beschwerden der Energieversorger in Nordamerika und Italien über Sicherheitssysteme, die mit den Herausforderungen eines liberalisierten und internationalisierten Marktes nicht schritt gehalten haben. Angriffswerkzeuge wie Viren, Spoofing Techniken oder verteilte schädliche Software und Nutzungsanleitungen dafür sind immer leichter über das Internet zu bekommen, und ihre Handhabung erfordert immer geringere Vorkenntnisse. Angriffskanäle, insbesondere über das Internet stehen zur „öffentlichen" Verfügung.

Erschwerend kommt hinzu, dass sie Rechtslage einigermaßen unsicher ist: National verschieden und bzgl. der Definition von Straftatenbeständen und der Strafverfolgung

[2] Carnegie Mellon University / CERT-CC

unscharf. Ebenso unklar ist, wer z.B. bei einem massiven Informationsangriff auf ein hochempfindliches System wie die Flugsicherung, möglicherweise mit der Folge von Flugzeugabstürzen, zuständig ist: Die Polizei, weil es sich um einen Vorfall im „Inneren“ handelt? Die Bundeswehr, weil der Angriff von einem sog. Schurkenstaat ausging? Oder der Grenzschutz, weil Terroristische Täter eingeschleust wurden?

Eine weitere Tatsache macht den seit Mitte der 90-er Jahr unternommenen Versuchen, unsere empfindlichen Infrastrukturen sicherer zu machen, zu schaffen: Die Frage der Systematik. Während es im militärischen Bereich klare Zuständigkeiten, Einsatzregeln, empirische Datenbasen für Waffenwirksamkeiten, umfangreiche Tests, Versuche, Übungen und nicht zuletzt eine Jahrzehnte alte Tradition (und entsprechende Investitionen) in der Sicherheitsforschung gibt, sind die Phänomene neuartiger ziviler Sicherheitsrisiken vergleichsweise kaum erforscht. Während bei der Bundeswehr seit Mitte der 60-er Jahre analysen mit leistungsfähige Modelle und Simulationen und computergestützte Planübungen zum Standard gehören, wurde z.B. die Länder- übergreifende Katastrophenübung LÜKEX[3] im Herbst 2004 weitgehend „zu Fuß“, d.h. mit relativ bescheidenen Analyse- und Unterstützungswerkzeugen durchgeführt.
Während ein Einsatz der Bundeswehr im Kosovo generalstabsmäßig durchgeplant wird, muss sich die Bekämpfung der Elbeflut mit Improvisationen, mangelhafter Frühwarnung, fehlenden Koordinierungsmitteln und nicht interoperablen Funksystemen begnügen[4].
Während es für Massenvernichtungswaffen Verträge über Nichtverbreitung und bei Landminen immerhin den Versuch der Eindämmung gibt, sind „Cyber-Waffen“ weltweit praktisch jedem verfügbar. Die „Proliferation“ ist quasi in den kommerziellen Systemen eingebaut.

Eine vorsichtige Abschätzung von Experten hat ergeben, dass sich die IT- bedingten Risiken auch unter Berücksichtigung der zweifellos auch entwickelten Sicherheitsmaßnahmen in den letzten 10 Jahren um den Faktor 10 bis 100 – je nach betrachtetem System- erhöht haben. Dabei treten denkbare Szenarien, die massive wirtschaftliche Schäden, aber auch Tote, Verwundete und Kranke in größerer Zahl nach sich ziehen immer mehr in den Vordergrund.

Kritische Infrastrukturen

Als kritisch bezeichnet man Infrastrukturen, deren Störung oder Zerstörung massiven Einfluss auf unser Gemeinwesen haben, und zwar auf

- Leben und Gesundheit der Bevölkerung
- Funktionsfähigkeit und Leistung der Wirtschaft
- Funktionsfähigkeit wichtiger staatlicher Einrichtungen
- Souveränität politischen Handels.

Zu den Kritischen Infrastrukturen zählen i.d.R.

- Telekommunikation
- Energie
- Wasser & Lebensmittel
- Transport & Verkehr
- Finanzwesen
- Sensitive Industrien
- Sicherheitsdienste und Militär
- Gesundheitswesen
- Politik & Verwaltung

Auch die Medien sollte man dazurechnen, da sie inzwischen in allen Katastrophen-Szenaren eine zentrale Rolle einnehmen.

[3] http://web1.vs155055.vserver.de/luekex/index.php
[4] Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung Flutkatastrophe 2003; Hans-Peter von Kirchbach

Kritische Infrastrukturen sind i.d.R. flächenmäßig verbreitet, hoch vernetzt und abhängig von Computern und Netzwerken. Zusätzlich risikobehaftet sind diese Infrastrukturen, weil sie auch durch sog. Interdependenzen extrem stark gegenseitig voneinander abhängen. Pumpen von Wasserwerken brauchen Strom, Stromversorger brauchen elektronische Überwachungs- und Steuerungseinrichtungen, und ein Krankenhaus benötigt alles gleichzeitig. Entsprechend komplex sind Schadensbilder und Schadensausbreitung bei realen Vorfällen und erst recht in antizipierten künftigen Szenarien:
Sie können reichen von Personenschäden über direkte finanzielle und materielle Verluste, Einbußen bei der Produktion, Verlust an Image und Marktanteilen von Firmen, Umweltschäden, Verlust oder Diebstahl wertvollen Wissens bis hin zur politischen Handlungsunfähigkeit, Massenpanik oder Vertrauensverlust der Bevölkerung in Politik, Wirtschaft und Technik.

Schutzkonzepte und Maßnahmen

Um sich einem so hoch komplexen Gebiet wie den neuen Sicherheitsrisiken bestehend aus einer Vielzahl möglicher Bedrohungen, Verwundbarkeiten und sich daraus ergebenden Risiken zu nähern, bedarf es zunächst grundlegender analytischer Verfahren und Modelle und entsprechender Daten. Aber ebenso einer Kapazität aus Forschern und Analytikern gepaart mit den eigentlichen „Bedarfsträgern“ – den Sicherheitskräften sowie den Infrastrukturbetreibern. Wiederum verglichen mit dem militärischen Sicherheitsbereich stecken wir hier noch in den Kinderschuhen. Das liegt einerseits daran, dass es für die „Innere Sicherheit“ keine vergleichbaren zentralen Institutionen der Forschung gibt, es gibt aber auch keine „ordnende Kraft“ diese zu schaffen, weder national (wie das BMVg) noch international (wie die NATO).

Die Kompetenzen für Fragen der inneren Sicherheit sind auf unzählige Institutionen verteilt, angefangen vom Bund über Länder, Kommunen bis hin zur privaten Wirtschaft, die ja auch in Eigeninteresse selbst Sicherheitsvorkehrungen schafft. Entsprechend gibt es keine ausreichend koordinierte Vorbereitung auf neue Sicherheits-Herausforderungen[5] und keine angemessenen Mittel. Dies ist keine Schuldzuweisung sondern eine Feststellung. Denn alle Zuständigen und ggf. Betroffenen tun ihr Bestes, jeweils eben reduziert auf die begrenzten Möglichkeiten in ihrem Kompetenzbereich. Wenn man beobachtet, wie mühsam bis fast unmöglich es beispielsweise ist, auf Kommunaler- und Länderebene einheitliche Leistellen für Rettungsdienste, Feuerwehr und Polizei einzurichten, so wird an diesen Beispiel deutlich, wie weit wir noch von einer „ganzheitlichen“ Sicherheitsstrategie in und für Deutschland entfernt sind. Die Einführung eines einheitlichen digitalen BOS- Funksystems in Deutschland rangiert zwischen Trauerspiel und Groteske – gemessen an deren Bedeutung und der Entwicklung in Nachbarländern.

Eine wirklich durchgreifende Änderung könnte und müsste von einer zentralen Kompetenz z.B. des Kanzleramtes ausgehen, was allerdings nicht ohne Eingriff in Ressortkompetenzen und die föderalen Verteilung realisierbar ist.

Natürlich gibt es viele Fortschritte im Detail, wie das Gemeinsame Melde- und Lagezentrum (GMLZ) auf Bundesebene und das deutsche Notfallvorsorge-Informationssystem deNIS oder die Bevorratung von Pocken-Impfstoff, die Abstimmung zwischen BMI mit BMVg über Ausrüstung mit ABC- Sensorik. Wohl erstmals hat die IMK /AK-V bereits 2002 beschlossen, die Umsetzung des Konzeptes „Neue Strategien zum Schutz der Bevölkerung in Deutschland“ voranzutreiben und - ein mutiger Schritt – die Einführung eines dringend erforderlichen einheitlichen und durchgängigen Führungssystems zu prüfen. Konkrete Umsetzungsmaßnahmen zu letzterem sind allerdings noch nicht bekannt.

[5] Dietrich Läpke: „Die Neuausrichtung der zivilen Sicherheitsvorsorge….“ In: Sicherheitspolitik in neuen Dimensionen, BAKS, Ergänzungsband 2004

Mit einem weiteren Prozess, dem allmählichen Zusammenwachsen verschiedener so genannter CERTs bzw. CERT[6]- Organisationen zu einem Verbund sind wir wieder bei dem Thema IT und Kritische Infrastrukturen angelangt. Der Grundstein für die Entwicklung eines „Nationalen Plans“ zum Schutz Kritischer Infrastrukturen wurde bereits im Herbst 1997, sicher auch angeregt durch die Pläne der USA , durch den damaligen Innenminister gelegt. Zur Zeit wird er für einen Teilbereich, nämlich kritische IT- abhängige Infrastrukturen erstellt. Mit der Schaffung des BBK ist zu hoffen, dass dieser Prozess auch übergreifend beschleunigt wird.

Vorbereitende Maßnahmen des BMI/BSI wie eine systematische Risikobewertung oder die globalen Abstimmungsprozesse von Maßnahmen zur Überwachung von Internet-Vorfällen lassen hoffen. Immerhin hat die IMK Schwachstellenanalysen der Infrastrukturen auf Länderebene vorgeschlagen. Das BMI hat Gespräche mit Infrastrukturbetreibern aufgenommen mit Ziel, sog. Public Private Partnerships zu schaffen, und im BBK wird das „Kompetenzzentrum Schutz Kritischer Infrastrukturen“ aufgebaut. Ein weiterer Anschub zu neuen Sicherheits-Konzepten, Abstimmungsprozessen und Koordinierungsmaßnahmen ist von der Fußball-Weltmeisterschaft 2006 zu erwarten.

Dennoch rangiert Deutschland im europäischen Vergleich eher im Mittelfeld: In Schweden wird Sicherheitspolitik unter den Schlagwort „Total Defense“ ganzheitlich betrachtet. Entsprechende Organisationen wie die SEMA haben zentrale Kompetenzen. Die Niederlande, die Schweiz und England arbeiten seit langem an politisch gewollten Konzepten für den besseren Schutz Kritischer Infrastrukturen und dem Aufbau entsprechender Organisationen. Bei allen Unterschieden der gesetzlichen und verfassungsrechtlichen Ausganglagen der einzelnen Staaten haben diese Programme doch Wesentliches gemeinsam:

- Sie sind von staatlicher Seite zentral gewollt.
- Sie versuchen, die verschiedenen Zuständigkeiten zumindest über Informations- und Abstimmungsprozesse zusammenzuführen.
- Sie haben die Notwendigkeit von starken sog. „Public Private Partnerships“ (PPP) erkannt und setzen sie schrittweise um.

PPPs sind vor allem deshalb notwendig, da fast alle großen Infrastrukturen wie Bahn, Energie, Telekommunikation, Luftverkehr nicht wie früher in staatlicher Obhut liegen, sondern privatwirtschaftlich betrieben werden. Hier stehen dann nicht mehr Sicherheitsinteressen und breite Versorgung der Bevölkerung als staatliche Aufgabe sondern der wirtschaftliche Betrieb und die Maximierung des Ergebnisses im Vordergrund.

Diese Modelle der gemeinsamen Vorsorge, welche sich in anderen Bereichen wie Mautsystem, e-Government oder dem Gesundheitswesen zunehmend bewähren oder auch gar nicht mehr entbehrlich sind, stoßen natürlich im Sicherheitsbereich auf größere Hürden. Hier geht es primär ja nicht um eine wirtschaftliche „Win-win“ Strategie, bei der im günstigsten Fall sowohl der Staat als auch die Privatwirtschaft jeweils Vorteile realisieren. Im Sicherheitssektor sind Verantwortlichkeiten zwischen Staat und Wirtschaft nicht so einfach teilbar, und der Nutzen der Wirtschaft aus einem stärkeren Engagement für mehr Sicherheit – im eigenen wie im Interesse des Gemeinwohls – lässt sich i. d. R. nicht mit rein betriebswirtschaftlichen Größen wie Kapitalrendite oder Marktanteilen messen.

In den USA genießt das Thema Schutz von Infrastrukturen nicht erst seit dem 11. September 2001 sondern bereits seit Mitte der 90-er Jahre die Aufmerksamkeit des Präsidenten. Mit der Einrichtung des Department of Homeland Security wurde auf höchster Ebene eine der vier Abteilungen der Behörde mit „Information Analysis and Infrastucture Protection“ beauftragt, was die strategische Bedeutung dieses Themas dort belegt. Strategiepapiere und Pläne gibt es in den USA inzwischen genügend. Aber trotz Investitionen von – im Vergleich zu Deutschland – riesigen Summen kommt man in den USA mit wirklich übergreifenden Maßnahmen auch nur sehr langsam voran.

[6] CERT = Computer Emergency Response Team

Auf internationaler Ebene wie EU, OSZE, VN, Europarat G8 gibt es kaum eine Organisation, die sich nicht schon mit Fragen der Sicherheit vernetzter Strukturen befasst und entsprechende Resolutionen, Beschlüsse, Empfehlungen verfasst hat. Eine gemeinsame internationale „Politik der nicht–militärischen Sicherheit“ gibt es bisher nur in Ansätzen. Dennoch lassen die Aktivitäten der EU zur ESDP[7]Hoffnung aufkommen:
Kommission, Rat und Parlament befassen sich zunehmend mit Fragen der Koordinierung von Sicherheitsaufgaben und in dem Forschungs-Rahmenprogramm Nr.6 sowie der „Preparatory Action in the field of Security Research“ (PASR) ist das Thema Schutz vernetzter Systeme und Infrastrukturen explizit verankert, ebenso in dem ab 2007 geplanten umfangreichen „European Security Research Programm“ (ESRP). Eine spezielle Rolle im IT-Sektor wird der Anfang 2004 gegründeten Behörde ENISA- European Network and Information Security Agency zukommen. Bis sich allerdings internationale Kooperationsstrukturen mit Europäischer Kompetenz herausgebildet haben, wird es noch Jahre dauern.

Das Fazit der Lagebeurteilung für Deutschland lautet also:
Es gibt durchaus akzeptable Sicherheitsstandards und Vorkehrungen für den Betrieb und die Verfügbarkeit wichtiger, u.U. lebenswichtiger vernetzter Infrastrukturen. Auf eine Störung katastrophalen Ausmaßes durch äußeren Angriff, z.B. Terrorismus – oder ein großes Naturereignis– beides vielleicht unwahrscheinlich aber im Bereich des Möglichen, sind wir nicht ausreichend vorbereitet.

Ein Mittel um hier pragmatisch voranzukommen sind so genannte Planübungen. Sie dienen vor allen der Sensibilisierung, der Erkenntnisgewinnung und der Vertrauensbildung zwischen den zahlreichen unterschiedlichen Organisationen und Zuständigkeiten. Erstmals wurde im Herbst 2004 die Länderübergreifende Krisenmanagement- Übung LÜKEX durchgeführt. Bleibt zu wünschen, dass Übungen dieser Art weiterentwickeln und sich möglichst auf internationaler Ebene auch gezielt mit der Problematik der Kritischen Infrastrukturen auseinandersetzen. Deren besondere Phänomene der Interdependenzen und Kaskadeneffekte sind bisher nicht ausreichend beleuchtet und vorausgedacht: Was passiert, wenn sich Folgeschäden im komplexen Netzwerk über verschiedene Infrastrukturen hinweg ausbreiten – von der Stromversorgung in die Transport- und Verkehrssysteme und Telekommunikation, von dort in das Banken- und Finanzwesen und die öffentliche Verwaltung usw. usw.? Und wie verbreiten sich Schäden grenzüberschreitend?
Diese äußerst komplexen Fragestellungen sind nur mit Hilfe leistungsstarker computer-gestützter Modelle – vielleicht vergleichbar mit der Wettervorhersage - beantwortbar.

Ausblick

Risikoeinschätzungen haben nach konkreten Schadensereignissen politische Konjunktur (s.h. Tsunami Katastrophe). Die Halbwertszeit des politischen Bewusstseins ist wesentlich kürzer im Vergleich zum notwendigen langfristigen strategischen Planen und Handeln. Die Phänomene der Risiken und Schadensentwicklungen im Falle massiver Störungen oder Zerstörung von vernetzten Strukturen, insbesondere mehrerer Infrastrukturen gleichzeitig, stellen uns vor neue analytische, politisch und operative Herausforderungen.

Institutionell verteilte Kompetenzen, z.T. unzureichende Ausrüstung und mangelndes Problembewusstsein behindern oder verzögern eine längerfristig angelegte und konsequente Planung und Umsetzung von Maßnahmen. Gerade vernetzte Infrastrukturen bedürfen übergreifender übernationaler Betrachtungsweisen und Schutzstrategien unter Einbezug der privaten Betreiber. Hierzu gibt es Ansätze aber kein adäquates „System“.

Dieses muss entwickelt werden mit dem Ziel „Prävention vor Reaktion“ auf

[7] European Security and Defence Policy

der Basis

- Hintanstellung partikularer Interessen (wie im Föderalismus angelegt).
- Der Zusammenarbeit aller relevanten Sicherheitskräfte.
- Vereinheitlichter Ausbildung und Führung.
- Partnerschaftlicher Zusammenarbeit von privatwirtschaftlichen Infrastrukturbetreibern und staatlichen Einrichtungen (PPP).
- Entsprechender staatlicher Anreize für die Wirtschaft.
- Internationaler Zusammenarbeit zur Beherrschung grenzüberschreitender Effekte.

Zusammenfassende Thesen

1. Die Sicherheits-Rahmenbedingungen haben sich in den letzten 15 Jahren grundlegend geändert.

2. Die Bedrohungen und deren Wahrnehmung sind vielseitig, z.T. diffus und ständigem Wandel unterworfen.

3. Die Verwundbarkeiten moderner Gesellschaften haben enorm zugenommen.

4. Einen großen Beitrag dazu leisten so genannte Kritische Infrastrukturen.

5. Diese werden heute vor allem unter wirtschaftlicher und nicht unter sicherheitspolitischer Zielsetzung betrieben.

6. Sie sind lebenswichtig für Staat, Wirtschaft und Gesellschaft.

7. Ihre gegenseitigen Abhängigkeiten, ihre Komplexität, ihre Durchdringung mit Informationstechnik und ihre globale Vernetzung werden nicht ausreichend als neue Sicherheitsrisiken gewürdigt.

8. Nationale und internationale Bemühungen zeigen in die richtige Richtung, sind aber erst der Anfang eines notwendigen Prozesses.

9. Dieser Prozess erfordert die Zusammenwirkung aller relevanten Kräfte, - von Staat und Sicherheitsorganen, Wirtschaft, Gesellschaft und der Forschung - im nationalen und im internationalen Rahmen.

10. Dieser Prozess muss in eine Gesamt-Sicherheitsstrategie eingebettet sein.