Staatsanwalts|Akademie

GRENZ-ÜBERSCHREITENDER ZUGRIFF AUF DATEN: STATUS QUO UND INTERNATIONALE ENTWICKLUNGEN

ALEXANDER SEGER
HEAD OF CYBERCRIME DIVISION
COUNCIL OF EUROPE
STRASBOURG, FRANCE

LUZERN, 5. SEPTEMBER 2024

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

1

Staatsanwalts|Akademie

CONTENT

Intro
- Cybercrime & electronic evidence
- Convention on Cybercrime (Budapest Convention) & Protocols

Access to e-evidence "transborder"
- Article 18.1.b Budapest Convention
- Article 32 Budapest Convention
- Second Protocol on enhanced cooperation and disclosure of e-evidence

Draft United Nations treaty against "cybercrime"

2

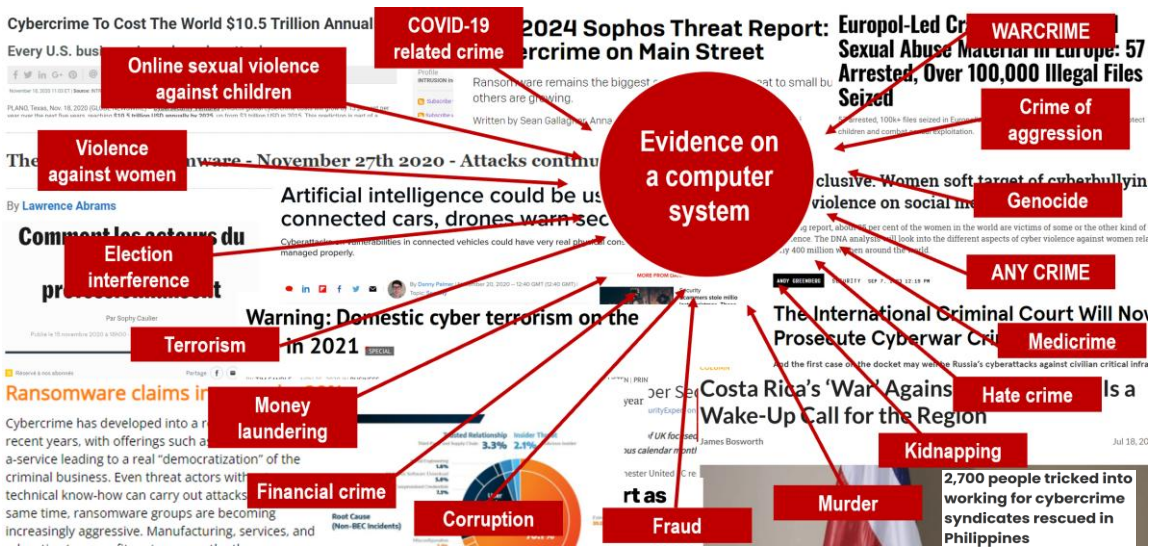
Staatsanwalts|Akademie

INTRO: CYBERCRIME & E-EVIDENCE

3

Staatsanwalts|Akademie

INTRO: CYBERCRIME & E-EVIDENCE



4

Staatsanwalts|Akademie

INTRO: CYBERCRIME & E-EVIDENCE /ELECTRONISCHE BEWEISMITTEL

Computer data:

- ► Subscriber information (Bestandsdaten)
- ► Traffic data (Verkehrsdaten)
- ► Content data (Inhaltsdaten)

Staatsanwalts|Akademie

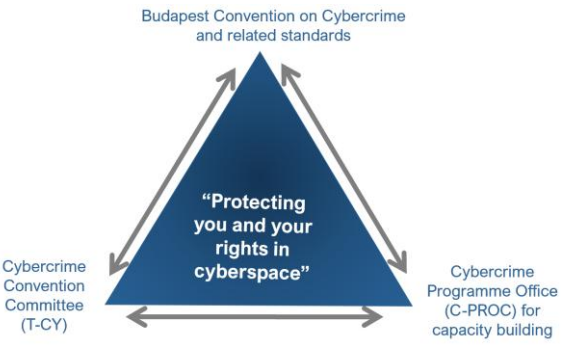
INTRO: CONVENTION ON CYBERCRIME +

► Budapester Übereinkommen über Computerkriminalität (2001)
- Spezifische Straftaten
- Ermittlungsbefugnisse
- Internationale Zusammenarbeit

► 1. Protokoll über Fremdenfeindlichkeit und Rassismus in Computersystemen (2003) ► 2. Protokoll über verstärkte Zusammenarbeit und Offenlegung elektronischer Beweismittel (2022)

► Leitlinien

By August 2024: **76 Parties and 17 "Observer States"**



Staatsanwalts|Akademie

ACCESS TO EVIDENCE “TRANSBORDER”: ART. 18 BC

Article 18 BC – Production order / Anordnung zur Herausgabe

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control.

(See **Guidance Note on Article 18** on the production of subscriber information)

7

Staatsanwalts|Akademie

ACCESS TO EVIDENCE “TRANSBORDER”: ART. 18 BC

Artikel 18 – Anordnung der Herausgabe
1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen,

a dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat und

b dass ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Bestandsdaten (1) in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, vorzulegen hat.

(See Guidance Note on Article 18 on the production of subscriber information)

8

Staatsanwalts|Akademie

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.

9

Staatsanwalts|Akademie

ACCESS TO EVIDENCE "TRANSBORDER": ART. 32 BC

Article 32 BC – 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.

(See **Guidance Note on Article 32**)

10

Staatsanwalts|Akademie

ACCESS TO EVIDENCE “TRANSBORDER”: ART. 32 BC

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.

(See Guidance Note on Article 32)

11

Staatsanwalts|Akademie

ACCESS TO EVIDENCE “TRANSBORDER”: ART. 32 BC

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

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.”

12

Staatsanwalts|Akademie

ACCESS TO EVIDENCE “TRANSBORDER”: ART. 32 BC

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.

Staatsanwalts|Akademie

ACCESS TO EVIDENCE “TRANSBORDER”: ART. 32 BC

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.

= The possibilities under Article 32 are very limited.

Staatsanwalts|Akademie

ACCESS TO EVIDENCE "TRANSBORDER": 2ND PROTOCOL

Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS 224)

- Prepared by the Cybercrime Convention Committee (T-CY) 2017 - 2021
- Opened for signature: Strasbourg, May 2022
- Status August 2024:
  - Parties: 2 (Serbia and Japan)
  - + Signatories: 44 (most recent Czechia, Georgia, Sierra Leone (June 2024)

15

Staatsanwalts|Akademie

ACCESS TO EVIDENCE "TRANSBORDER": 2ND PROTOCOL

Why this Protocol (rationale):

Positive obligation: governments to provide the means to protect individuals against crime, including cybercrime

- ► How to obtain subscriber information efficiently?
- ► How to cooperate directly with a service provider in another Party?
- ► How to obtain WHOIS data (domain name registration information) from registrars?
- ► How to obtain stored data, including content, in an emergency situation?
- ► How to make mutual assistance more effective?
- ► How to reconcile efficient and effective measures with rule of law and data protection requirements?

16

Staatsanwalts|Akademie

ACCESS TO EVIDENCE "TRANSBORDER": 2ND PROTOCOL

Warum dieses Protokoll (Begründung): Positive Verpflichtung:
Regierungen müssen Mittel bereitstellen, um Einzelpersonen vor Kriminalität, einschließlich Cyberkriminalität, zu schützen.

- Wie erhält man Abonnenteninformationen / Bestandsdaten effizient?
- Wie arbeitet man direkt mit einem Dienstanbieter einer anderen Partei zusammen?
- Wie erhält man WHOIS-Daten (Registrierungsinformationen für Domänennamen) von Registraren?
- Wie erhält man in einer Notsituation gespeicherte Daten, einschließlich Inhalte?
- Wie kann die Rechtshilfe wirksamer gestaltet werden?
- Wie können effiziente und wirksame Maßnahmen mit Rechtsstaatlichkeit und Datenschutzanforderungen in Einklang gebracht werden?

17

Staatsanwalts|Akademie

ACCESS TO EVIDENCE "TRANSBORDER": 2ND PROTOCOL

Tools of the Second Protocol:

Chapter II: Measures for enhanced cooperation

Article 6 Request for domain name registration information ►**Public2Private**

Article 7 Disclosure of subscriber information ►**Public2Private**

Article 8 Giving effect to orders from another party for expedited production of subscriber information and traffic data ►Public2Public

Article 9 Expedited disclosure of stored computer data in an emergency ►Public2Public (via 24/7 network)

Article 10 Emergency mutual assistance ►Public2Public

Article 11 Video conferencing ►Public2Public

Article 12 Joint investigation teams and joint investigations ►Public2Public

18

Staatsanwalts|Akademie

ACCESS TO EVIDENCE "TRANSBORDER": 2ND PROTOCOL

Tools of the Second Protocol:

Chapter II: Maßnahmen zur verstärkten Zusammenarbeit

- Artikel 6 Anforderung von Informationen zur Domänennamenregistrierung ►Public2Private
- Artikel 7 Offenlegung von Teilnehmerinformationen ►Public2Private
- Artikel 8 Umsetzung von Anordnungen einer anderen Partei zur beschleunigten Herausgabe von Teilnehmerinformationen und Verkehrsdaten ►Public2Public
- Artikel 9 Beschleunigte Offenlegung gespeicherter Computerdaten im Notfall ►Public2Public (über ein rund um die Uhr verfügbares Netzwerk)
- Artikel 10 Gegenseitige Unterstützung in Notfällen ►Public2Public
- Artikel 11 Videokonferenzen ►Public2Public
- Artikel 12 Gemeinsame Ermittlungsgruppen und gemeinsame Ermittlungen ►Public2Public

19

Staatsanwalts|Akademie

ACCESS TO EVIDENCE "TRANSBORDER": 2ND PROTOCOL

Article 7 – Disclosure of subscriber information

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.

2. a. Each Party shall adopt such legislative and other measures as may be necessary for a service provider in its territory to disclose subscriber information in response to an order under paragraph 1.

…..

Optional notification regime

Reservations

Declarations

Enforcement via Article 8

20

Staatsanwalts|Akademie

ACCESS TO EVIDENCE “TRANSBORDER”: 2ND PROTOCOL

Artikel 7 – Offenlegung von Bestandsdaten

1. Jede Vertragspartei ergreift die erforderlichen gesetzgeberischen und sonstigen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen, eine Anordnung zu erlassen, die direkt an einen Diensteanbieter im Hoheitsgebiet einer anderen Vertragspartei zu richten ist, um die Offenlegung bestimmter, gespeicherter Bestandsdaten zu erwirken, die sich im Besitz oder unter der Kontrolle dieses Diensteanbieters befinden, wenn die Teilnehmerinformationen für die spezifischen strafrechtlichen Ermittlungen oder Verfahren der erlassenden Vertragspartei benötigt werden.

2. a. Jede Vertragspartei ergreift die erforderlichen gesetzgeberischen und sonstigen Maßnahmen, damit ein Diensteanbieter in ihrem Hoheitsgebiet Bestandsdaten als Reaktion auf eine Anordnung gemäß Absatz 1 offenlegen kann..

…..

Optional notification regime

Reservations

Declarations

Enforcement via Article 8

Staatsanwalts|Akademie

ACCESS TO EVIDENCE “TRANSBORDER”: 2ND PROTOCOL

► Efficiency with safeguards

- Article 2 – scope of Protocol: specific criminal investigations or proceedings related to cybercrime and e-evidence
- Article 13 incorporates Article 15 of the Convention to ensure the adequate protection of human rights and liberties and that provides for the principle of proportionality
- Article 14 provides for detailed data protection safeguards that are unique for a criminal justice treaty
- Articles specify types of data to be disclosed
- Articles specify information to be included to permit application of domestic safeguards
- Reservations and declarations to permit domestic safeguards and limit information to be provided

Staatsanwalts|Akademie

ACCESS TO EVIDENCE "TRANSBORDER": 2ND PROTOCOL

► Efficiency with safeguards

- Artikel 7 – Offenlegung des Abonnenten in Artikel 2 – Geltungsbereich des Protokolls:
- spezifische strafrechtliche Ermittlungen oder Verfahren im Zusammenhang mit Cyberkriminalität und elektronischen Beweismitteln
- Artikel 13 übernimmt Artikel 15 der Konvention, um einen angemessenen Schutz der Menschenrechte und Freiheiten zu gewährleisten, und sieht den Grundsatz der Verhältnismäßigkeit vor
- Artikel 14 sieht detaillierte Datenschutzvorkehrungen vor, die für einen Strafrechtsvertrag einzigartig sind
- Artikel spezifizieren die Arten der offenzulegenden Daten Artikel spezifizieren die aufzunehmenden Informationen, um die Anwendung innerstaatlicher Schutzmaßnahmen zu ermöglichen
- Vorbehalte und Erklärungen, um innerstaatliche Schutzmaßnahmen zu ermöglichen und die Bereitstellung von Informationen zu begrenzen

Staatsanwalts|Akademie

CURRENT DEVELOPMENTS: UN TREATY

Background:

- UNGA initiative by Russia ► Dec 2019: UNGA Resolution 74/247 ► Decision to establish an Ad Hoc Committee (AHC) to elaborate "a comprehensive international convention on countering the use of information and communications technologies for criminal purposes".
- Feb 2022 – Aug 2024: 8 formal sessions and numerous informal and intersessional meetings of the AHC
- 8 Aug 2024: Agreement by AHC on the draft text of a UN treaty and a draft resolution for submission to and adoption by UNGA

Result:

Draft "United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes"

Staatsanwalts|Akademie

CURRENT DEVELOPMENTS: DRAFT UN TREATY

AHC agreement on draft UN treaty:

- Major political success considering history and current international context.
- A narrow criminal justice treaty.
- Largely consistent with BC.
- Draft UN treaty is broader in some (crime proceeds) and narrower in other (scope of international cooperation) respects than BC.
- With minimum safeguards necessary for international cooperation.
- Maximum achievable and agreeable result.
- Will benefit cooperation between and with States that are not Parties to the BC.
- Will take some years until it be in force and operational.
- Protocol negotiations to commence two years after adoption by UNGA

25

Staatsanwalts|Akademie

CURRENT DEVELOPMENTS: DRAFT UN TREATY

AHC agreement on draft UN treaty:

- Großer politischer Erfolg in Anbetracht der Geschichte und des aktuellen internationalen Kontexts.
- Ein enger Strafrechtsvertrag.
- Großteils im Einklang mit BC.
- Der UN-Vertragsentwurf ist in mancher Hinsicht (Erlöse aus Straftaten) weiter gefasst und in anderer Hinsicht (Umfang der internationalen Zusammenarbeit) enger gefasst als BC. Mit den für die internationale Zusammenarbeit erforderlichen Mindestschutzmaßnahmen.
- Maximal erreichbares und akzeptables Ergebnis.
- Wird der Zusammenarbeit zwischen und mit Staaten zugutekommen, die nicht Vertragsstaaten des BC sind.
- Es wird einige Jahre dauern, bis es in Kraft und einsatzbereit ist.
- Die Protokollverhandlungen beginnen zwei Jahre nach der Annahme durch die Generalversammlung der Vereinten Nationen

26

Staatsanwalts|Akademie

CURRENT DEVELOPMENTS: DRAFT UN TREATY

Core concepts and measures of the draft treaty

- are drawn from the BC on Cybercrime (2001)
- complemented by provisions adapted from the UN Conventions on Transnational Organised Crime (UNTOC, 2000) and Corruption (UNCAC, 2003

► confirms the timeless quality and relevance of the BC

Example:

Art.	Budapest Convention		Draft UN treaty
2	Rechtswidriger Zugang	7	Illegal access
3	Rechtswidriges Abfangen	8	Illegal interception
4	Eingriff in Daten	9	Interference with electronic data
5	Eingriff in ein System	10	Interference with an information and communications technology system
6	Missbrauch von Vorrichtungen	11	Misuse of devices
7	computerbezogene Fälschung	12	Information and communications technology system-related forgery
8	Computerbezogener Betrug	13	Information and communications technology system-related theft or fraud
9	Kinderpornographie	14	Offences related to online child sexual abuse or child sexual exploitation material

Staatsanwalts|Akademie

CURRENT DEVELOPMENTS: DRAFT UN TREATY

New in draft UN treaty:

- Solicitation or grooming of children for sexual offences (Article 15)
- Non-consensual dissemination of intimate images (Article 16)
- Adapted from UNTOC and UNCAC: measures on money laundering and crime proceeds
- Safeguards beyond UNTOC and UNCAC

NOT in draft UN treaty:

- None of the measures of the Second Protocol to the BC on enhanced cooperation and disclosure of electronic evidence (2022)
- No transborder access to data (Article 32 BC)

Staatsanwalts|Akademie

CURRENT DEVELOPMENTS: DRAFT UN TREATY

Neu im UN-Vertragsentwurf:

Anwerbung oder Anbahnung von Kindern für Sexualstraftaten (Artikel 15)

Nicht einvernehmliche Verbreitung intimer Bilder (Artikel 16)

Adaptiert von UNTOC und UNCAC: Maßnahmen zu Geldwäsche und Erträgen aus Straftaten Schutzmaßnahmen über UNTOC und UNCAC hinaus

NICHT im UN-Vertragsentwurf:

Keine der Maßnahmen des zweiten Protokolls zum BC über verstärkte Zusammenarbeit und Offenlegung elektronischer Beweismittel (2022)

Kein grenzüberschreitender Zugriff auf Daten (Artikel 32 BC)

Staatsanwalts|Akademie

CURRENT DEVELOPMENTS: DRAFT UN TREATY

Risks/concerns:

- Risk that some States will not respect human rights and rule of law conditions*. Conference of States Parties (COSP) unlikely to review compliance.
- Risk of targeting assets of individuals, private sector organisations, media or civil society organisations through combination of provisions on fraud, money laundering, corporate liability, participation and attempt, and crime proceeds.
- Risk of supplementary criminalisation through a protocol (negotiations to commence two years after adoption of the convention as per draft UNGA resolution.

► Concerns raised by governments, civil society and industry stakeholders during the AHC process remain valid.

► Governments to decide on signature and ratification.

Staatsanwalts|Akademie

CURRENT DEVELOPMENTS: DRAFT UN TREATY

Risiken/Bedenken:

- Risiko, dass einige Staaten die Menschenrechte und die Bedingungen der Rechtsstaatlichkeit nicht respektieren*.
- Die Konferenz der Vertragsstaaten (COSP) wird die Einhaltung wahrscheinlich nicht überprüfen.
- Risiko, dass Vermögenswerte von Einzelpersonen, Organisationen des privaten Sektors, Medien oder Organisationen der Zivilgesellschaft durch eine Kombination von Bestimmungen zu Betrug, Geldwäsche, Unternehmenshaftung, Beteiligung und Versuch sowie Erträgen aus Straftaten ins Visier genommen werden.
- Risiko zusätzlicher Kriminalisierung durch ein Protokoll (Verhandlungen beginnen zwei Jahre nach Annahme des Übereinkommens gemäß dem Entwurf der UNGA-Resolution.
- Die während des AHC-Prozesses von Regierungen, der Zivilgesellschaft und Interessenvertretern der Industrie geäußerten Bedenken bleiben gültig.
- Die Regierungen entscheiden über Unterzeichnung und Ratifizierung.

Staatsanwalts|Akademie

CURRENT DEVELOPMENTS: DRAFT UN TREATY

Implications for Convention on Cybercrime (Budapest Convention):

- BC with its Protocols will remain the more relevant framework in the foreseeable future.
- Synergies between both treaties (including capacity building) feasible.
- More States will seek accession to the BC (based on experience during AHC process).
- However, a clear commitment to meeting human rights and rule of law conditions will be necessary when governments are seeking accession to the Budapest Convention on Cybercrime.

Staatsanwalts|Akademie

CURRENT DEVELOPMENTS: DRAFT UN TREATY

Auswirkungen auf die Konvention über Cyberkriminalität (Budapester Konvention):

- Die Konvention über Cyberkriminalität mit ihren Protokollen wird in absehbarer Zukunft der relevantere Rahmen bleiben.
- Synergien zwischen beiden Verträgen (einschließlich Kapazitätsaufbau) sind möglich.
- Weitere Staaten werden den Beitritt zur Konvention über Cyberkriminalität anstreben (basierend auf den Erfahrungen während des AHC-Prozesses).
- Wenn Regierungen jedoch den Beitritt zur Budapester Konvention über Cyberkriminalität anstreben, ist eine klare Verpflichtung zur Einhaltung der Bedingungen in Bezug auf Menschenrechte und Rechtsstaatlichkeit erforderlich.

Staatsanwalts|Akademie

Q & A

Alexander.seger@coe.int
www.coe.int/cybercrime