Rede
von Innenminister
Dr. Fritz Behrens
anlässlich der Eröffnung des Kongresses
"Netz- und Computersicherheit - sind wir auf einen
Angriff auf unsere Informationssysteme und
Informationsinfrastruktur vorbereitet?"
am 7. Oktober 2003
in der
Heinrich-Heine-Universität, Düsseldorf

Anrede,

neulich habe ich in einer Fachzeitschrift zum Thema Sicherheitssysteme das alte niederländische Sprichwort gelesen "Wenn der Wind weht, bauen manche Schutzhütten, andere errichten Windmühlen".

Um in diesem Bild zu bleiben - ich denke, dass der heute beginnende Kongress zeigen wird, dass es manchmal auch klug ist, beides zu tun. Diese Taktik verfolgt nämlich das Land Nordrhein-Westfalen.

Die Bundesrepublik Deutschland hat längst ihre ersten Schritte in der Entwicklung von einem Industriestaat in eine moderne Informationsgesellschaft hinter sich. Die dynamische Verbreitung und Nutzung digitaler Informations- und Kommunikationstechnologien durchdringt alle Lebensbereiche und verändert dadurch den Alltag jedes Einzelnen. Das Internet wird mit wachsender Geschwindigkeit zum gesellschaftlichen Allgemeingut und führt dazu, dass Kontakte aller Art von dem Leitmotiv des "any time - any place" geprägt sind.

Wir alle wissen, dass die Nutzung moderner Informationstechnologien von entscheidender Bedeutung für die Zukunftsfähigkeit unseres Landes in einer globalisierten Welt ist. Aus diesem Grunde hat das Innenministerium Nordrhein-Westfalen im März dieses Jahres den Masterplan E-Government zum weiteren Ausbau der Internet-Angebote der Landesverwaltung

beschlossen. Ich werde später mehr darüber berichten. Mit zunehmender Verbreitung dieser Kommunikationsmittel entstehen aber auch neue Gefährdungspotenziale, beispielhaft möchte ich hier nur die Begriffe "Cyberwar" und "Hackerangriffe" nennen, auf die ich noch zurückkommen werde. Ich spreche hier bewusst nur von Potenzialen, da nach wie vor die Anteile der kriminellen oder schädigenden Handlungen nur einen geringen Bruchteil aller Kontakte ausmachen. Dennoch ist die von dort ausgehende Gefahr nicht zu unterschätzen. Es ist nämlich ein Merkmal der modernen Informations- und Kommunikationstechnologien, dass sie den Einzelnen in die Lage versetzen, mit verhältnismäßig geringem Aufwand innerhalb kürzester Zeit gewaltige Schäden anzurichten. Es ist meine feste Überzeugung, dass diesen Gefahren mit einem Bündel von vielfältigen Maßnahmen begegnet werden muss, das von allen gesellschaftlichen Kräften - öffentlichen und privaten - Staat und Wirtschaft - im Sinne eines Netzwerks getragen wird. Hier sind Partnerschaften auf allen Ebenen gefordert!

Weil der heute beginnende Kongress genau diesem Ziel dienen soll, ein Netzwerk der Verantwortlichen zu initiieren, und dies unmittelbar der Sicherheit in unserem Landes zugute kommt, habe ich gerne die Schirmherrschaft übernommen.

Das Innenministerium Nordrhein-Westfalen ist das federführende Ressort für die Koordinierung aller ADV-Vorhaben der Landesverwaltung. Diese Aufgabe hat in dem Maße an Bedeutung gewonnen, in dem die Informationstechnik (IT) als unverzichtbarer Bestandteil einer modernen und effizienten Verwaltung erkannt worden ist. Viele Geschäfts- und Kommunikationsprozesse bauen darauf auf. In gleichem Maße ist die Verwaltung aber auch an diesem Punkt verwundbar. Hackerangriffe führen uns immer wieder vor Augen, wie verletzlich speziell Computersysteme mit einer Anbindung an das Internet sind. Ich möchte dieses an zwei Beispielen aus der Landesverwaltung, die sich in jüngster Zeit ereignet haben, verdeutlichen:

1. Beispiel

Wie Sie vielleicht der Presse entnommen haben, wurden das Internetangebot der Landesverwaltung und des Landtags am 23. und 24. Juli dieses Jahres durch einen Hacker-Angriff blockiert. Es handelte sich dabei um einen Angriff, bei dem ein sehr großer Datenstrom zu einer Überlastung der Systeme führte. Nahezu 700 Internetangebote aus NRW waren nicht mehr zugänglich. Zugleich konnten keine elektronischen Nachrichten mit Partnern über das Internet ausgetauscht werden.

Derartige Angriffe sind nicht ungewöhnlich, bemerkenswert war jedoch die große Intensität des Datenstromes. Sie reichte aus, den Internetzugang der Landesverwaltung mit einer Bandbreite von 155 Megabit pro Sekunde lahm zu legen. Der Angriff konnte nur in enger Kooperation vom Landesamt für Datenverarbeitung und Statistik und der Telekom abgewehrt werden, und zwar durch Konfigurationsmaßnahmen an Netzwerkkomponenten in New York.

Zu Ihrer - und natürlich auch meiner - Beruhigung möchte ich an dieser Stelle allerdings betonen, dass es den Angreifern dank der Sicherheitssysteme des Landes nicht gelungen ist, in das Netz der Landesverwaltung einzudringen. Es gab auch trotz des Angriffs keine Einschränkungen in der Kommunikation zwischen den Landesbehörden und anderen öffentlichen Verwaltungen, da diese über geschlossene Netzwerke erfolgt.

2. Beispiel

Mitte August trat mit "Sobig.F" (sprich: "Sobig F") ein Computervirus auf, das durch seine rasante Ausbreitung und weite Verbreitung in die Schlagzeilen geriet. Schneller als andere Viren verbreitete sich die Schadsoftware über E-Mail - und machte auch vor der öffentlichen Verwaltung nicht halt. Bei derzeit 2,8 Millionen elektronischen Nachrichten, die die Landesverwaltung monatlich mit Kommunikationspartnern im Internet ausgetauscht, überrascht es nicht, dass auch NRW hiervon betroffen war. In den ersten Tagen konnten nahezu 200.000 infizierte Nachrichten am zentralen Internetübergang abgefangen werden. In Spitzenzeiten war jede dritte Nachricht mit dem Virus infiziert. Ich bin froh, dass durch präventive zentrale Virenschutz-Maßnahmen, die das Landesamt für Datenverarbeitung und Statistik im Auftrag des Innenministeriums durchführt, beträchtlicher Schaden von der Landesverwaltung abgewendet werden konnte.

Diese Vorfälle sind ein Beispiel für die wachsende Bedrohung der kritischen Infrastrukturen - sowohl in Qualität als auch in Quantität - durch die fort-schreitende globale Vernetzung. Die öffentliche Verwaltung sitzt hierbei gleichsam mit Wirtschaft, Wissenschaft und Privatnutzern in einem Boot.

Die Landesverwaltung hat bereits sehr früh damit begonnen, das Internet zur Kommunikation mit unseren Kunden zu nutzen. Mittlerweile erschließen sich über das Internetangebot der Landesregierung mehr als 700 Informationsangebote der Behörden und Einrichtungen das

Landes. Ich freue mich, dass dieses Angebot eine sehr hohe Akzeptanz findet. Nahezu 15 Millionen Zugriffe pro Monat belegen das.

Von Anfang an wurde der Auf- und Ausbau des Internetangebotes von aufwändigen Sicherheitsmaßnahmen begleitet. Die Entwicklung eines mehrstufigen Sicherheitskonzeptes, die Einrichtung von drei zentralen Übergangspunkten zum Internet, die nach dem neuesten Stand der Technik gesichert sind, und anwendungsspezifische Maßnahmen wie Signaturen und Verschlüsselung sollen hier nur beispielhaft genannt werden. Nach wie vor werden erhebliche Investitionen getätigt, um mit modernster Technologie die Vertraulichkeit, Integrität und Authentizität von Daten in der Landesverwaltung sicherzustellen. Die Abwehr der eben beschriebenen Angriffe zeigt mir, dass dieses Geld sehr gut angelegt ist.

In einem nächsten Schritt wollen wir bis zum Jahr 2005 die wesentlichen Behördendienste des Landes rund um die Uhr und an jedem Ort den Bürgerinnen und Bürgern, der Wirtschaft, den Verbänden, anderen Verwaltungen sowie sonstigen Kunden der Verwaltung auf einem neuen Weg über das Internet zugänglich machen. Der im März dieses Jahres von der Landesregierung beschlossene Masterplan E-Government, den ich eingangs erwähnt habe, sieht die weitere Bereitstellung von 92 transaktionsorientierten Dienstleistungen, wie Antrags- oder Förderverfahren, in elektronischer Form vor.

Dies zeigt einmal mehr, dass die Landesregierung E-Government als eine wichtige Säule der Verwaltungsmodernisierung und gleichzeitig als einen Motor dieser Entwicklung ansieht. Wir werden die Möglichkeiten von E-Government zur Optimierung und Neugestaltung von Verwaltungsprozessen, zur Erhöhung der Kundenzufriedenheit sowie zur Erhöhung der Attraktivität des Wirtschaftsstandorts Nordrhein-Westfalen konsequent nutzen.

Bei allen damit verbundenen Vorteilen ist dieser Weg aber auch mit Risiken behaftet. Die Bereitstellung von Dienstleistungen im Internet erfordert einen besonderen Schutz der Daten und Systeme, denn die Angebote sind in dem weltweiten Netz für jedermann zugänglich. Sowohl für den Kunden, der Verwaltungsdienstleistungen elektronisch abwickeln möchte, als auch für den Hacker, der nur die Manipulation von Systemen und Daten im Sinn hat. Dennoch, so meine ich, haben wir keine andere Wahl, als diesen Weg der Modernisierung weiter zu beschreiten und uns mit den Gefahren auseinander zu setzen.

Sicherheit ist daher für die Landesregierung immer wieder ein sehr wichtiger Aspekt beim weiteren Ausbau der für E-Government benötigten Infrastruktur und bei der Umsetzung der Fachverfahren. Diese Anforderung muss nicht im Widerspruch zu wirtschaftlichen Erwägungen stehen. Unser Masterplan sieht den Aufbau und die Bereitstellung zentraler Infrastrukturkomponenten für die Landesverwaltung vor, die von allen Behörden bei der Kommunikation mit den Kunden verwendet werden können. Durch die Nutzung einer gemeinsamen E-Government-Infrastruktur können Sicherheitsmaßnahmen auf wenige, wichtige Punkte konzentriert werden und an diesen Stellen professionell und entsprechend dem Stand der Technik realisiert werden.

Die Bürgerinnen und Bürger werden die neuen Kommunikationsmöglichkeiten nur dann nutzen, wenn sie ihnen vertrauen! Sie erwarten zu recht, dass ihre Daten vor unbefugtem Zugriff oder Manipulation sicher sind und die Vertraulichkeit gewahrt bleibt. Die Arbeit hieran ist für mich eine der wichtigsten Voraussetzungen für den Erfolg von E-Government. Das gilt natürlich nicht nur für das Angebot von Nordrhein-Westfalen, sondern auch für andere Verwaltungen. Ich hoffe deswegen, dass die intensive fachliche Kooperation, die wir bei E-Government mit dem kommunalen Bereich sowie anderen Bundesländern und der Bundesverwaltung eingegangen sind, auch auf dem Gebiet der Sicherheit von IT-Infrastrukturen fortgesetzt wird.

Um die Datensicherheit in Verwaltungsprozessen zu gewährleisten, hat NRW schon früh auf Signaturen und Verschlüsselung gesetzt. Innovative Lösungen wie das OSCI-Protokoll und die Governikus-Plattform sind wichtige Komponenten unserer E-Government-Infrastruktur. Und ich bin überzeugt, dass die Frage der IT-Sicherheit zukünftig noch stärker als bisher bei diesen Kooperationen in den Mittelpunkt rücken wird.

Der größte Teil der elektronischen Kommunikation, der von Behörden und Einrichtungen der Landesverwaltung ausgeht, bleibt innerhalb der Landesverwaltung oder richtet sich übergreifend an andere Verwaltungen. Hierfür hat Nordrhein-Westfalen bereits mit der erfolgreichen Umsetzung des IT-Konzeptes 2002 eine hervorragende Infrastruktur für effizient organisierte Verwaltungsprozesse geschaffen. Neben der Ausstattung von Arbeitsplätzen mit moderner IT wurde die flächendeckende Vernetzung der Behörden und Einrichtungen des Landes vollzogen.

Dabei verfolgt Nordrhein-Westfalen die Strategie eines vom Internet separierten Verwaltungsnetzwerks mit zentralen Sicherheitsvorkehrungen, die durch lokale Schutzmaßnahmen in

den Häusern ergänzt werden. Das vom Landesamt für Datenverarbeitung und Statistik betriebene Landesverwaltungsnetz bietet allen Ressorts eine auf modernen Technologien basierende Kommunikationsinfrastruktur. Daran angeschlossene Behörden und Einrichtungen des Landes stellen einen Sicherheitsverbund dar, dessen verbindliche Richtlinien in allen angeschlossenen Stellen Gültigkeit besitzen. Eine Verbindung zum Internet wird nur an drei Stellen hergestellt, die in besonderer Weise gesichert sind. Diese Kommunikation in einem geschlossenen Netzwerk erfüllt die Forderung der Bürgerinnen und Bürger nach einem vertrauensvollen Umgang mit den teils hochsensiblen Daten innerhalb der Landesverwaltung. Dies geht soweit, dass in dem besonders sicherheitsempfindlichen Bereich des Verfassungsschutzes, der in meinem Hause angesiedelt ist, die physikalische Abschirmung des Netzes als ultima ratio praktiziert wird.

Die gleiche Sorgfalt müssen wir auch bei der Übermittlung von Daten an Behörden und Einrichtungen außerhalb der Landesverwaltung beachten. Daher nutzen wir für diese Kommunikation das von der Europäischen Union ins Leben gerufene und mit besonderen Sicherheitsfunktionen versehene europäische Verwaltungsnetzwerk TESTA (Trans European Services for Telematics between Admnistrations). Die Kommunen in Nordrhein-Westfalen nehmen bundesweit einen Spitzenplatz in der Vernetzung über TESTA ein. Derzeit ist es möglich, annähernd 70% der Kommunen und Kreise in NRW auf diesem Weg zu erreichen. Aus meiner Sicht ist es wünschenswert, die Kommunikation zwischen Landes- und Kommunalverwaltung in einem gemeinsamen Netz zu realisieren. Die Vorteile geschlossener Netze sind angesichts zahlreicher Störfälle und Attacken im Internet meines Erachtens offenkundig.

Wie bereits dieser kurze Abriss der IT-Vorhaben der Landesverwaltung zeigt, stellen die Ansprüche an die IT-Sicherheit eine sich dynamisch verändernde Herausforderung dar. Dieses Bewusstsein prägt das Handeln des Innenministeriums Nordrhein-Westfalen als Anbieter von Informationsnetzen und Kommunikationsinfrastrukturen.

Mein Haus ist aber nicht nur in dieser Rolle unmittelbar von dem Thema des Kongresses betroffen. Wie ich eingangs angesprochen habe, sind durch die moderne IT neue Gefährdungspotenziale unterschiedlichster Art entstanden. Diese genau zu beobachten, ihre Auswirkungen realistisch einzuschätzen und sie zu bekämpfen ist gerade auch für den Schwerpunkt der Verantwortung meines Hauses - dem hochsensiblen Bereich der inneren Sicherheit - von besonderer Bedeutung!

Die Veränderungen durch die breitere Nutzung moderner IT wurden bereits frühzeitig in der Kriminalität sichtbar. Das kriminelle Eindringen in fremde Computersysteme und das Sabotieren von Daten und Anlagen zieht nicht selten spektakuläre Strafverfahren nach sich. Wir alle erinnern uns noch an den I-Love-You-Virus, der im globalen Datenstrom in Stunden um die Welt ging. Allerdings muss man heute kein begabter Informatikstudent mehr sein - wie es der Urheber des eben genannten Virus´ war - um eine immens schädliche Anwendung zu programmieren. Dank bedienerfreundlicher Software gelingen Viren, Würmer und Trojaner auch schon dem weniger erfahrenen DV-Anwender. Dennoch ist der Anteil dieser Straftaten - gemessen an der Gesamtkriminalität - gering, der durch sie verursachte Schaden allerdings oft gewaltig. Tatsächlich haben die Informationstechnologien nur wenige Formen wirklich neuer Kriminalität entstehen lassen. Vielmehr wurden in den traditionellen Bereichen der Kriminalität viele Tatbegehungsformen einfach digitalisiert. Dadurch haben sich Ausmaß und Qualität dieser Delikte teilweise erheblich verändert. Die zunehmende Verbreitung von E-Commerce, Business-to-Business-Geschäften oder Finanztransaktionen mit "Cyber-Money" ziehen neue Spielarten des Betruges bzw. der Wirtschaftskriminalität nach sich. Täter treffen z.B. bei Online-Auktionen auf ein unbegrenztes Potenzial an möglichen Opfern. Schwarze Geldströme werden im uferlosen Netz mit Mausklicks um die ganze Welt geleitet. Erpresserforderungen werden via E-Mail gestellt und müssen aufwändig zurückverfolgt werden. Auch die Leistungsfähigkeit der digitalen Telefonnetze - seien sie nun fest oder mobil - wird von Straftätern inzwischen umfassend für ihre Tatkommunikation genutzt.

Ein weiteres Beispiel dafür, wie sich der alltägliche Einsatz von IT auch auswirken kann, ist das sogenannte "Homejacking". Nachdem heutzutage mehr und mehr Fahrzeuge über elektronische Wegfahrsperren verfügen, ging der Diebstahl von Kraftfahrzeugen erwartungsgemäß zurück. Gleichzeitig ist die Zahl der Wohnungseinbrüche gestiegen, die allein vorgenommen werden, um an die Zündschlüssel von hochwertigen Fahrzeugen zu gelangen.

Straftaten, die unter Einsatz der modernen IT begangen werden, machen sich häufig die virtuelle Grenzenlosigkeit des Netzes zu Nutze. Staatsgrenzen halten zwar Computer und Internet nicht zurück, errichten damit aber hohe Hürden für die Strafverfolgungsbehörden. Inkriminierte Inhalte können heute ohne besonderen Aufwand in das Internet gestellt oder anonym heruntergeladen werden. Dadurch steigt auch die Verbreitung von extremistischer Propaganda und Kinderpornografie. Viele Straftaten werden über einen Server oder Rechner abgewickelt, der nicht auf deutschem Staatsgebiet installiert ist. Täter nutzen bewusst den Umstand aus, dass bestimmte Tathandlungen im Aus-lind nicht oder nur mit geringer Rechtsfolge unter

Strafe gestellt sind. Die bereits bestehenden Vereinbarungen zur internationalen Rechtshilfe und Übereinkommen zur Harmonisierung der Rechtsgrundlagen bei der Bekämpfung von Kriminalität im Internet müssen noch effektiver gestaltet werden. Ich trete dafür ein, weiterhin auf supranationale Initiativen hinzuwirken, mit denen besonders schädliche Formen der Computerkriminalität international geächtet und damit leichter verfolgbar werden. Ein Weg dorthin ist die Normierung der sogenannten "Preservation Order" in möglichst vielen Staaten. Sie ermöglicht es einem ersuchten Staat, bei einem tatrelevanten Provider im eigenen Hoheitsgebiet, die meist nur kurzfristig gespeicherten Verbindungsdaten einer Netz-Straftat vorläufig zu sichern bis das begleitende, aber zeitintensive Rechtshilfeverfahren abgeschlossen ist.

Dies alles macht deutlich, welche Herausforderung die zunehmende Verbreitung moderner Informationstechniken für die tägliche Arbeit der Polizei darstellt. Täterermittlung und Beweissicherung müssen sich an der IT ausrichten. Das setzt natürlich ein doppelt spezialisiertes Fachwissen der Ermittlungsbeamten und eine moderne Ausstattung mit Hard- und Softwarekomponenten voraus. Computerkriminalität wie zum Beispiel Kapitalanlagebetrug, Wirtschaftskriminalität, Produktpiraterie und ausspähende oder sabotierende Hackerangriffe auf Datennetze von Unternehmen erfordern entsprechende Präventionsstrategien. Potenzielle und tatsächliche Opfer erwarten traditionell, von der Polizei, fachlich beraten zu werden, wie sie sich vor derartigen Straftaten schützen können. Angesichts der geringen Halbwertzeit von IT-Fachwissen werden dabei auch hohe Anforderungen an die polizeiliche Aus- und Fortbildung gestellt.

Wir in Nordrhein-Westfalen passen die polizeilichen Ermittlungs- und Präventionspotenziale diesem Trend an. Die Bekämpfung der Computerkriminalität in den Kreispolizeibehörden wurde neu organisiert. Neu geschaffene Fachdienststellen erhalten eine Ausstattung mit moderner Hard- und Software, die regelmäßig aktualisiert wird. In großen Behörden vorgesehene Informations- und Service-Center werden u.a. den notwendigen Wissenstransfer unter den Kreispolizeibehörden des Landes sicherstellen. Und ein breit angelegtes, stufenförmiges Fortbildungskonzept wird dafür sorgen, dass alle betroffenen Polizeibeamtinnen und -beamten aufgabenorientiert in der Bekämpfung der Computerkriminalität fortgebildet werden. Herr Schürmann vom Landeskriminalamt NRW wird Ihnen zu dem Maßnahmenkatalog in seinem Vortrag "Verfolgung und Verhütung von Computerkriminalität durch eine moderne Polizei" weitere interessante Einzelheiten vermitteln.

Ich setze in Fragen der Netzsicherheit und Verbrechensbekämpfung auch auf eine vertrauensvolle Zusammenarbeit mit Ihnen und den Institutionen, die Sie vertreten. Wie ich eingangs sagte, bin ich der festen Überzeugung, dass Partnerschaften und Netzwerke die einzige Antwort auf die gegenwärtigen und zukünftigen technologischen Herausforderungen sind. Als ein erfolgreiches Beispiel für eine solche "Public-Private-Partnership" - wie es so schön neudeutsch heißt - wird Ihnen der Leiter der Spionageabwehr aus meinem Hause, Herr von Bauer, gleich im Anschluss an die Pause, die "Sicherheitspartnerschaft zur Bekämpfung von Wirtschaftsspionage und Wirtschaftskriminalität" vorstellen.

Lassen Sie mich nur soviel dazu bemerken: Hier ist es gelungen, nachrichtendienstliches und polizeiliches Wissen über die verschiedenen Erscheinungsformen der Angriffe und deren Kontrollmöglichkeiten mit Ihren Kenntnissen und Erfahrungen zusammenführen. Dies wird langfristig allen Betroffenen und insbesondere den Bürgerinnen und Bürgern in unserem Land von großem Nutzen sein.

Wenn man die dynamische Entwicklung der modernen IT betrachtet, drängt sich die Frage auf "was wird uns die Zukunft bringen?". Mit großem Interesse habe ich gesehen, dass dieser Kongress sich auch mit den Begriffen Cyber-Terrorismus, Cyberwar und Information Warfare beschäftigt. Mein Eindruck ist, dass diese Themen häufig in der Öffentlichkeit behandelt werden, ohne dass es eine zuverlässige Aussage darüber gibt, wie real diese Gefahren tatsächlich sind. Allein die theoretische Möglichkeit wird von vielen als hineichende Grundlage dafür angesehen, Schreckensszenarien über Terroranschläge, von Menschenhand ausgelöste Katastrophen und sogar einen nächsten Weltkrieg zu zeichnen. Als Beleg hierfür werden häufig Äußerungen von Sicherheitsexperten in den USA beigezogen. Nach deren Einschätzung sollen Terroristen bzw. Extremisten in der Lage sein, mit Hilfe des Internets Energieversorgungs- und Kommunikationsnetze bzw. andere kritische Infrastrukturen unserer Gesellschaft auszuschalten.

Es gibt aber auch andere Stimmen, die behaupten, derartige Szenarien seien eher irreal. Einzelpersonen seien heutzutage gar nicht in der Lage, solche Angriffe zu entwickeln.

Mit diesen widersprüchlichen Einschätzungen setzen sich zur Zeit die Sicherheitsbehörden von Bund und Ländern in gemeinsamen Arbeitsgruppen und in enger Zusammenarbeit mit der freien Wirtschaft intensiv auseinander. Die nachrichtendienstlichen Erkenntnisse Nordrhein-Westfalens sprechen jedenfalls aktuell nicht dafür, dass Extremisten oder Terroristen

das Internet in einem als reale Bedrohung zu empfindenden Maße als Waffe gegen technische Systeme nutzen. In Einzelfällen hat es allerdings auch derartige Versuche bereits gegeben. Bei der in den Kreisen der Antiglobalisierungsbewegung so genannten "Battle of Seattle" sollen Computer-Hacker aus Anlass der im November 1999 dort durchgeführten Welthandelskonferenz die Steuerungsrechner für die Anlagen im Straßenverkehr manipuliert haben. Der Ausfall der Ampelanlagen ermöglichte es den Demonstranten, durch Tumulte auf den Straßen den Abbruch der Konferenz zu provozieren. Allerdings ist der grundsätzliche Eindruck entstanden, dass die Möglichkeiten begrenzt sind, ein wirksames "war-fare" durchzuführen. Dies zeigt sich z.B. an dem vergeblichen Versuch von Linksextremisten, den Server der Lufthansa, als Airline, die an Abschiebungen mitwirkt, durch DOS-Attacken (Denial of Service = extrem gehäufte E-mails) zu blockieren.

Auf der anderen Seite wird das Internet aber auch von Extremisten aller Art zur kostengünstigen, schnellen, internationalen Kommunikation und Agitation genutzt, insbesondere, wenn sie - wie z.B. das terroristische Netzwerk um Usama bin Laden - weltweit tätig sind. Diese Aktivitäten werden selbstverständlich von den Nachrichtendiensten intensiv beobachtet.

Im Zusammenhang mit der Bedrohung durch Terroranschläge darf ein Thema nicht unerwähnt bleiben: Der 11. September 2001! Vor etwa drei Wochen hat er sich zum zweiten Mal gejährt. Das Datum hat sich in unseren Köpfen festgesetzt. Es ist unvergesslich, weil sich damit Urängste realisiert haben. Der 11. September, dessen terroristische Nachbeben und die daraus entstandenen politischen Konsequenzen haben die Welt verändert. Sie haben uns allen vor Augen geführt, wie verletzlich unsere Gesellschaft ist.

Das Bild der von Menschenhand geschaffenen Katastrophe steht uns noch allen deutlich vor Augen. Zum Schutze der Bevölkerung vor den Bedrohungen durch den islamistischen Terrorismus sowie zu dessen Bekämpfung war es notwendig, die Sicherheitsbehörden des Landes zeit- und sachgerecht auf die neue Situation einzustellen. Die Landesregierung hat mit den Sicherheitspaketen I und II auf diese Bedrohung unverzüglich und angemessen reagiert. Hinter den Sicherheitspaketen verbergen sich allein für das aktuelle Jahr Investitionen in Höhe von 22 Millionen Euro. Mit diesem Geld werden bei Polizei und Verfassungsschutz u.a. zusätzliche Stellen geschaffen und insbesondere in moderne Informationstechnologie investiert. Ein gutes Beispiel dafür, wie der Einsatz von IT den Staat unterstützt.

Als eine weitere Folge aus den Ereignissen des 11.09.2001 wurde der staatliche Katastrophen- und Zivilschutz überprüft. Letzterer soll durch geplante Gesetzesänderungen der gewandelten Gefahrensituation angepasst werden. Für den Katastrophenschutz hat die Landesregierung Nordrhein-Westfalen das "Zukunftskonzept Großschadensabwehr" im April d.J. beschlossen, das eine Fortentwicklung der bestehenden Systeme vorsieht. Auch hier erweist sich die IT als hilfreich. Zwecks einer optimalen Koordinierung wird Nordrhein-Westfalen den Aufbau eines landesweiten Informations- und Kommunikationssystems in Ergänzung zu der Ressourcendatenbank des Bundes in Angriff nehmen. Eines muss uns jedoch immer klar sein: Eine gesetzliche Regelung aller zukünftigen Gefahren und eine 100%-ige Sicherheit kann es und wird es niemals geben.

Anrede,

am Schluss meiner Rede möchte ich wieder auf den Anfang zurückkommen. Der rasante Fortschritt in der Informationstechnologie und der damit verbundene Wandel der Bedrohungen machen es notwendig, vorhandene Sicherheitskonzepte ständig auf ihre Tauglichkeit hin zu untersuchen und anzupassen. Neue Arbeitsformen, neue Technologien und nicht zuletzt auch neue Angriffsmethoden sorgen für eine große Dynamik. Die Anforderungen an Abwehrmaßnahmen werden steigen. Und mehr denn je ist es notwendig, präventive Maßnahmen zu entwickeln.

Der Erhalt und Ausbau einer sicheren IT-Infrastruktur ist keine leichte und auch keine billige Aufgabe. Zur Abwehr der Gefahren ist eine intensive Zusammenarbeit aller Beteiligten erforderlich, die alle gesellschaftlichen Kräfte - öffentliche und private - Staat und Wirtschaft - einbinden muss. Ich würde mich sehr freuen, wenn dieser Kongress den Weg für neue Netzwerke und Partnerschaften bereiten würde. Unter anderem deshalb werde ich - und ich denke, ich spreche auch für die Mitarbeiter meines Hauses - den Verlauf dieses Kongresses mit großem Interesse verfolgen.

Abschließend möchte ich mich bei Ihnen allen dafür bedanken, dass Sie auf dieser Veranstaltung gemeinsam daran arbeiten wollen, Informationstechnik und die damit verbundenen Prozesse sicherer zu gestalten und wünsche dem Kongress einen guten Verlauf und eine hohe Resonanz in der Öffentlichkeit.