"Les cybermenaces à l'horizon 2020"

Table ronde :
Réponses judiciaires aux cybermenaces

Podiumsdiskussion : Juristische Antworten auf die Cybergefahren

Animation par René ECKHARDT

La législation française : sa pertinence pour combattre la cybercriminalité

Mail: cdoutriaux@avocats-strasbourg.com

par Maître Cécile DOUTRIAUX

Avocate au Barreau de Strasbourg
Diplômée du Conservatoire National des Arts et Métiers
Chef d'escadron (RC) de la Gendarmerie Nationale

I - La législation française face aux cybermenaces

La répression des agissements fautifs commis dans le cyberespace

A - Les atteintes aux biens et aux personnes en ligne

- Atteintes aux personnes physiques
  - Atteinte à la vie privée et à l'image (A.9 C.Civil – A. 226-1 Code Pénal)
  - Diffamation – injure (A.29 Loi de la Presse du 29 juillet 1881)
  - L'usurpation d'identité numérique (A.226-4-1 Code Pénal)
- Atteintes aux personnes morales
  - Concurrence déloyale (A.L.420-1 Code de Commerce et L.120-1 C.
  - Contrefaçon de marque (A.L.716-1 Code de la Propriété Intellectuelle)
- Atteintes aux biens
  - Escroquerie (A.313-1 Code Pénal)
  - Abus de confiance (A.314-1 Code Pénal)
  - Vol et recel d'informations dématérialisées

B - Les attaques *informatiques*

- Infractions aux systèmes de traitement automatisé des données réprimées par la Loi Godfrain du 5 janvier 1988

  - Accès ou maintien frauduleux (A.323-1 Code Pénal)
  - Atteinte à l'intégrité du système (A.323-2 Code Pénal)
  - Atteinte à l'intégrité des données (A.323-3 Code Pénal)

C - Apport de la JP pour définir les auteurs d'infractions

- Les fournisseurs d'accès à internet
- Les hébergeurs
- Les éditeurs de contenus :

  blog et forum de discussion

II- La procédure judiciaire - Obstacles et Remèdes

La pertinence de l'arsenal juridique français face aux cybermenaces

A - Moyens des enquêteurs et Procédure judiciaire

- L'établissement de la preuve de l'infraction : Les OPJ

  - Principe général : la production de preuve est libre en matière pénale
  - Les contraintes : le respect des principes de légalité et de loyauté
  - Des moyens renforcés depuis la loi Loppsi 2

- Les magistrats :

  - Les moyens d'investigation :
    * réquisitions informatiques
    * interceptions de communications effectuées sur internet
    * rendre l'accès d'un site impossible

- Les partenaires de la procédure judiciaire :

  - Les experts judiciaires
  - Les huissiers de justice
  - Les avocats

B - Obstacles à l'efficacité de la lutte

- Le problème de la prescription et de la propagation rapide de l'infraction sur de nombreux sites
- La difficile qualification des faits fautifs face à l'éparpillement des textes répressifs
- Le problème de la compétence territoriale des juridictions
- La lenteur de l'élaboration de la loi face à l'évolution rapide des NTIC et à des cyber-délinquants organisés et astucieux
- Le problème de l'exécution des décisions de justice et de la solvabilité de l'auteur de l'infraction

C - Remèdes *pour une réponse plus efficace*

- Une meilleure spécialisation des acteurs de la procédure
- L'élaboration d'un code spécifique à la cybercriminalité ?
- La centralisation des plaintes : signalement en ligne des infractions
  - La C.N.I.L.
  - Signalement-gouv.fr
- Une nécessaire collaboration européenne et internationale

Merci!

Vielen Dank!

Pour une approche globale de maitrise des cyber menaces

Perspectives internationale et suisse

Email : sgh@unil.ch

par Solange GHERNAOUTI-HELIE

Professeure HEC – Université de Lausanne
Dr. en informatique de l'Université Paris VI
Expert international en sécurité et criminalité du numérique

De nouveaux risques

- Les TICs introduisent de nouveaux risques pour
  - Les individus
  - Les organisations
  - Les Etats

- Risque structurel, omniprésent
  - Dépendance & interdépendance des
    - Infrastructures informatiques et télécoms
    - Infrastructures vitales

Risque informatique d'origine criminelle

mais pas seulement …

Cyberespace & gestion des risques

- Le cyberespace induit un nouveau paradigme
  - Le cyber pouvoir dont la cybersécurité est un des instruments

Le cyberespace: un nouveau champ de bataille

Le cyber pouvoir: une arme

de la guerre économique et / ou de la guerre militaire

- La notion de risque s'exprime toujours par rapport à des vulnérabilités et leurs conséquences
  - C'est la conjonction des menaces et des vulnérabilités qui devraient être abordées aux niveaux individuel, des organisations et de l'Etat
    - Les vulnérabilités devraient toujours en principe, être connues
      - C'est sur elles qu'il faut agir afin de se prémunir contres les menaces et leurs impacts…

Cyber menaces & cyber risques

Sommes-nous prêts?

- La question de la robustesse des infrastructures face aux cyber menaces est

  - Générale
  - Permanente
  - Prépondérante

Cybersécurité
des réponses
aux niveaux national et
International

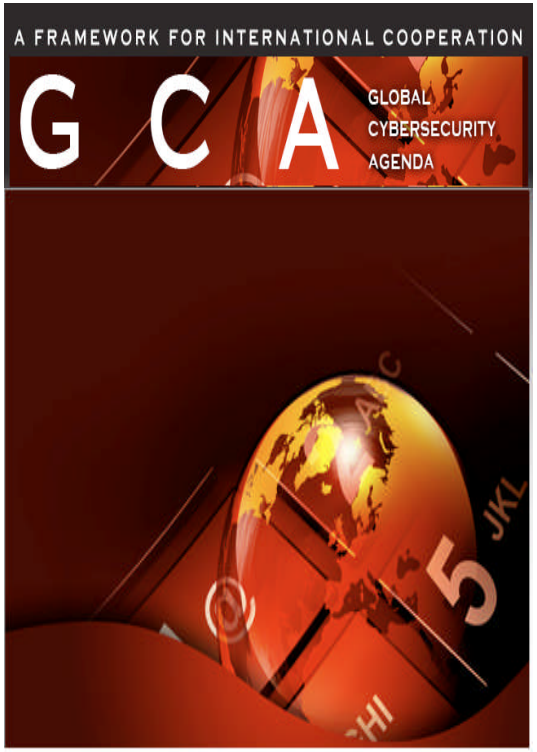
Une approche holistique

Une question internationale

Helping the world communicate

International Telecommunication Union

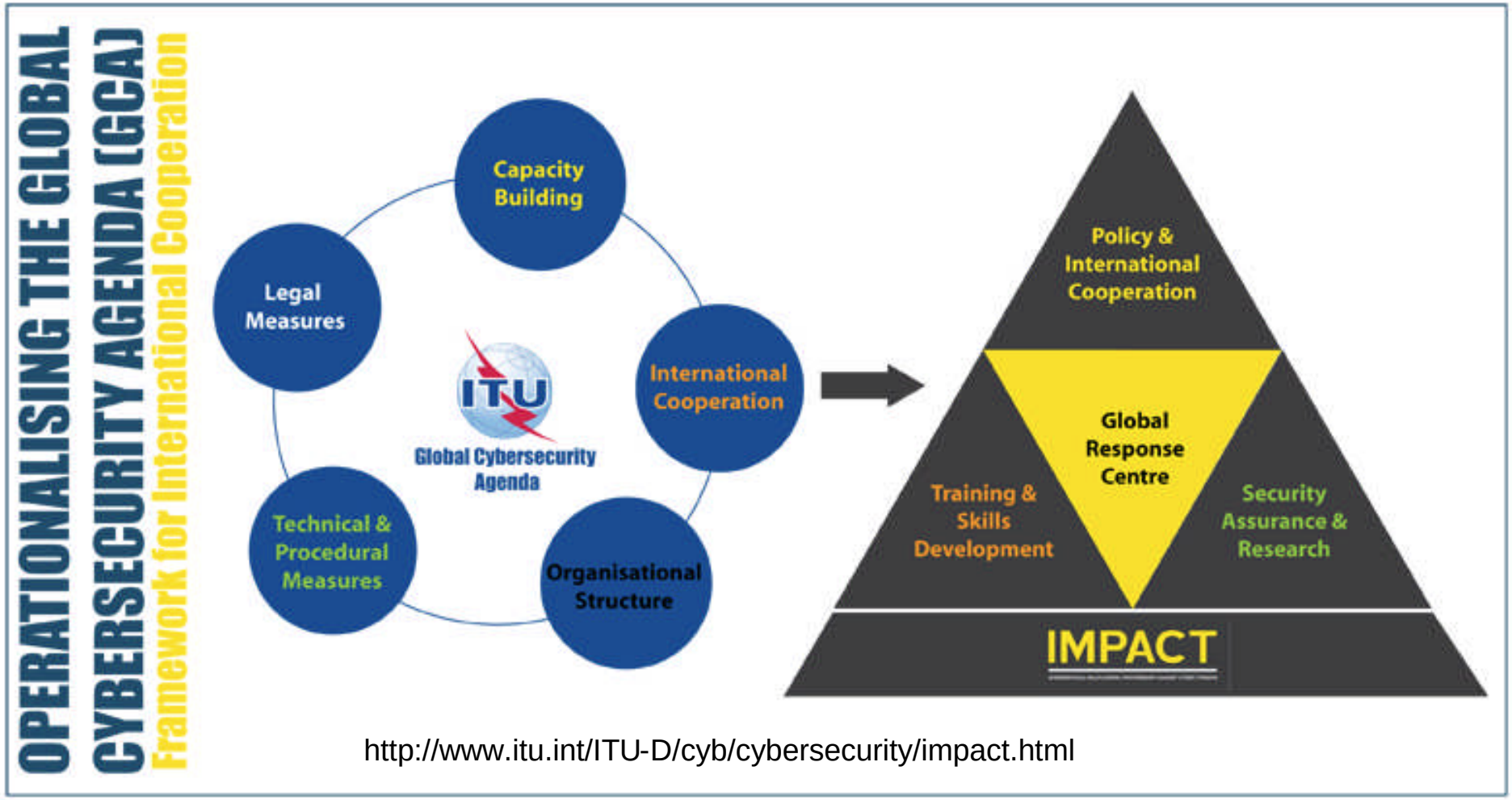
- *Global Cybersecurity Agenda*
  - (ITU 2007)http://www.itu.int/osg/csd/cybersecurity/gca/



- Une approche intégrée: une référence mondiale
  - Mesures légales
  - Mesures techniques et procédurales
  - Construire les capacités
  - Structures organisationnelles
  - Coopération internationale

Un centre de compétences en Malaisie

IMPACT

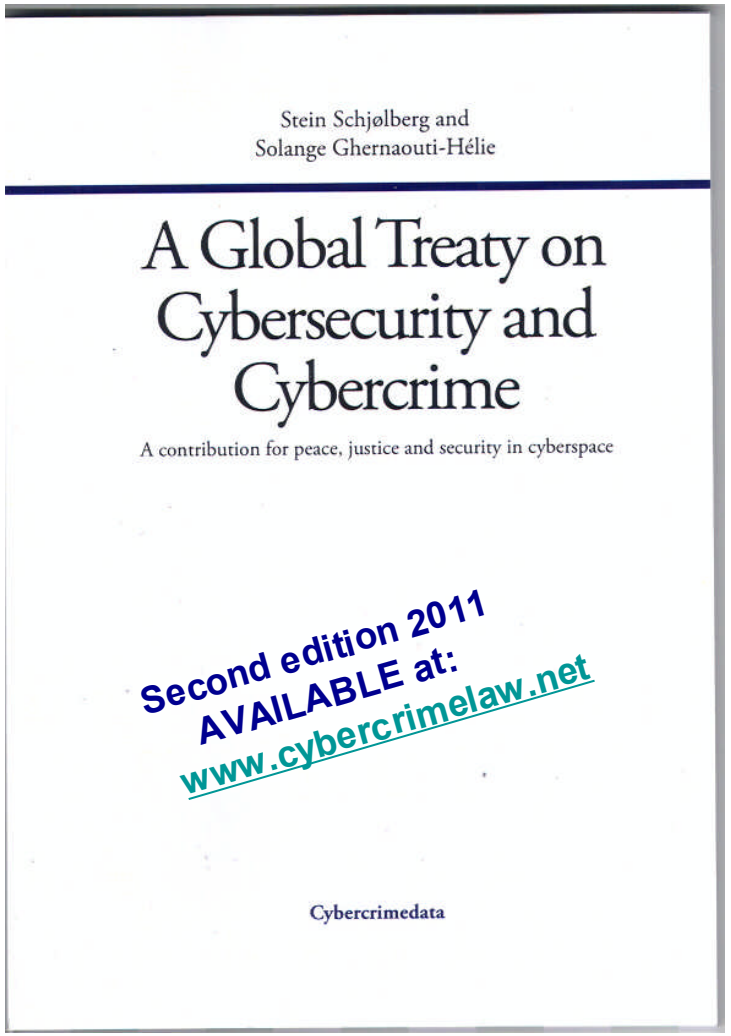


http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html

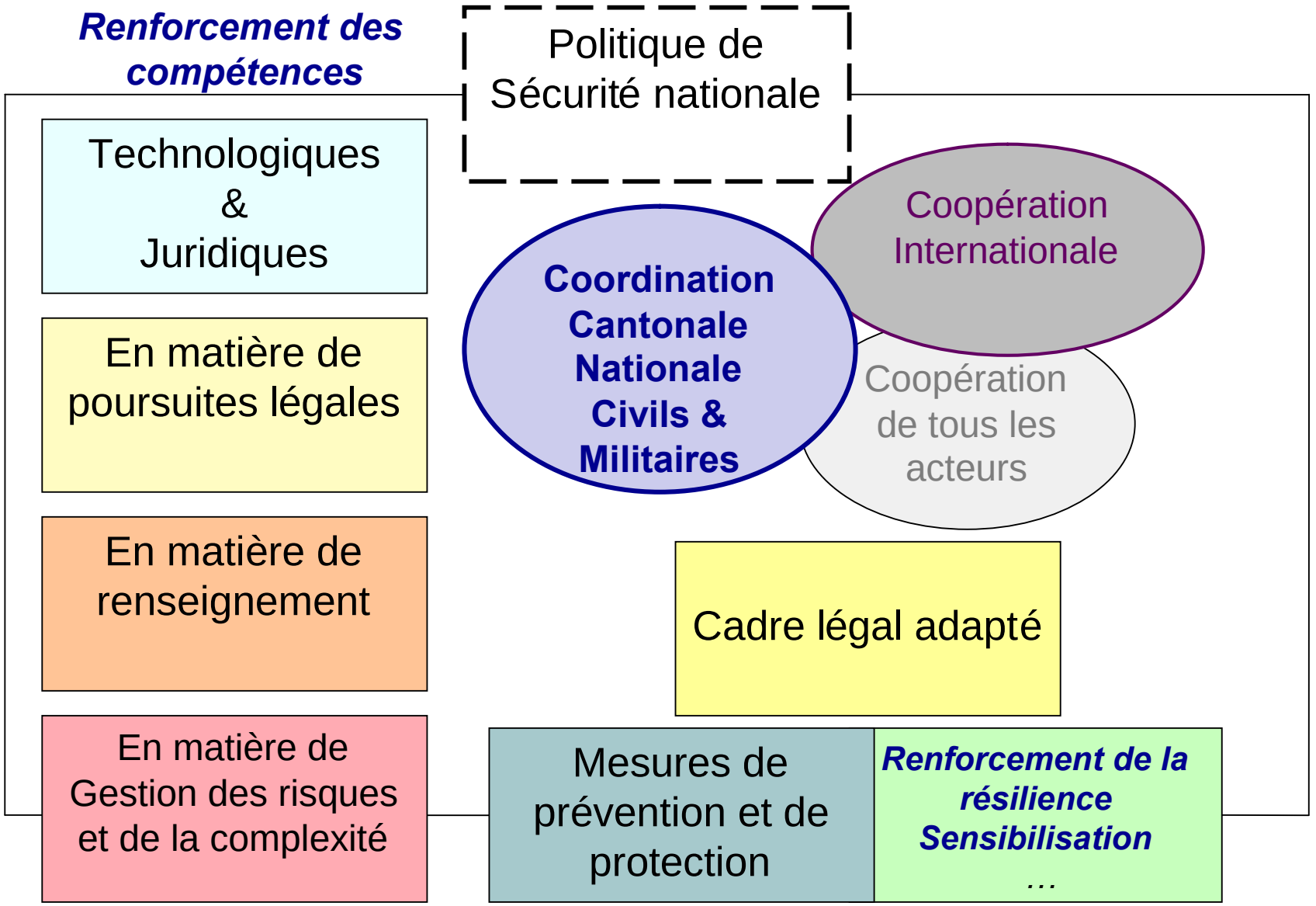
Pour un traité international du cyberespace

La Terre, la mer, l'air, l'espace
… *et le **cyberespace***

- *Table of contents*
- Part one
  - *Draft code on peace, justice and security in cyberspace*
- Part two
  - *Measures on cybersecurity*
- Part three
  - *New legal mechanisms for combatting cybercrime*
- Appendix & references



De la prise de conscience aux mesures : le programme Cyber Défense suisse



Une réponse judiciaire mais pas seulement

Merci!

Vielen Dank!

Der rechtliche Rahmen Für Ermittlungsmaßnahmen in Deutschland

Email : Stefan.Fahrion@stastuttgart.justiz.bwl.de

Staatsanwalt Stefan FAHRION

Staatsanwalt
Generalstaatsanwaltschaft Stuttgart
Zentralstelle für die Bekämpfung der Informations- und Kommunikationskriminalität

Ermittlungsmaßnahmen

- Erhebung von Verkehrsdaten (§ 100g StPO)
- TKÜ-Maßnahmen/Erhebung von Inhaltsdaten (§ 100a StPO)
- Einsatz technischer Mittel (§ 100h StPO –insbesondere GPS)
- Online-Durchsuchung (unzulässig, keine Rechtsgrundlage)
- Beschlagnahme von Daten, §§ 94, 98 StPO als offene Ermittlungsmaßnahme
- letzteres ggf. in Verbindung mit einer Durchsuchung beim Provider gemäß § 103 StPO

Erhebung von Verkehrsdaten (§100g StPO)

- Problem Wegfall der Vorratsdatenspeicherung in den §§ 113a und 113b TKG durch Urteil des BVerfG vom 02.03.2010 → Es können nur noch Verkehrsdaten nach § 96 TKG erhoben werden. Pflicht zur Vorratsdatenspeicherung ist entfallen.
- Am 27.10.2011 setzte die EU-Kommission Deutschland eine Frist von 2 Monaten zur Umsetzung der entsprechenden EU-Richtlinie
- Datenschutzrechtliche Speicherbefugnis für Verkehrsdaten in § 96 TKG nur für Abrechnungszwecke:

  nähere Umstände der Kommunikation (Absender/ Empfänger, Zeitpunkt/Dauer, Standortkennung bei Mobiltelefon, dynamische IP-Adressen bei Internet-Kommunikation -> insbesondere bei IP-Adressen

Katalogtaten für die Telekommunikationsüberwachung (§100a,b StPO)

Aus dem Bereich Cybercrime u.a.:

- Fälschung von Zahlungskarten (white plastics)
- gewerbsmäßiger sowie bandenmäßiger Betrug und Computerbetrug (Phishing, Carding, Warenbetrug)
- Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften
- Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte
- Erpressung (DDos mit Zahlungsaufforderung)

Formen der Telekommunikationsüberwachung

- Klassische Telefonüberwachung (auch über IMEI)
- Überwachung sonstiger Datenübertragung (UMTS, DSL, sonstige Internetanschlüsse, Hotspots, Voice-Over-IP, Chats, E-Mails, usw.)
- Überwachung von Datentransfer zwischen Mobilgerät und WLAN-Router/Hotspot
- Serverüberwachung
- Auslandskopfüberwachung (aus dem Ausland eingehende Anrufe von einem bestimmten Anschluss)

Quellen-Telekommunikationsüberwachung

- Streitig, aber nach überwiegender Meinung zulässig*
- die Überwachung darf sich ausschließlich auf die Daten einer laufenden Kommunikation beziehen und es ist durch technische Vorkehrungen sicher zu stellen, dass es zu keiner Erhebung weiterer persönlichkeitsrelevanter Daten (z.B. Dateien auf der Festplatte des Rechners) kommt (keine Online-Durchsuchung.
- Einsatz und Intstallation der Überwachungssoftware auf dem Rechner des Betroffenen Annexkompetenz aus § 100a STPO

* AG Bayreuth Beschluss vom 17.09.2009 — Gs 911/09 (MMR 2010, 266 m. Anm. *Bär); Meyer-Goßner* StPO 53. Aufl. § 100a Rn. 7a; KK-StPO/Nack § 100a Rn. 27; *BeckOK-StPO/Graf, §* 100a Rn. 114 f. *Bär* MMR 2008, 215 [218] und LG Hamburg, Beschluss vom 13.09.2010 — Az. 608 Qs 17/10

E-Mail-Überwachung (BVerfG Urteil vom 16.06.2009 -NJW 2009, 2431)

Übermittlung in 4 Phasen:

- vom Absender bis zum Mailserver des Empfängers (TKÜ nach § 100a StPO, verdeckt)
- Zwischenspeicherung am Mailserver des Empfänger-Providers (Beschlagnahme nach §§ 94, 98 StPO, offene Maßnahme, falls die Ausleitung zukünftiger Nachrichten erfolgen soll, verdeckt nach § 100a StPO [str.])
- Datenabruf vom Mailserver durch den Empfänger (TKÜ nach § 100a StPO)
- Speicherung der Nachricht am Rechner des Empfängers (§§ 94, 98 StPO, offene Maßnahme)
- Bei offenen Maßnahmen ist der Beschuldigte von der Maßnahme zu benachrichtigen

Online-Durchsuchung

- Im repressiven Bereich Mangels Eingriffsgrundlage unzulässig (BVerfG, 1 BvR 370/07 vom 27.2.2008)
- Nur präventiv zulässig (BKA, Geheimdienste)

Zugriff auf externe Datenspeicher im Inland (§110 Abs. 3 StPO)

- Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden.
  - Daten innerhalb eines LAN (Unternehmen, usw.)
  - Daten auf Online-Speichermedien (insb. in der Cloud)
  - Zugriff auf beim Provider gespeicherte E-Mails zulässig
  - Zugriff mittels vor Ort aufgefundener Passwörter zulässig

Merci!

Vielen Dank!

Questions

"Les cybermenaces à l'horizon 2020"

Clôture de la journée

Abschlusswort

par le colonel Jean-Thierry DAUMONT
Commandant de la région de gendarmerie d'Alsace
Leiter der Région de gendarmerie d'Alsace

"Les cybermenaces à l'horizon 2020"