Das neue Verbot des Hackings

- Praktische Auswirkungen -

von RA Peter Voigt

Was wird vorgetragen?

- Grundzüge des Gesetzentwurfs
- Strafbarkeit von Hackertechniken
- Strafbarkeit sog. Hackersoftware
- Fernwirkungen (falls Zeit bleibt)

Was kann man mit- und nachlesen?

Fundstellen und neue Gesetzestexte

liegen am Schluß vorne beim Referenten aus

aktueller Stand (Ende Dez. 2006)

Bundestagsdrucksache 16/3656
http://dip.bundestag.de/btd/16/035/1603656.pdf

Stellungnahme CCC e.V.

http://www.ccc.de/press/releases/2006/20060925
/forderungen.xml

(bitte Link als eine einzige Zeile eingeben)

Bis wann sollte man *gewisse* Arbeiten beendet haben?

15.03.2007

Was soll der Gesetzesentwurf bewirken?

(Stand Ende Dez. 2006)

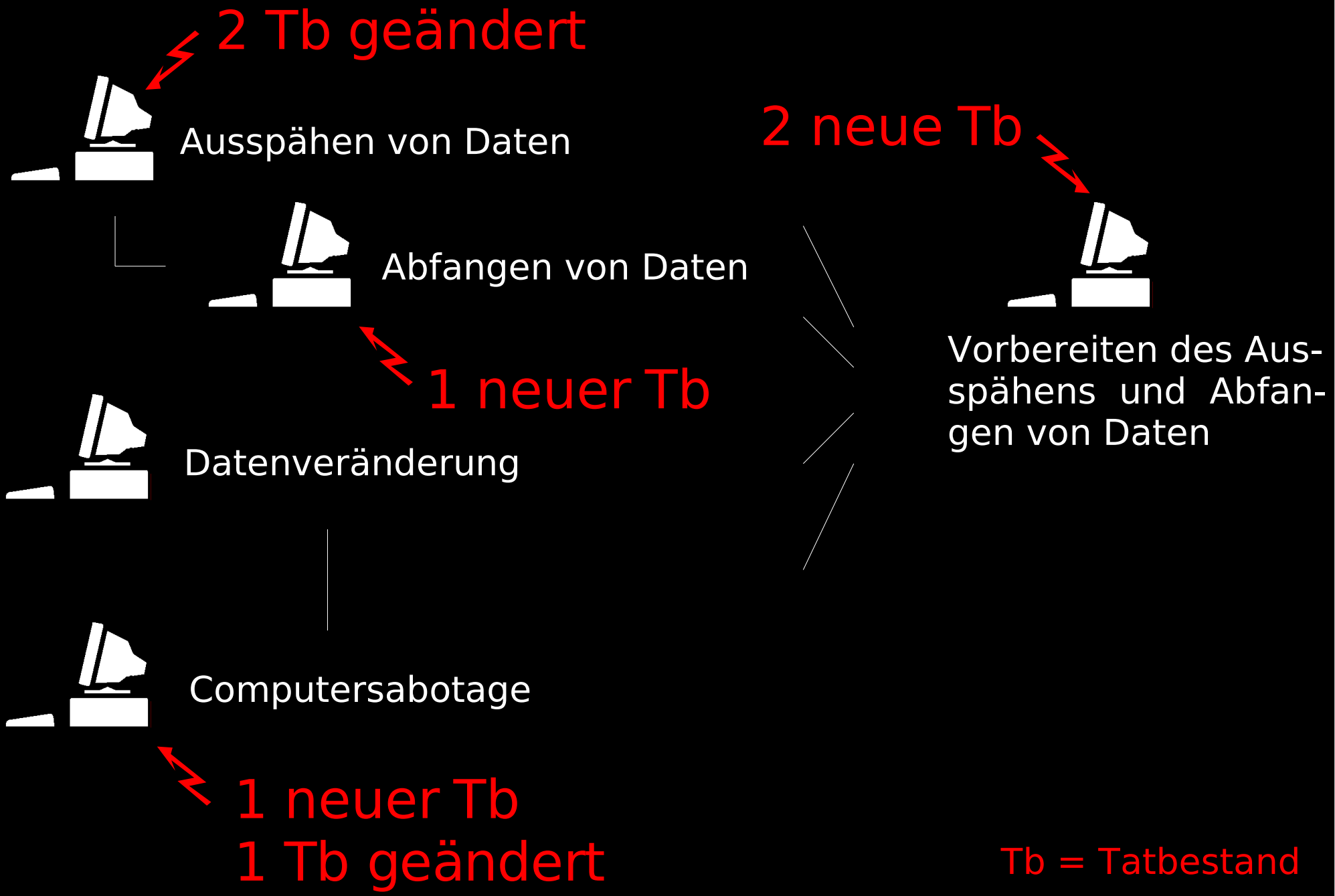
(1) internationale Abkommen umsetzen

(2) bestehende Strafbarkeitslücken schliessen

(3) Grenzen der Strafbarkeit vorverlegen

(4) Vorfeldhandlungen kriminalisieren

Was ändert sich bei den einzelnen Tatbeständen?



Welche *Handlungen* werden strafbar?

qualifiziertes, simples Portscanning

Sniffing

Pfishing (k.A.)

Denial of Service

Password cracking (k.A.)

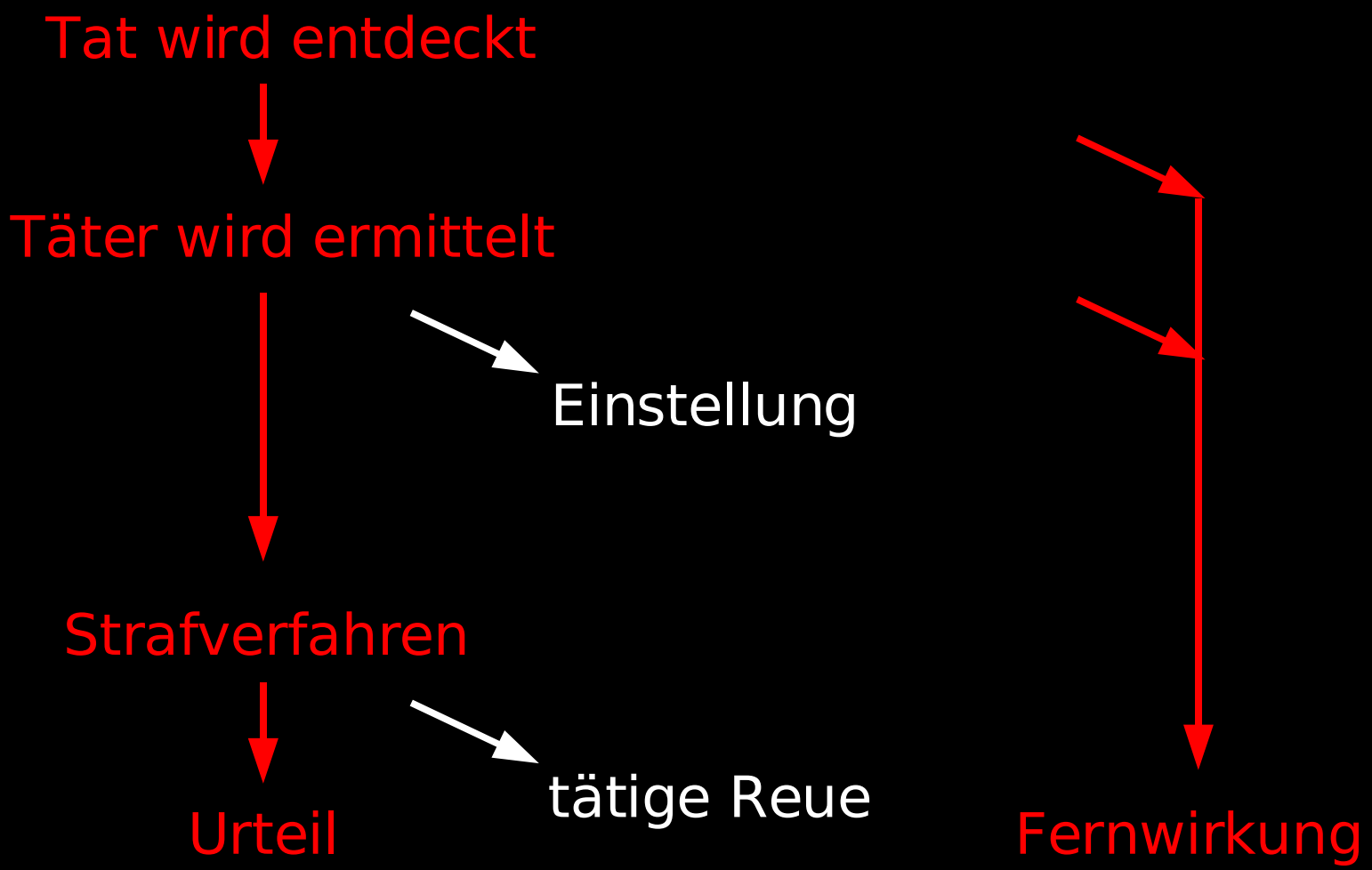
Intrusion via Network

Trojaner verbreiten

Viren verbreiten

Würmer verbreiten

Wartet am Ende immer ein Strafurteil?

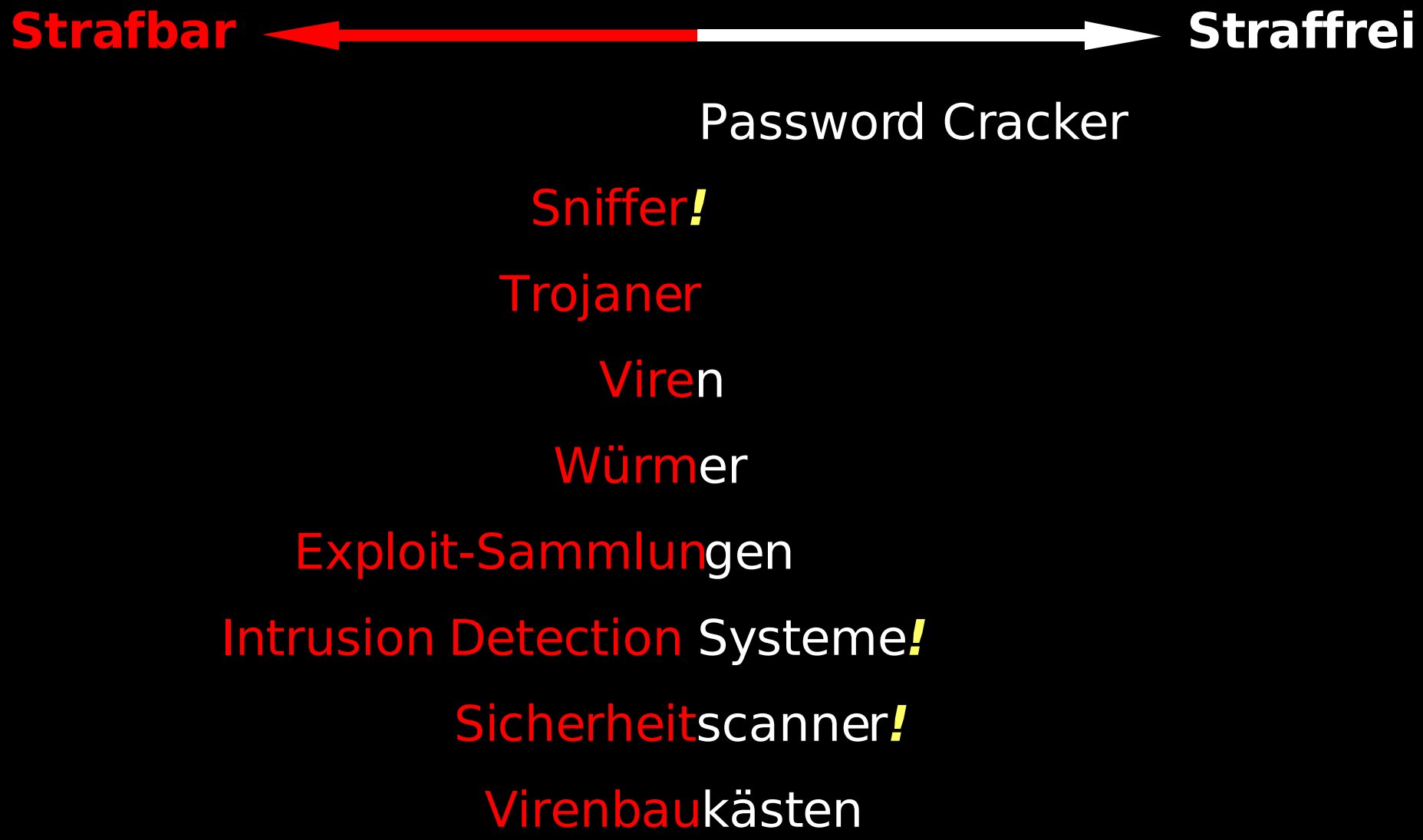


Verbot von Hackertools – worum geht es?

„Wer eine Straftat nach § ... vorbereitet, indem er ... Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird ... bestraft.“

Entwurf § 202 c Abs. 1 Alt. 2 StGB

Welche Programme *könnten* für die bezeichneten Straftaten eingesetzt werden?



Bereit das Beschaffen oder Überlassen solcher Software eine Straftrat vor?

- Falls ja, endet die Entwicklung und der Einsatz vieler Sicherheitstools am Standort Deutschland.
- Falls ja, kann die Qualität neuer Sicherheitstools in Deutschland nicht mehr getestet werden.
- Falls nein, kann niemand seriös voraussagen, was die Gerichte machen werden.
- Auf alle Fälle entsteht akuter Handlungsbedarf für Distributoren und für Nutzer.

Kann man das Verbot legal umgehen?

- Aufsplittung in eigenständige Programm-Module
- Auslagerung auf tiefere Softwareschichten (Bibliotheken, Kernel, Treiber)
- Verlagerung auf vorhergehende Lebensphasen von Software (Hackerbaukästen)
- Vorkehrungen zur tätigen Reue (reverse Backdoor)

Alle Varianten enthalten strafrechtliche Risiken.

Was bleibt Entwicklern und Penetrations-testern übrig, wenn das Gesetz ohne Änderung in Kraft tritt?

- sofort handeln und auswandern
- beobachten, in welchen Fällen die Gerichte wie entscheiden
- ins Risiko greifen

Welche Fernwirkungen sind zu befürchten?

- Neben Strafe und Verfahrenskosten lauern Schadensersatzpflichten.
- Im Betrieb verbotene Software einzusetzen, kann Abmahnungen auslösen.
- Geschäftsführer können bußgeldpflichtig werden.
- Eine Straftat (auch zugunsten des Arbeitgebers) kann zur Kündigung führen.
- Das gilt auch im Rahmen von Support- und Consulting-Verträgen.

Abschliessende Bewertung

- Zur Frage des Verbotes von Dual Use Software gibt es tendenziell widersprüchliche Aussagen.

- Es bleiben Zweifel, ob der Zeitdruck im Gesetzgebungsverfahren berechtigt ist.

- Eine öffentliche Beteiligung betroffener IT-Fachverbände oder -Fachleute ist nicht erkennbar.

Das alles läuft eine Frage hinaus ...

Who can you trust ?

und jetzt höre ich mal zu