“Grenzüberschreitender” Zugriff auf Daten im Rahmen der Budapest Konvention

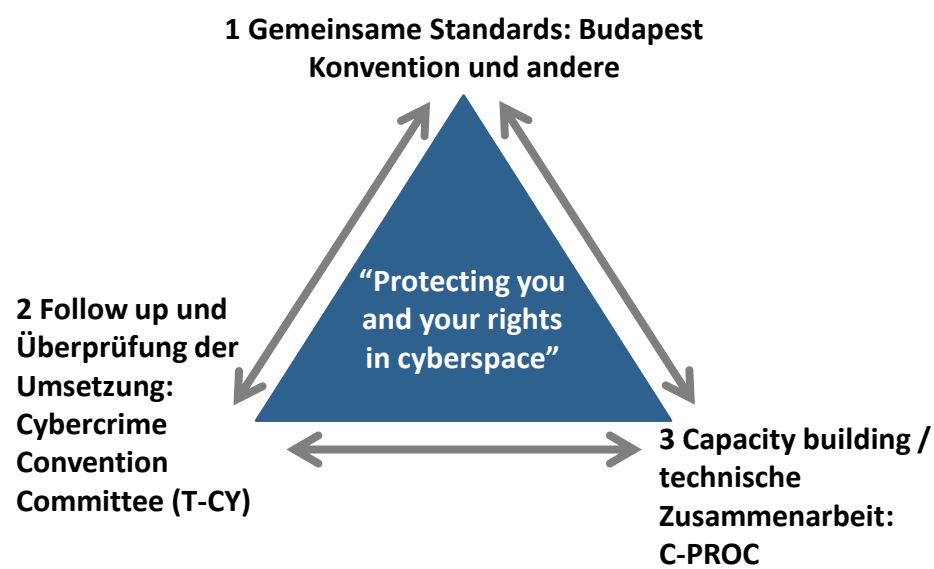
Alexander Seger
Executive Secretary
Cybercrime Convention Committee
Council of Europe
Strasbourg, France

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

1

Kooperation gegen Cybercrime: Der Ansatz des Europarats



2

Zur Budapest Konvention: Cybercrime UND elektronische Beweismittel

Criminalising conduct
- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools
- Expedited preservation
- Production orders
- Search and seizure
- Interception of computer data

+

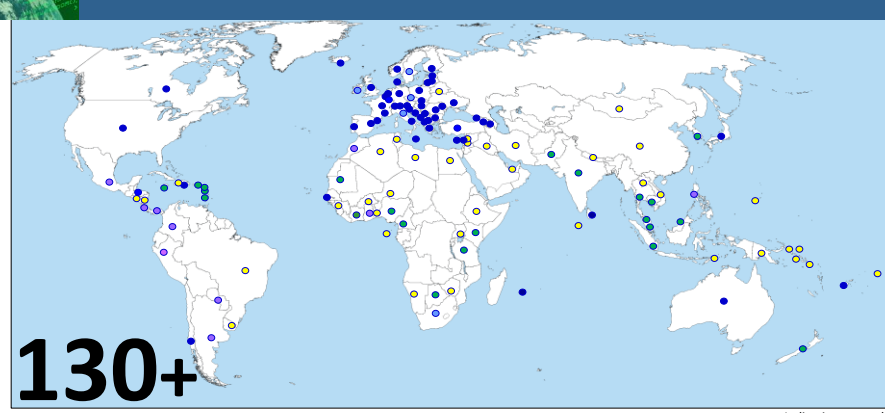
International cooperation
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- Transborder access (Art. 32)
- 24/7 points of contact

Harmonisation

www.coe.int/cybercrime

3

Reichweite der Budapest Konvention



Indicative map only

Ratified/acceded: 55

+ Signed: 5

+ Invited to accede: 8

= 68

Other States with laws/draft laws largely in line with Budapest Convention = 20+

Further States drawing on Budapest Convention for legislation = 45+

4

T-CY Cloud Evidence Group: Zugriff auf Daten in der Cloud - Erwägungen

- E-evidence on servers in foreign, unknown, multiple or shifting jurisdictions, in the cloud
- Budapest Convention: Criminal justice treaty
- Focus on specified data within specific criminal investigations
- Cybercrime AND electronic evidence in relation to any crime
- Less than 1% of cybercrime reported eventually adjudicated = rule of law in cyberspace? = governments meeting obligation to protect (K.U. v Finland)?
- No data, no evidence, no prosecution, no justice, no rule of law

5

T-CY Cloud Evidence Group: Zugriff auf Daten in der Cloud - Erwägungen

How to ensure the rule of law in cyberspace through more efficient access to electronic evidence for criminal justice purposes?

- Assessment of mutual legal assistance provisions ► 24 recommendations to make MLA more efficient (Dec 2014)
- Transborder access to data (T-CY Transborder Group 2012-2014)
  - Clarification of Article 32b Budapest Convention ► Guidance Note (Dec 2014)
  - Additional options for transborder access ► necessary but politically not feasible in 2014. (Risk of increasing unilateral action)
- T-CY Cloud Evidence Group (2015-2016): Proposals submitted to Cybercrime Convention Committee in November 2016

www.coe.int/cybercrime

6

Cloud Evidence Group: Problembereiche

- Differentiating subscriber (Bestandsdaten) versus traffic (Verkehrsdaten) versus content data (Inhalte)
- Effectiveness of MLA
- Loss of location and transborder access jungle
- Provider present or offering a service in the territory of a Party
- Voluntary disclosure by US-providers
- Emergency procedures
- Data protection

Problem: Subscriber vs traffic vs content data

- Subscriber information (Verkehrsdaten) most often required in criminal investigations.
- Less privacy-sensitive than traffic or content data. Rules for access to subscriber information not harmonised.
- Subscriber information held by service providers and obtained through production orders. Lesser interference in rights than search and seizure.

Problem: Internationale Rechtshilfe

- Mutual legal assistance remains a primary means to obtain electronic evidence for criminal justice purposes
- MLA needs to be made more efficient
- Often subscriber information or traffic data needed first to substantiate or address an MLA request
- MLA often not feasible to secure volatile evidence in unknown or multiple jurisdictions

Problem: "Loss of location"

- In "loss of location" situations (unknown source of attack, servers in multiple or changing locations, live forensics, etc.) MLA not feasible ► principle of territoriality not always applicable
- Direct transborder access to data may be necessary
- What conditions and safeguards?
- Article 32b Budapest Convention limited ► Absence of international legal framework for lawful transborder access
- Unilateral solutions by governments / jungle ► risks to rights of individuals and state to state relations

Problem: Loss of location und Grenzen des Artikel 32

Article 32 Budapest Convention – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

11

Problem: Loss of location und Grenzen des Artikel 32

Artikel 32 –Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind

Eine Vertragspartei darf ohne die Genehmigung einer anderen Vertragspartei

a auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen, gleichviel, wo sich die Daten geographisch befinden, oder

b auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die rechtmäßige und freiwillige Zustimmung der Person einholt, die rechtmäßig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben.

12

Problem: Loss of location und Grenzen des Artikel 32

T-CY Guidance Note on Transborder Access to Data (Article 32), December 2014

Regarding Article 32b, typical situations may include:

"A suspected drug trafficker is lawfully arrested while his/her mailbox - possibly with evidence of a crime - is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b."

Problem: Loss of location und Grenzen des Artikel 32

Guidance Note on Article 32

General considerations: Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14.

On the notion of "access without the authorisation of another Party": Article 32b does not require mutual assistance, and the Budapest Convention does not require a notification of the other Party. At the same time, the Budapest Convention does not exclude notification. Parties may notify the other Party if they deem it appropriate.

On the applicable law: In all cases, law enforcement authorities must apply the same legal standards under Article 32b as they would domestically. If access or disclosure would not be permitted domestically it would also not be permitted under Article 32b.

Problem: Loss of location und Grenzen des Artikel 32

Guidance Note on Article 32

On the person who can provide access or disclose data: Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32.

Domestic lawful requests versus Article 32b: Article 32b is not relevant to domestic production orders or similar lawful requests internal to a Party.

On the location of the person consenting to provide access or disclose data: The standard hypothesis is that the person providing access is physically located in the territory of the requesting Party. However, multiple situations are possible.

= Artikel 32 ist sehr begrenzt

15

Problem: Loss of location und transborder access jungle

Long-arm doctrine of EU anti-trust law (Cases *ICI* 48/69; *Woodpulp* 89/85)

► the European Commission recommends that competition authorities within the European Union obtain access to servers anywhere in the world to gather evidence in anti-trust proceedings:

"To have effective powers to gather digital evidence, it is important that the Authorities can in the exercise of their inspection powers gather digital information which is accessible to the undertaking or person whose premises are being inspected irrespective of where it is stored, including on servers or other storage media located outside the territory of the respective national competition authority or outside the European Union."

Source: European Competition Network "Recommendation on the power to collect digital evidence, including by forensic means"
http://ec.europa.eu/competition/ecn/ecn_recommendation_09122013_digital_evidence_en.pdf

www.coe.int/cybercrime

16

Problem: Wann ist ein Provider "hier"?

- When is a service provider
  - "present" in the territory of a State?
  - "offering a service" in the territory of a State?
- Therefore, when is a service provider subject to a domestic production or other type of coercive order?
- If domestic production orders for subscriber information ► reduction of pressure on MLA system

Problem: Freiwillige Herausgabe durch Provider

- More than 100,000 requests/year by European States to major US providers
- Disclosure of subscriber or traffic data (ca. 60%)
- Providers decide whether or not to respond to lawful requests and whether to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No disclosure by European providers
- No admissibility of data received in some States

► Clearer / more stable framework required

Problem: Freiwillige Herausgabe durch Provider

	Requests for data sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2015		
Parties	Received	Disclosure	%
Austria	254	119	47%
Belgium	1 992	1 453	73%
Canada	1 157	884	76%
France	27 213	14 746	54%
Germany	29 092	15 469	53%
Italy	7 847	3 591	46%
Netherlands	1 605	1 213	76%
Poland	2 378	820	34%
Portugal	3 255	1 751	54%
Spain	4 151	2 092	50%
United Kingdom	29 937	21 075	70%
USA	89 350	70 116	78%
Total excluding USA	**138 612**	**82 529**	**60%**
Total including USA	227 962	152 644	67%

Problem: Notfall-Prozeduren

- Emergency procedures needed to obtain evidence located in foreign jurisdictions through
  - Mutual legal assistance

  and through
  - Direct cooperation with a service provider

Problem: Datenschutz und andere Rechtsstaatsgarantien

- Data protection requirements normally met if powers to obtain data defined in domestic criminal procedure law and/or MLA agreements
- MLA not always feasible
- Increasing "asymmetric" disclosure of data transborder
  - From LEA to service provider ► Permitted with conditions
  - From service provider to LEA ► Unclear legal basis ► providers to assess lawfulness, legitimate interest ► risk of being held liable ▌ Confidentiality requirements

= Clearer framework for public to private to public disclosure transborder required

T-CY Cloud Evidence Group: Lösungen

Five solutions to be pursued in parallel:

1. More efficient MLA
2. Guidance Note on Article 18
3. Domestic rules on production orders (Article 18)
4. Cooperation with providers: practical measures
5. Protocol to Budapest Convention

Lösung 1: Effizientere Rechtshilfe

- Implement legal and practical measures
  ▶ Recommendations 1 – 15 of T-CY assessment report on MLA at domestic levels
  - More resources and training
  - Electronic transmission of requests
  - Streamlining of procedures
  - Etc.
- Parties to establish emergency procedures for obtaining data in their MLA systems
- Parties to facilitate access to subscriber information in domestic legislation (full implementation of Article 18 Budapest Convention)

Lösung 2: Leitfaden zu Artikel 18

Guidance Note on Article 18 Budapest Convention on production of subscriber information (Anordnung der Herausgabe von Bestandsdaten):

- Domestic production orders if a provider is in the territory of a Party even if data is stored in another jurisdiction (Article 18.1.a)
- Domestic production orders for subscriber information if a provider is NOT necessarily in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)

Lösung 2: Leitfaden zu Artikel 18

The production of subscriber information under Article 18 Budapest Convention could be ordered if the following criteria are met in a specific criminal investigation and with regard to specified subscribers

IF

The criminal justice authority has jurisdiction over the offence;

AND IF

the service provider is in possession or control of the subscriber information;

AND IF

Article 18.1.a **The person (service provider) is in the territory of the Party.**	**OR**	**Article 18.1.b** **A Party considers that a service provider is "offering its services in the territory of the Party" when, for example:** – **the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services);** **and** – **the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.**

25

25

Lösung 3: Nationale Regeln für Anordnung der Herausgabe (production orders)

- **Proper implementation of Article 18 at domestic levels**
- **Lighter regime for production of subscriber information (as compared to traffic and content data)**
- **Use of information obtained as evidence in criminal proceedings**

Lösung 4: Kooperation mit Providern

Pending longer-term solutions:

Practical measures to facilitate transborder cooperation between service providers and criminal justice authorities

- Focus on disclosure of subscriber information upon lawful requests in specific criminal investigations
- Emergency situations
- Consideration of legitimate interests and data protection requirements

Lösung 5: Protokoll zur Budapest Konvention

A. Provisions for more efficient MLA

- International production orders
- Simplified MLA for subscriber information
- Direct cooperation between judicial authorities in MLA
- Joint investigations and joint investigation teams
- Requests in English. Audio-video hearings.
- Emergency procedures

B. Provisions for direct cooperation with providers in other jurisdictions

- Disclosure of data by LEA to a service provider abroad in specific situations
- Disclosure of subscriber information by service providers to LEA abroad with conditions and safeguards
- Direct preservation requests to providers abroad
- Admissibility of data obtained directly in domestic proceedings
- Emergency procedures

Lösung 5 cont'd: Protocol to Budapest Convention

C. Framework and safeguards for existing practices of transborder access to data

- Transborder access to data with lawfully obtained credentials
- Transborder access in good faith or in exigent circumstances
- The power of disposal as connecting legal factor

D. Data protection

- Requirements for transfer transborder by LEA to a service provider abroad
- Requirements for transfer transborder by a service provider to LEA abroad

Lösungen: Status 19. Mai 2017

1. **More efficient MLA**
   - Umsetzung wird derzeit überprüft (T-CY 7.-9. Juni 2017).
   - Siehe Lösung 5
2. **Guidance Note on Article 18**
   - Am 28. Februar 2017 angenommen
3. **Domestic rules on production orders (Article 18)**
   - Umsetzung wird von Vertragsparteien erwogen.
4. **Cooperation with providers: practical measures**
   - Von Vertragsparteien angenommen.
5. **Protocol to Budapest Convention**
   - Verhandlung soll am 7.-9. Juni 2017 beschlossen werden.