Homeland Security

- Auftrag
- Entstehung des Departments of Homeland Security
- Aufgaben und Entwicklungen
- Drei Gesetze
- Fallbeispiele
- Fazit

Auftrag (1/3)

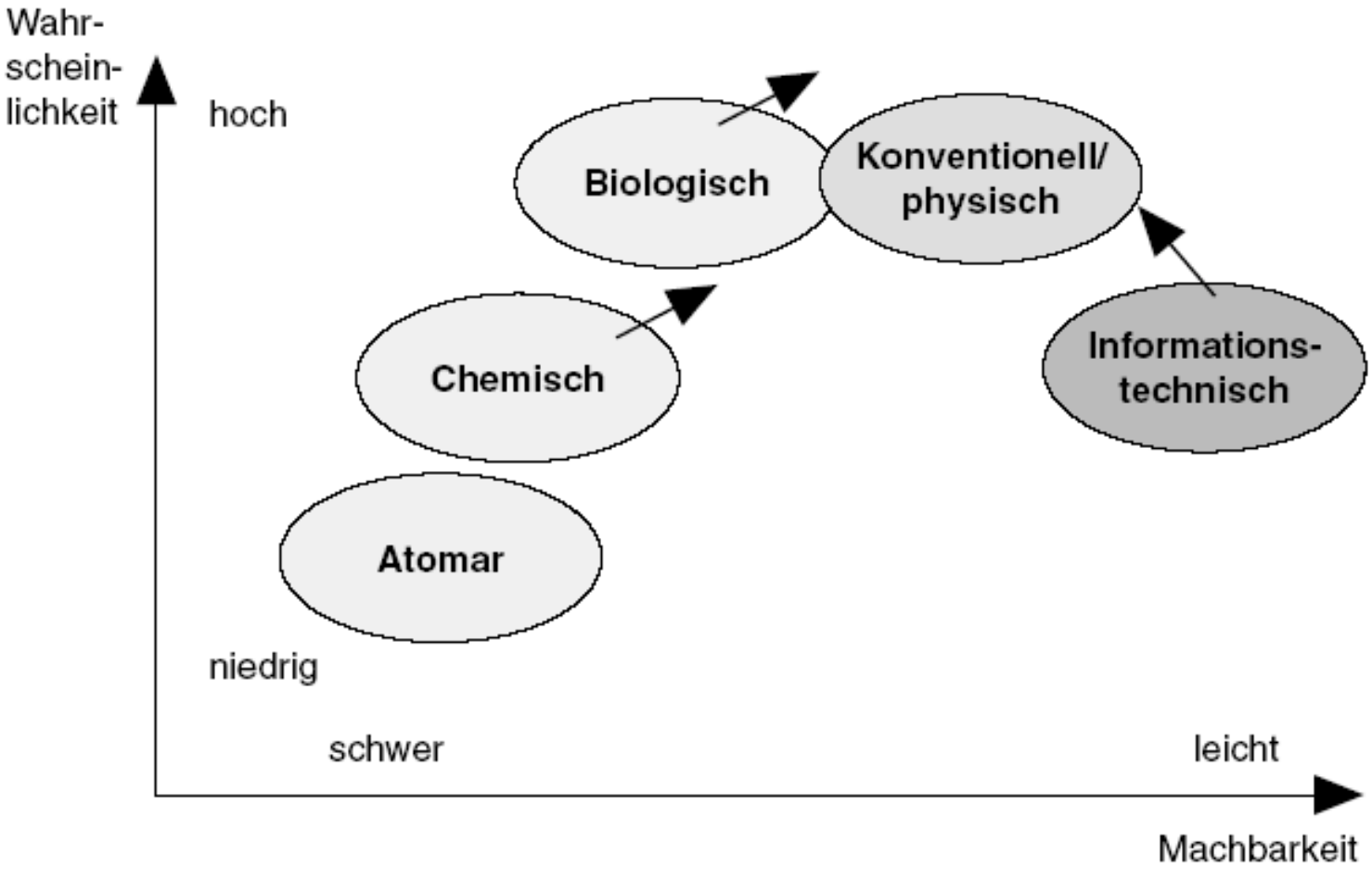
- Konventionelle Formen von Anschlägen sind meistens mit einem hohen Aufwand verbunden und ohne entsprechendes Budget nicht durchführbar

- Angriffe im elektronischen Bereich sind leichter und anonymer durchführbar und häufig auf den ersten Blick nicht als solche erkennbar

- Wirkung auf ganze Volkswirtschaften fataler als bei anderen Arten von Angriffen

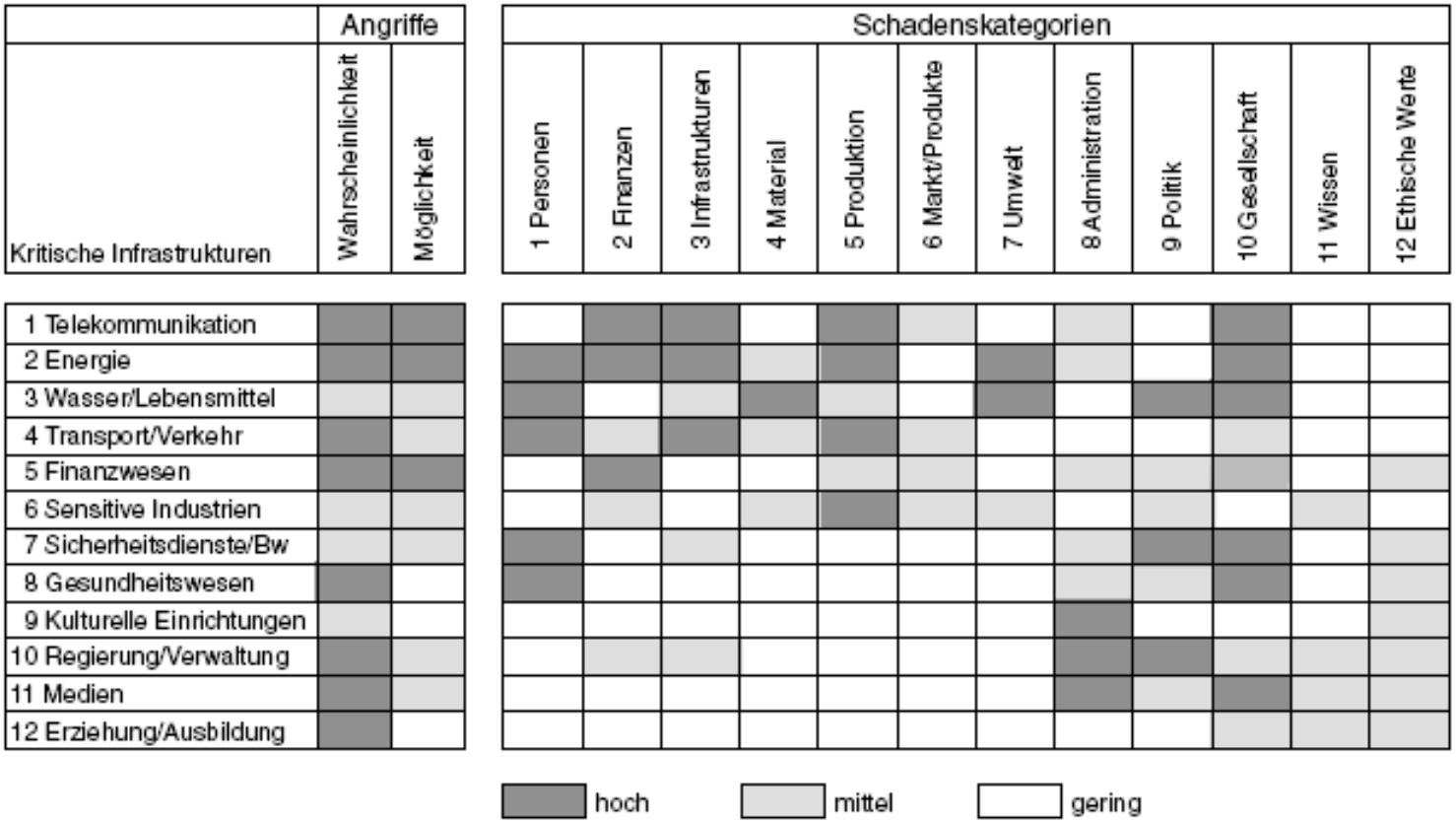
Auftrag (2/3)

- Übersicht Bedrohungstrends



Auftrag (3/3)

- Infrastrukturen, Bedrohungen und Schadenskategorien



Entstehung des DHS (1/3)

- Anschläge auf World Trade Center ’93 und Alfred P. Murrah Federal Building in Oklahoma City ’95 zeigen das erstemal Verwundbarkeit der USA im eigenen Land

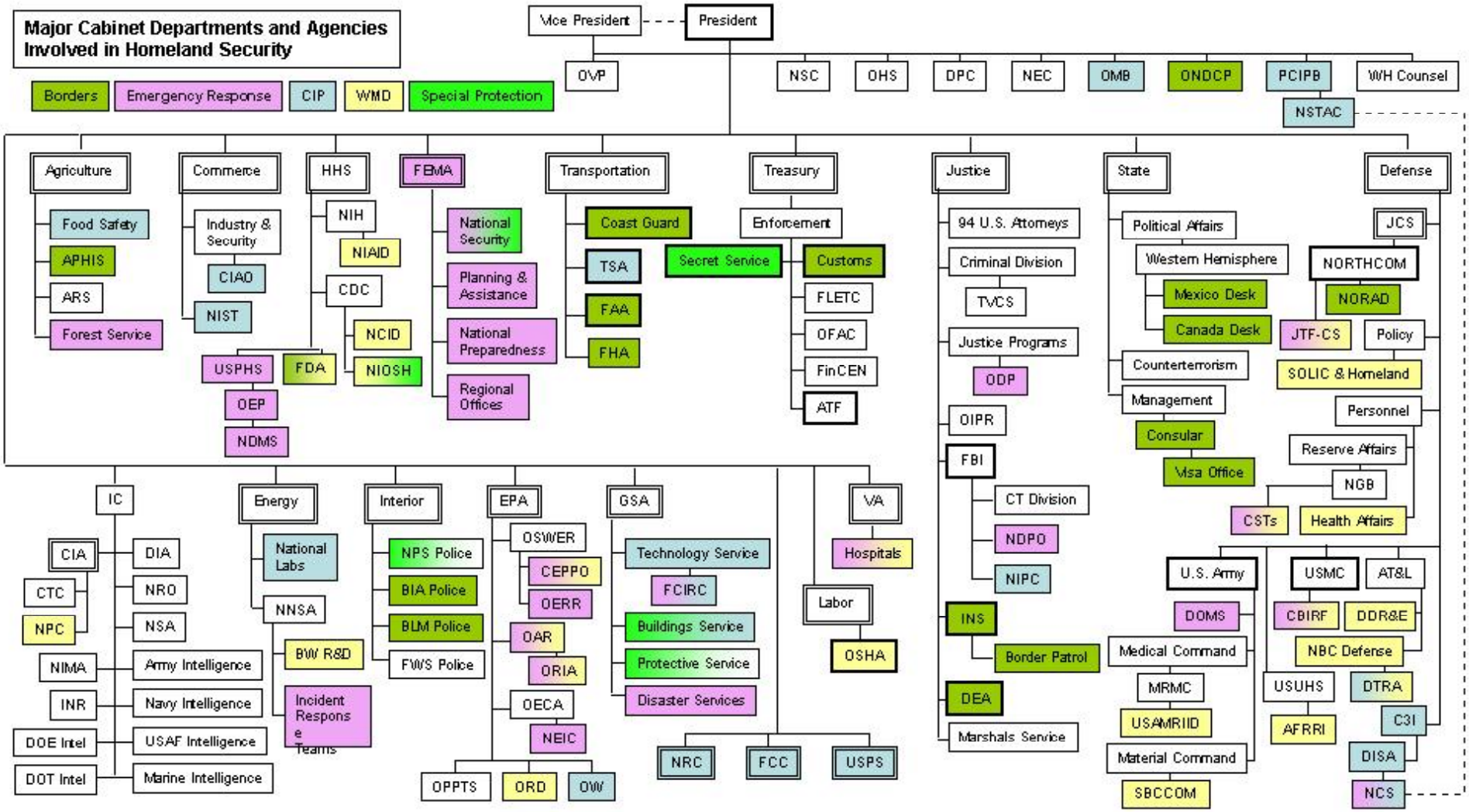
- Keine zentrale Stelle um auf Anschläge im vor- wie nachhinein adäquat zu reagieren

- Clintons erste Schritte
  - **State Department** - terroristischer Bedrohungen im Ausland
  - **FBI** - terroristische Bedrohungen im Inland
  - **Federal Emergency Management Agency** - Krisenmanagement nach einem Anschlag
  - **Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism** – Koordinierung aller Maßnahmen ohne gesetzlich verankerte Vollmachten

  reduzierten Verantwortlichkeiten nur unwesentlich

Entstehung des DHS (2/3)

An der Thematik „Homeland Security“ beteiligte Abteilungen



Entstehung des DHS (3/3)

- Nach dem 11.9.2001 hatte das Weiße Haus eine groß angelegte Umstrukturierung innerhalb der Administration eigentlich abgelehnt und sich auf die Einrichtung eines

- "Office of Homeland Security" wird gegründet

- Druck aus dem US-Kongress / Bekannt werden vermeintlicher Versäumnisse von FBI und CIA im Vorfeld der Anschläge führten zu einem Stimmungswandel

- Am 19.11.2002 stimmte der US-Senat (90 Ja, 9 Nein, 1 Enthaltung) für den „Homeland Security Act 2002“, und somit für die Gründung des „Departments of Homeland Security“ (DHS)

Aufgaben und Entwicklungen (1/4)

- Zentrale Aufgaben
  - Vereitelung von Terroranschlägen in den USA
  - Reduzierung der Verwundbarkeit gegenüber Terrorismus
  - Schadensbegrenzung und -behebung im Fall von Terroranschlägen

- Vier Abteilungen, die insgesamt 22 Behörden aus anderen Ministerien zusammenfassen
  - The Border and Transportation Security directorate
    - Sicherheit der amerikanischen Grenzen
    - Transportinfrastruktur
    - Hoheitsgewässer
  - The Emergency Preparedness and Response directorate
    - Koordinierung aller Vorkehrungen, die auf Bundes-, Landes- und Gemeindeebene zur Vorbereitung bzw. Reaktion auf mögliche Terroranschläge stattfinden
  - The Science and Technology directorate
    - Schutz der Bevölkerung und Infrastruktur gegen Angriffe mit chemischen, biologischen oder nuklearen Waffen
    - Unterabteilung für Forschung und Entwicklung, chemische Waffen und Substanzen, biologische Waffen und Substanzen sowie radiologisch/nukleare Waffen und Materialien

Aufgaben und Entwicklungen (2/4)

- The Information Analysis and Infrastructure Protection directorate
  - Bewertung terroristischer Bedrohungsszenarien
  - Beurteilungen der Verwundbarkeit kritischer Infrastruktureinrichtungen
  - Bündelung sonstiger Informationen zum Thema Terrorismus, die die amerikanische Intelligence Community hervorbringt

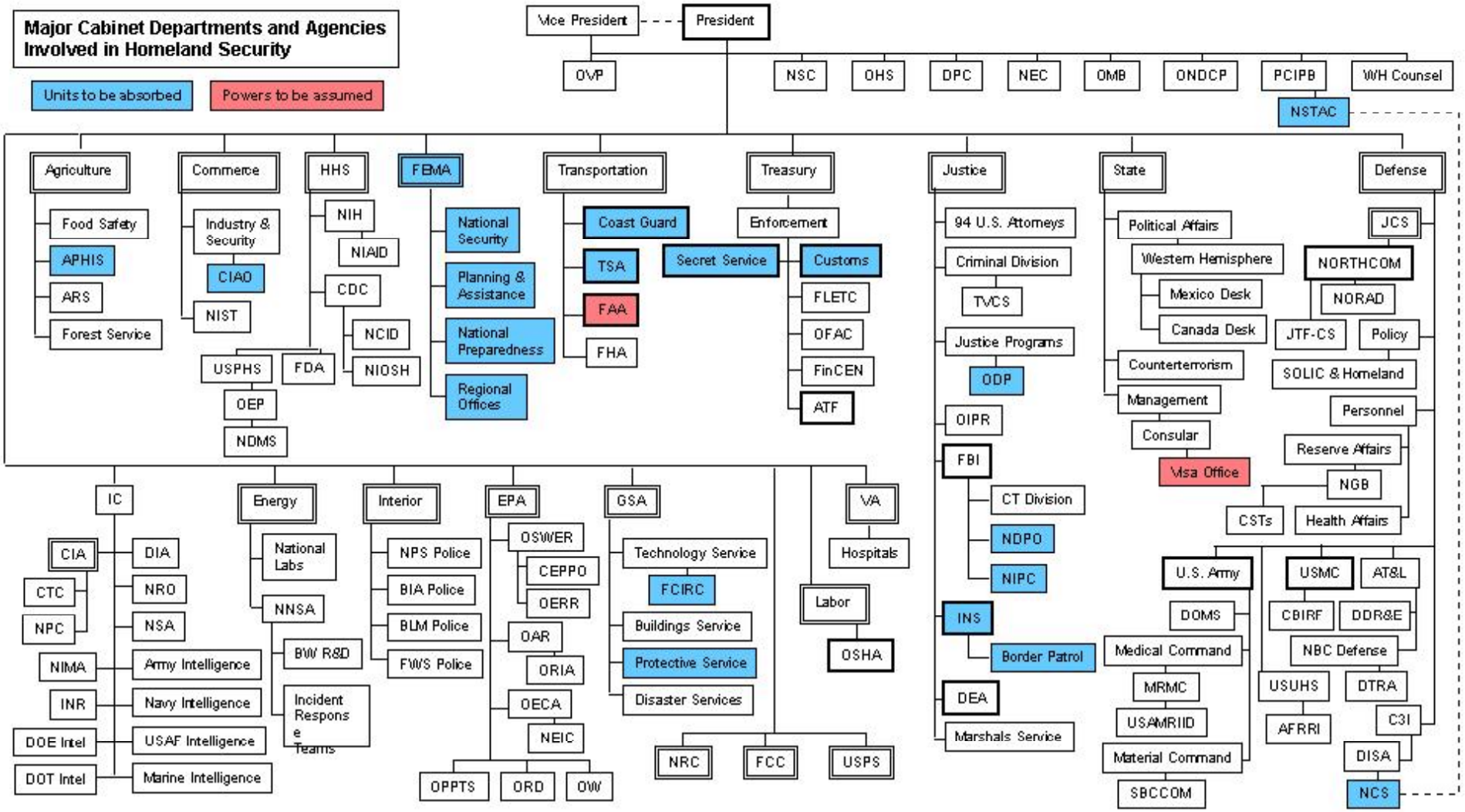
- Einrichtung des Departments und die Transferierung der 22 Unterbehörden sollte bis zum 30.09.2003 abgeschlossen sein

- 170.000 Mitarbeiter

- Jährliches Budget von US$ 36.2 Mrd.

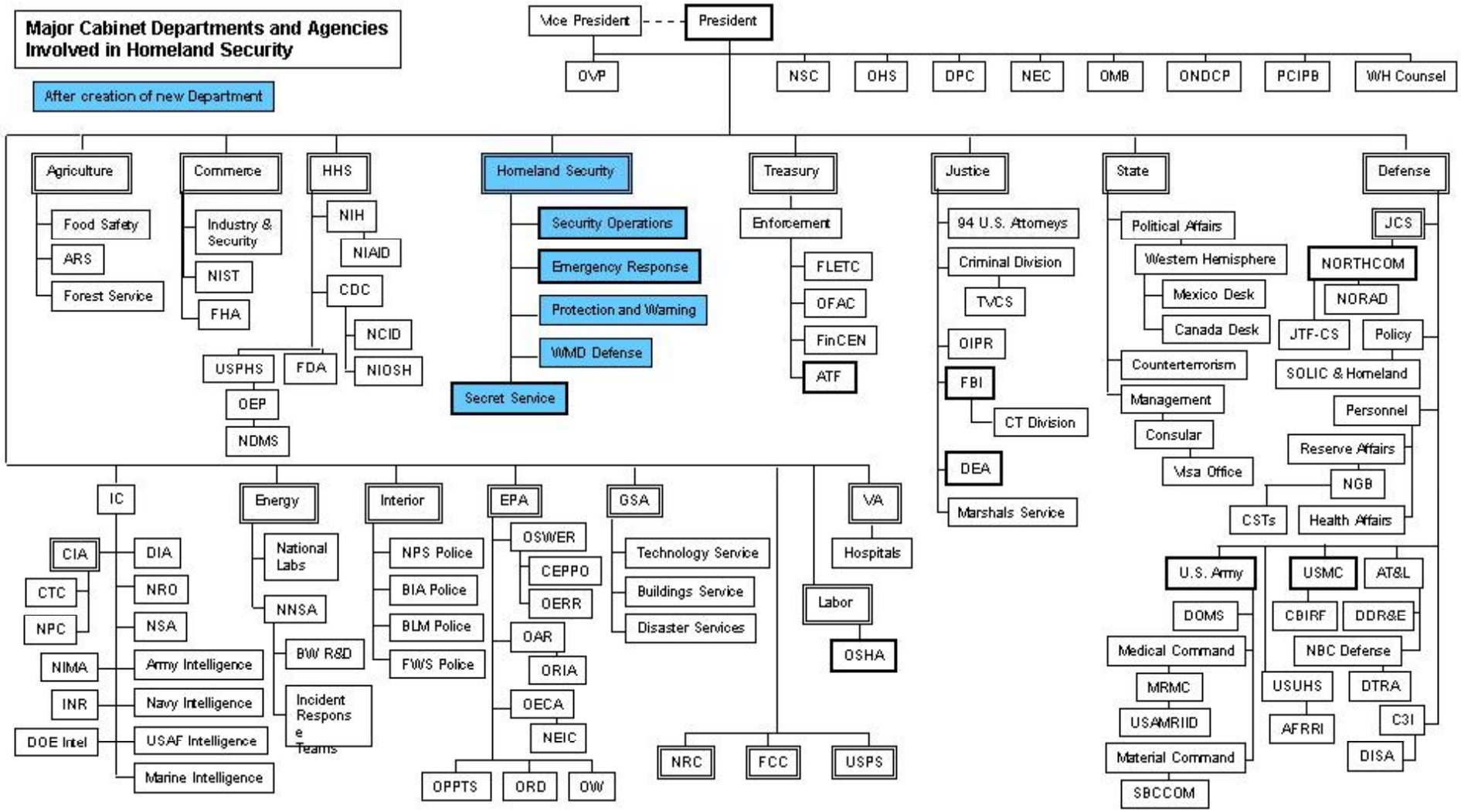
Aufgaben und Entwicklungen (3/4)

Abteilungen die vom DHS aufgenommen werden



Aufgaben und Entwicklungen (4/4)

Regierungsstruktur nach der Gründung des DHS



Informationsfluss

- Gesetzliche Verpflichtung unaufgefordert dem DHS Informationen über potentielle Bedrohungen zur Verfügung zu stellen.

- Dieser Informationsfluss soll horizontal (Bundesbehörden weit) aber auch vertikal (von den Kommunen über Land bis hin zum Bund) verlaufen, die ebenfalls die Privatwirtschaft mit einschließen soll.

- Das „National Infrastructure Protection Center“ (NIPC), ursprünglich beim FBI gegründet, entwickelt gemeinsam mit der Industrie den „InfraGuard“, eine sichere Kommunikationsplattform zwischen Regierung und Privatwirtschaft.

Sensible Angriffsziele

Das DHS ist vor allem auch für den Schutz der kritischen Infrastruktur zuständig. Beschützt wird alles was auch nur im entferntesten als terroristisches Angriffsziel attraktiv erscheinen könnte.

- Öffentliches Transportwesen (Flughäfen, Bahnhöfe, ...)
- Denkmäler und sonstige Wahrzeichen
- Großveranstaltungen (Superbowle)
- Kraftwerke, Raffinerien, Dämme, ...
- Wasseraufbereitungsanlagen, Agrarwirtschaft, ...
- ...

Reaktion (1/2)

Neben dem Ziel Terroranschläge zu verhindern gilt es auch auf einen erfolgten Anschlag schnell zu reagieren um Auswirkungen möglichst gering zu halten. Hierfür wurden bereits Programme ausgearbeitet.

- Schulungsprogramme für Polizei, Feuerwehr und die Rettungsdienste.
- Biologische oder chemische Angriffe erfordern kurze Entwicklungs-dauer für Impfstoffe oder sonstige Medikamente sowie deren schnelle Verteilung.
- Autorisierte Personen müssen nach Zusammenbruch des leitungs-gebundenen Kommunikationsnetz einen priorisierten Zugriff auf das kabellose Netz erhalten.

Reaktion (2/2)

- Nach Cyberattacken müssen schnell Informationen über die Behebung von Virenbefall, Schließen der Sicherheitslücke oder Recoverymaß-nahmen zur Verfügung gestellt werden.

  – Neben dem NIPC informiert auch das Federal Computer Incident Response Center (FedCIRC) über aktuelle Virenwarnungen oder Sicherheitslücken in Software und stellt auf dem zivilen Sektor das Störungsvorfallmeldungs-zentrum dar.

  – Das FedCIRC bietet neben Statistiken über Cybercrime-Aktivitäten auch Analyse-Tools die Schwachstellen im eigenen Computernetz aufspüren und Patches zu deren Behebung an.

Der Cyberspace

- Neben der physisch schutzbedürftigen kritischen Infrastruktur die einem Anschlag zum Opfer fallen könnte existieren auch virtuelle Angriffsobjekte in Form von Rechner- bzw. Kommunikationsnetzen jeglicher Art.

- Diese sind deshalb besonders gefährdet, da sie auch von außerhalb des Landes über das Internet als potentielle Ziele erscheinen.

- Veröffentlichung der „National Strategy to Secure Cyberspace“ im Februar 2003 bestehend aus 5 Prioritätsebenen:

  - Schnelles staatliches Reagieren auf Attacken im Cyberspace.
  - Ein staatliches Sicherheitsprogramm zur Verminderung von Bedrohungen und Schwachstellen im Cyberspace.
  - Ein staatliches Trainingsprogramm sowie schaffen eines Cyberspace-Sicherheits-Bewusstseins.
  - Sicherung des Regierungs-Cyberspaces.
  - Sicherheit auch auf internationaler Ebene im Cyberspace schaffen.

Entwicklungen zum Schutz des Cyberspace (1/2)

- "Global Early Warning Information System" GEWIS
  - Vom National Communications System (NCS) entwickelt.
  - Daten der Provider über den Zustand ihrer jeweiligen Infrastruktur in Echtzeit zu sammeln und zu analysieren um ungewöhnliches oder verdächtiges Verhalten erkennen und dem DHS melden zu können.
  - also **nicht** Terabytes an Daten sammeln, um sie dann zu analysieren, wie dies bei TIA (Total/Terror Information Awareness) der Fall ist.
  - Es soll also nicht zu Verletzungen des Datenschutzes kommen.
  - GEWIS arbeitet schon jetzt mit den wichtigsten Internet-Providern zusammen und wurde von VeriSign im Auftrag des DHS auf allen 13 Root-Servern installiert.
  - Mit einer finalen Version ist aber erst im März 2004 zu rechnen.

Entwicklungen zum Schutz des Cyberspace (2/2)

- “Cyberspace Warning Intelligence Network” (CWIN)
  - Ebenfalls vom National Communications System (NCS) entwickelt.
  - Ein separates auf IP basierendes sicheres Datennetzwerk für Notfälle.
  - Kann von der US-Regierung und ausgewählten Usern aus Bereichen der Industrie unabhängig vom öffentlichen Internet genutzt werden.

- Auf kommunaler Ebene gibt es NET Guards die das Internet nach möglichen Bedrohungen durchsuchen, diese arbeiten zumeist ehrenamtlich.

Drei Gesetze (1/2)

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

  USA PATRIOT ACT 2001

  – Verschärfte Regelungen zur Art der Abwehr terroristischer Angriffe und derer Bestrafung
  – Ändert die Möglichkeiten Personen aus Verdachtsgründen festzuhalten
  – Regelt z.B. das Strafmass für Datenkriminalität. Hierbei muß die Straftat nicht von US Hoheitsgebiet ausgeführt werden, vielmehr genügt es wenn die relevanten Daten über Grund und Boden der USA transferiert werden.

- Homeland Security Act 2002
  – Gesetz zur Einrichtung des Departments of Homeland Security und die Umstrukturierungen weiterer Departments.
  – Enthält darüber hinaus den „Cyber Security Enhancement Act“.

Drei Gesetze (2/2)

- Cyber Security Enhancement Act

  CSEA

  – Überwachen von Kommunikation ohne richterliche Genehmigung

  – Erfassung von Verbindungsdaten einschließlich der besuchten URLs oder der Email-Adressen

  – Bei Annahme einer Gefahr für Leib und Leben eines Menschen sogar Inhalte von Emails und anderen Dateien

  – Erhöhung des Strafmasses für Cyber Crime

    - Auf bis zu 20 Jahre bei unberechtigtem Eindringen in Computersysteme mit Folge einer (versuchten) schweren Körperverletzung und im Fall der Tötung eines Menschen auf ein lebenslangen Freiheitsentzug
    - Von 2 auf 10 Jahre Gefängnis bei unberechtigten Zugriff auf gespeicherte Daten

  – Unter Strafe gestellt wird jegliche "Werbung" für verbotene Abhörmittel, so dass diese nun auch Online-Werbung und die Verbreitung über das Internet mit einschließt

Die Flugdatenaffäre

- US Gesetz, das nicht amerikanische Fluggesellschaften dazu zwingt ihre Buchungssysteme für die Zollbehörden der USA zu öffnen

- Daten, die eingesehen werden sollen
  - normale Passagierdaten
  - Kreditkartennummern + Ablaufdatum, Mietwagenreservierungen, Hotelbuchungen
  - die Art des bestellten Essens (vegetarisch, kosher, kein Schweinefleisch)
  - Teilweise E-Mail Adressen und Telefonnummern, sofern vorhanden

- Data-Mining-System CAPPS/CAPPS II verarbeitet Daten und stuft jeden Passagier nach seiner „Gefährlichkeit“ ein

- Daten sollen sieben Jahre gespeichert und noch nicht spezifizierter Weiterverarbeitung zugeführt, und danach für weitere acht Jahre in einer "Datei der gelöschten Datensätze" (deleted record file) aufbewahrt werden

Stromnetz als Teil der sensiblen Infrastruktur (1/2)

- 14. August 2003: 21 Kraftwerke gingen innerhalb von drei Minuten vom Netz (Der größten Stromausfall in der Geschichte der USA).
- Das DHS meisterte die Bewährungsprobe teilweise:
  - Sofortiges Einsetzen von Luftüberwachungsjets.
  - "Crisis Action Team" war innerhalb von Minuten zusammengestellt, das die Infrastrukturen nun rund um die Uhr nach verdächtigen Mustern überwachte. Ungewöhnliches Verhalten in den verschiedenen Versorgungs- und Kommunikationsnetzen konnte überprüft werden.
  - DHS gibt bekannt: „Kein Terroranschlag! Kein Virus!“

- Warum versagten die Sicherheits- und Alarmsysteme der Stromversorger?
  - Control Area Operators (CAO) steuern die Anschlüsse ans Netz.
  - Die CAOs geben den Kraftwerken vor, wie viel Leistung sie in das Netz einzuspeisen haben. Bei einem Ausfall erfolgt erhöhte Einspeisung durch die anderen Stromerzeuger. Kann die Mehrleistung nicht aufgebracht werden, koppelt das CAO notfalls Versorgungsgebiete ab.
  - Wenn das nicht schnell genug erfolgt, trennen sich die Kraftwerke zum eigenen Schutz selbsttätig vom Stromnetz -> Blackout!

Stromnetz als Teil der sensiblen Infrastruktur (2/2)

Die Prozesssteuerung ist zwar autonom, allerdings findet die Kontrolle so genannter SCADA-Systeme welche zum Sammeln und Übertragen von Messwerten dienen, auf Windows- und UNIX-Rechnern statt.

Diese kommunizieren über IPSec-verschlüsselte VPNs via Internet. In diese Verbindungen kann man zwar nicht eindringen, allerdings können sie gestört werden. -> Die Folge wäre ein Ausfall der Bedienstationen. Da auf Störungen im allgemeinen manuell reagiert wird käme es zu folgenschweren Verzögerungen.

Zur Visualisierung und Überwachung der SCADA-Systeme wird eine einheitliche Schnittstelle für Kontrollsysteme verwendet die auf Microsofts COM/DCOM-Modell basiert, Technik mit dem Sicherheitsloch, das W32.Lovsan ausnutzt. Zwei Tage vor dem großen Blackout hatte sich der Wurm Lovsan über das Internet verbreitet .

In allen Warnungen zum Schutz vor Lovsan wurde empfohlen, Port 135 auf den Firewalls zu sperren - genau der Port, über den OPC/DCOM kommuniziert. Blackout?

Glasfasernetz als Teil der sensiblen Infrastruktur

Geographie-Student Sean Gorman thematisiert in seiner Doktorarbeit die Verwundbarkeit des Glasfasernetzes der USA.

Aus öffentlichen, frei zugänglichen Quellen wie dem Internet oder von Kartografie-Unternehmen bezog er seine Informationen und erstellte damit eine Karte die die Knoten und Leitungswege des Netzes genau so darstellen wie sie auch verlegt wurden.

Es lässt sich blitzschnell nachvollziehen welches Unternehmen mit welchen Telekommunikationsfirmen zusammenarbeitet und wie diese Leitungen verlaufen.

Gorman hat zudem eine Software geschrieben, mit der sich für jeden in seiner Karte ausgewiesenen Ort berechnen lässt, welche Folgen ein Anschlag dort hätte. Somit könnten gezielte „Anschläge mit Heckenscheren“ ein Chaos mit milliardenschweren Folgen herbeiführen.

Fazit (1/2)

Das DHS ist eine sich noch im Aufbau befindende Behörde.

Kürzere Reaktionszeiten.

Datenschützer fürchten totale Überwachung.

Probleme beim Informationsaustausch zwischen Staat und Wirtschaft. Viele Unternehmen fürchten, dass Informationen in die Hände der Konkurrenz fallen.

Globale Auswirkungen wird es geben: Cybercrime-Konvention vom 8. November 2001

- 34 Staaten (auch die USA und Deutschland) die Cybercrime-Konvention unterzeichnet. Ratifiziert hat sie bisher 3 Staaten. Die Cybercrime-Konvention tritt in Kraft, sobald sie mindestens fünf Staaten, davon mindestens drei Mitgliedsstaaten, ratifiziert haben.

Fazit (2/2)

Im Dezember 2002 hieß es von der Deutschen Bundesregierung, sie wolle die Konvention in der laufenden Legislaturperiode umsetzen.

Otto Schily und Tom Ridge haben bei ihrem Zusammentreffen am 12. Juni in Washington, D.C., eine bilaterale Kooperation zum Schutz von Computer-systemen und Computernetzen beschlossen.

Am 19.11.2003 berichtete Heise, dass der US-amerikanische Präsident George W. Bush in einem Brief den Senat gebeten hat, die Cybercrime-Konvention des Europarates zu ratifizieren.