International Workshop on Cybercrime
Kizilcahamam / Ankara, 10-13 December 2018

Cybercrime and e-evidence – challenges and solutions under the Budapest Convention

Siber suçlar ve elektronik deliller– Budapeşte Sözleşmesi kapsamındaki zorluklar ve çözümler

Alexander Seger
Head of Cybercrime Division
Council of Europe
alexander.seger@coe.int

www.coe.int/cybercrime

Cybercrime and electronic evidence: Cooperate!
Siber suç ve elektronik kanıt: İşbirliği!

Cooperation needed at all levels:

- Interagency cooperation
- Public / private cooperation
- International cooperation
- Trust

Turkey is a strong partner:

- Party to Budapest Convention
- Capacity building
- Expertise in cybercrime investigations and computer forensics
- Operational cooperation

Her düzeyde işbirliği gerekli:

- Kurumlararası işbirliği
- Kamu / özel sektör işbirliği
- Uluslararası işbirliği
- Güven

Türkiye güçlü bir ortaktır:

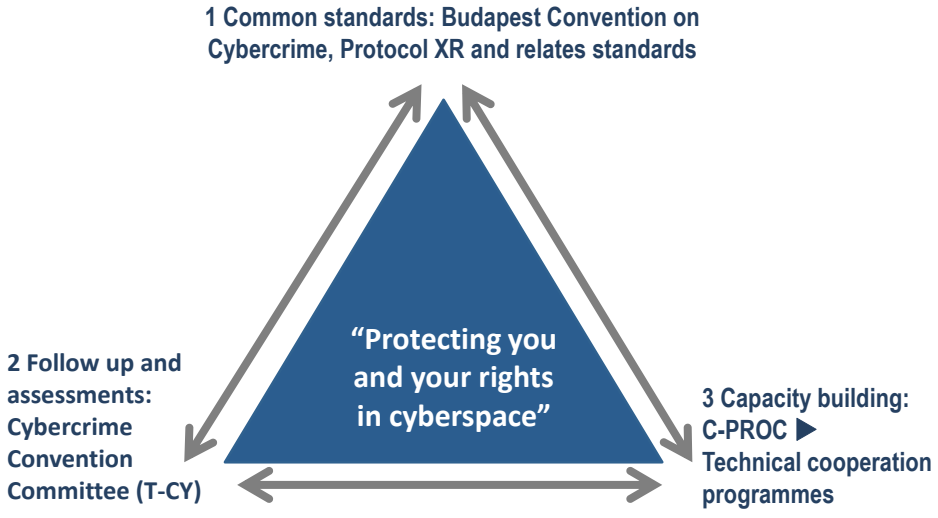
- Budapeşte Konvansiyonuna Taraf
- Kapasite oluşturma
- Siber suç soruşturmaları ve adli bilişimde uzmanlık
- Operasyonel işbirliği

Cybercrime and electronic evidence: Challenges
Siber suç ve elektronik delil: Zorluklar

- The scale and quantity of cybercrime, devices, users and victims
- Technical challenges
  - Virtual Private Networks (VPN)
  - Network Address Translators (CG-NATs)
  - Problem of attribution
- Cloud computing, territoriality and jurisdiction
- The challenge of mutual legal assistance
- Human rights and rule of law safeguards

- Siber suçun ölçeği ve miktarı, cihazlar, kullanıcılar ve mağdurlar
- Teknik zorluklar
  - Sanal Özel Ağlar (VPN)
  - Ağ Adresi Çeviricileri (CG-NATs)
  - İlişkilendirme sorunu
- Bulut bilişim, egemenlik bölgesi ve yargı yetkisi
- Karşılıklı adli yardımlaşmanın zorluğu
- İnsan hakları ve hukukun üstünlüğünü koruyan önlemler

Solutions under the Budapest Convention: Criminal justice response with safeguards
Budapeşte Sözleşmesi kapsamında çözümler: Önlemler ile ceza adaleti cevabı



Scope of Budapest Convention: cybercrime & e-evidence
Budapeşte Konvansiyonunun Kapsamı: siber suçlar ve e-delil

Criminalising conduct – offences against and by means of computers

Eylemi suç olarak tanımlama- bilgisayarlara karşı ve bilgisayar aracılığıyla eylemler

+

Procedural tools to secure e-evidence in relation to any crime

Herhangi bir suçla ilgili olarak elektronik delili güvence altına alacak prosedürler

Limited by safeguards

Şartlar ve koruma önlemer

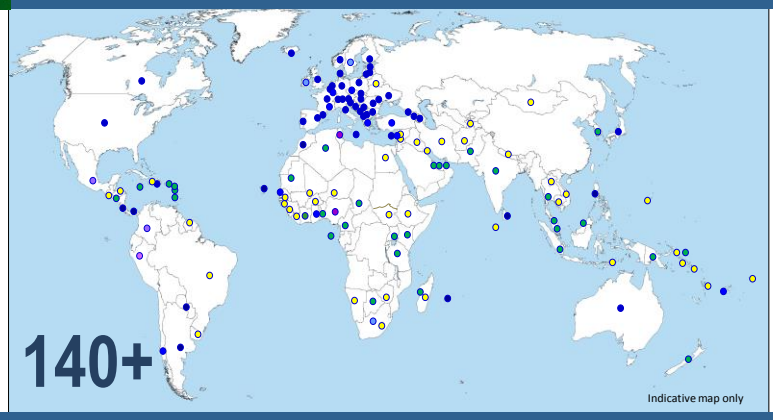
+

International cooperation on cybercrime and e-evidence

Siber suçlar ve elektronik deliller konusunda uluslararası işbirliği

Harmonisation
Uyum

Reach of the Budapest Convention
Budapeşte Konvansiyonuna Erişim



Ratified/acceded: 62

Signed: 4

Invited to accede: 5

= 71

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

Further States drawing on Budapest Convention for legislation = 50+

Capacity building

Kapasite geliştirme

Cybercrime@IPA (2010-2013)

iPROCEEDS (2016 – 2019):

- Turkey participated in more than 60 activities with 500+ officials
- Guidelines on online crime proceeds
- Cybercrime Simulation Exercises to promote interagency cooperation
- Indicators on online fraud and criminal money on the Internet (MASAK)
- Training courses for judges and prosecutors (Judicial Academy)
- Support to partnerships and sharing experience at
  - Cybercrime Convention Committee
  - EUROJUST
  - UNODC
  - UN Intergovermental Expert Group on Cybercrime

Cybercrime@IPA (2010-2013)

iPROCEEDS (2016 – 2019):

- Türkiye, 500'den fazla görevliyle 60'dan fazla etkinliğe katıldı
- Online suçlarla ilgili rehberler
- Kurumlararası işbirliğini geliştirmek için Siber Suç Simülasyon Egzersizleri
- İnternet üzerinde dolandırıcılık ve suçdan elde edilmiş paranın internette dolaşımıyla ilgili göstergeler (MASAK)
  Hâkimler ve savcılar için eğitim kursları (Adalet Akademisi)
  Ortaklığa destek ve tecrübe paylaşımı
  - Siber Suç Konvansiyonu Komitesi
  - EUROJUST
  - UNODC
  - BM Hükümetlerarası Siber Suç Uzmanlar

Towards a protocol to the Budapest Convention on Cybercrime

Siber Suçlarla İlgili Budapeşte Konvansiyonu'na Doğru Protokol

A. Provisions for more efficient MLA
- Emergency MLA
- Joint investigations
- Video conferencing
- Language of requests
- Etc.

B. Provisions for direct cooperation with providers in other jurisdictions

C. Framework and safeguards for existing practices of extending searches transborder

D. Safeguards/data protection

Terms of reference approved in June 2017.

Negotiations: Sep 2017 – Dec 2019.

Şartname Haziran 2017'de onaylandı.

Müzakereler: Eylül 2017 - Aralık 2019.

A. Daha etkili adli yardımlaşma için hükümler
- Acil MLA
- Ortak soruşturmalar
- Video konferans
- Taleplerin dili
- Vb.

B. Diğer yargı sahalarındaki sağlayıcılarla doğrudan işbirliği hükümleri

C. Mevcut sınır ötesi aramaların genişletilmesine ilişkin çerçeve ve koruma tedbirleri

D. Koruma tedbirleri/ veri koruma

Budapest Convention: some specific points
Budapeşte Sözleşmesi: Bazı özel konular

Article 14 ▶ Specific criminal investigation

Madde 14 ▶ Özel ceza soruşturması

Article 15 ▶ Conditions and safeguards, including independent judicial supervision

Madde 15 ▶ Bağımsız adli denetim dahil olmak üzere, şartlar ve koruma önlemer

Budapest Convention: some specific points
Budapeşte Sözleşmesi: Bazı özel noktalar

Article 19: Search and seizure ▶ Extending a search to a computer system IN the territory

Madde 19: Arama ve el koyma ▶ Bölgedeki (yargı sahası içerindeki) bir bilgisayar sistemine yapılan aramayı genişletme

Article 32 ▶ Transborder access IF voluntary and lawful consent of person who has lawful authority to disclose the data

Madde 32 ▶ Verilerin paylaşılması konusunda kanuni yetki sahibi olan kişinin, kanuna uygun bir şekilde gönüllü rızası olması durumunda, sınıraşan erişim

Some concerns

Bazı endişeler

Supreme Court of Cassation decision 2017/370 (24 April 2017)

Obtaining ByLock data by the MIT from a server in Lithuania legitimate because Budapest Convention:

- **permitting extension of searches**
- **transborder access to data**

Questions:

- **Specific criminal investigation?**
- **Independent judicial supervision?**
- **Consent?**
- **Basis for extending searches?**

Yargıtay Yüksek Mahkemesi kararı 2017/370 (24 Nisan 2017)

Litvanya'daki bir sunucudan MIT tarafından ByLock verilerinin elde edilmesi yasal çünkü Budapeşte Konvansiyonu:

- **aramaların genişletilmesine izin veriyor**
- **sınır aşan veriye erişim**

Sorular:

- **Özel bir ceza soruşturması mı?**
- **Bağımsız yargı gözetimi?**
- **Rıza ?**
- **Aramaları genişletme temelinde mi?**

Some concerns

Bazı endişeler

Further questions:

- **ByLock exclusively for members of FETÖ/PDY?**
- **ByLock operational April 2014 – March 2016 ▶ Not in July 2016, what role?**
- **Data obtained by MIT:**
  - **Judicial authorisation?**
  - **Forensic protocols? Reliability?**
  - **Admissibility under Constitution and CPC? Fruit of a poisonous tree?**
- **Attribution vs VPN, CG-NATs?**
- **Why is the simple fact of using ByLock evidence of a criminal offence?**
- **Retroactive criminal law?**

Diğer sorular:

- **ByLock sadece FETÖ / PDY üyeleri için mi?**
- **ByLock Nisan 2014 – Mart 2016 arası aktif ▶ Temmuz 2016'da değil, rolü nedir?**
- **MIT tarafından elde edilen veriler:**
  - **Yargı yetkisi?**
  - **Adli protokoller? Güvenilirliği?**
  - **Anayasa ve CMK kapsamında kabul edilebilirlik? Zehirli bir ağacın meyvesi mi?**
- **VPN, CG-NATs vs ilişkilendirmesi?**
- **ByLock kullanımının suç delili olmasının basit sebebi nedir?**
- **Geriye dönük ceza hukuku?**

Some concerns

Bazı endişeler

UN Human Rights Council – Working Group on Arbitrary Detention (October 2018)

Opinions 42/2018 and 44/2018:

- **"Failure to show how the mere use of a regular communication application as ByLock constituted an illegal criminal activity …"**
- **"Deprivation of liberty is arbitrary …"**

BM İnsan Hakları Konseyi - Keyfi Gözaltılar Çalışma Grubu (Ekim 2018)

Görüşler 42/2018 ve 44/2018:

- **"ByLock gibi normal bir iletişim uygulamasının sadece kullanımının yasadışı bir suç faaliyeti oluşturduğunu gösterememek…"**
- **"Özgürlükten yoksun bırakma keyfidir…"**

Conclusions

Sonuçlar

- Turkey is a strong Party to the Budapest Convention.
- Much experience to share.
- Turkey needed as a partner against cybercrime.
- Council of Europe prepared to support further capacity building, including for judges and prosecutors.
- Clear legal basis and procedures for electronic evidence in place.
- Reassurance needed that laws and procedures are applied in practice and that rule of law requirements are respected.

- Türkiye, Budapeşte Konvansiyonuna güçlü bir Taraftır.
- Paylaşacak çok deneyimi var.
- Siber suçlarla mücadelede Türkiye'nin ortaklığına ihtiyaç var.
- Avrupa Konseyi, hâkimler ve savcılar da dahil olmak üzere daha fazla kapasite geliştirmeye destek vermeye hazır.
- Net yasal dayanakların ve usullerin elektronik delil için uygulanması.
- Yasaların ve prosedürlerin pratikte uygulandığı ve hukukun üstünlüğünün gereklerine saygı duyulduğu konusunda şüphelerin giderilmesi gerekli.


Thank you for the dialogue on this difficult question!
Bu zor sorudaki diyalog için teşekkürler!
www.coe.int/cybercrime