Council of Europe

Seminar on cybercrime
Bolu, Turkey,
23-24 October 2008

Siber suçlarla (İnternet suçları) ilgili seminer,
Bolu, Türkiye,
23-24 Ekim 2008

The Convention on Cybercrime and its implementation in Turkey

Alexander Seger
Economic Crime Division, Council of Europe
Strasbourg, France
alexander.seger@coe.int

Siber suç Sözleşmesi ve Türkiye'de Uygulanması

www.coe.int/cybercrime

1

1

Council of Europe | I. About cybercrime

Why worry about cybercrime?

- Opportunities provided by information and communication technologies
- Information society
- Confidentiality, integrity, and availability of your computer data
- Reliance of public infrastructure on ICT
- Reliance of business on ICT
- Dependency of societies on ICT = vulnerability to cybercrime
- Need for secure and accessible ICT

Siber suçlardan neden endişe duymalıyız?

- Bilgi ve iletişim teknolojilerinin (BİT) sunduğu fırsatlar
- Bilgi toplumu
- Bilgisayar verilerinizin gizliliğine, doğruluğuna ve ulaşılabilirliğine karşı işlenen suçlar
- Kamu altyapısının BİT'e bağımlılığı
- İşletmelerin BİT'e bağımlılığı
- >Toplumların BİT'e bağımlılığı= siber suçlara karşı zaaf
- Emniyetli ve erişilebilir BİT'e ihtiyaç duyulması

2

2

What is cybercrime?

- Offences against the confidentiality, integrity and availability of computer data and systems
- Computer-related forgery and fraud
- Content-related offences
- Offences related to intellectual property rights and similar rights

Siber suç nedir?

- Bilgisayar veri ve sistemlerinin gizliliği, doğruluğu ve ulaşılabilirliğine karşı işlenen suçlar.
- Bilgisayarlarla ilgili sahtecilik ve dolandırıcılık
- İçerikle ilgili suçlar
- Fikri mülkiyet ve benzer haklar

3

3

What is cybercrime?

Offences against the confidentiality, integrity and availability of computer data and systems (CIA offences)

- Illegal access to a computer system
- Illegal interception
- Data interference
- System interference
- Misuse of devices

Siber suç nedir?

Bilgisayar veri ve sistemlerinin gizliliğine, doğruluğuna ve ulaşılabilirliğine karşı işlenen suçlar

- Bilgisayara yasal olmayan yollardan erişim sağlamak
- Yasal olmayan bir şekilde bilgisayara girmek
- Sistem enterferansı
- Cihazların kötüye kullanılması

4

4

Council of Europe | I. About cybercrime

What is cybercrime?

Computer-related forgery and fraud

Shift in the threat landscape: from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes

- Security breaches and financial losses in companies
- Credit card fraud and other financial crime
- Advance fee fraud
- Extortion
- Internet marketing and retail fraud
- Auction fraud and stock market manipulation
- Phishing and other forms of identity theft
- Etc.

Siber suç nedir?

Bilgisayarlarla ilgili sahtecilik ve dolandırıcılık

Tehdit ortamında değişiklik: geniş kapsamlı, kitlesel, çok amaçlı saldırılardan giderek daha ekonomik suç amaçlı ve spesifik kullanıcı, grup, kuruluş veya sanayilere yönelik spesifik saldırılar
Şirketlerde güvenlik boşlukları ve finansal kayıplar
- Kredi kartı dolandırıcılığı ve diğer finansal suçlar
- Peşin alınan ücretlerde dolandırıcılık
- Şantaj ve zorla para alma
- Internet pazarlama ve perakende satış dolandırıcılığı
- Açık arttırma dolandırıcılığı ve borsada manipülasyonu
- Oltalama (Phishing) ve diğer tür kimlik hırsızlıkları
- Vs.

5

5

Council of Europe | I. About cybercrime

What is cybercrime?

Content-related offences

- Child pornography
- Xenophobia, racism, hate speech

Issue:
- Security and protection versus freedom of expression

Siber suç nedir?

İçerikler ilgili suçlar

- Çocuk pornografisi
- Aşırı milliyetçilik, ırkçılık, nefret duygularını körükleyen konuşmalar

Sorun:
- İfade özgürlüğü karşısında emniyet ve koruma

6

6

What is cybercrime?

Offences related to intellectual property rights and similar rights

- IPR protected by national and international regulations
- Counterfeit products
- Health and safety risks
- Economic loss to companies and unfair competition
- Feeds organised crime

Siber suç nedir?

Fikri mülkiyet hakları (FMH) ve benzer haklarla ilgili suçlar

- Ulusal ve uluslararası yönetmeliklerle korunan FMH
- Sahte ürünler
- Sağlık ve emniyet riskleri
- Şirketlere ekonomik kayıplar verdirilmesi ve haksız rekabet
- Organize suçun beslenmesi

7

7

What is cybercrime?
Key issues

Malware

- Software inserted into an information system that causes harm to this or other systems
- Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading

Siber suç nedir? Temel Sorunlar

Kötü amaçlı yazılım

- Bilgi sistemine yerleştirilen ve hem o sisteme hem de diğer sistemlere zarar veren yazılım
- Kötü amaçlı yazılım – yani, sürekli geliştirilen ve süratle yayılan, virüsler, 'solucan'lar, 'Truva atları', casus yazılımlar, 'bot'lar ve bot ağları gibi kötü amaçlı kod ve programlar

8

8

What is cybercrime?
Key issues

SPAM

- Accounts for a large amount of internet traffic (70%+)
- Vector for malware

Siber suç nedir?
Temel konular

SPAM

- Internet trafiğinin büyük bir bölümüne (%70) tekabül etmektedir
- Kötü amaçlı yazılımın taşıyıcısıdır

9

9

What is cybercrime?
Key issues

Bots and botnets

Covertly installed programmes on a computer to allow unauthorised remote control

Can be used:

- for distributed denial of service (DDOS) attacks
- to harvest confidential information (identity theft)
- to distribute spam, spyware, adware
- for phishing attacks

Siber suç nedir?
Temel konular

'Bot'lar ve bot ağları

Yetkisiz uzaktan kontrol sağlayan ve bilgisayara gizlice yerleştirilmiş programlar

Şu amaçlarla kullanılır:

- Hizmeti engelleyen dağıtık saldırılar
- Gizli bilgi elde etme (kimlik bilgileri hırsızlığı)
- Spam, casus yazılım ve reklam yazılımını yayma
- Oltalama (phishing) saldırıları

10

10

Council of Europe | I. About cybercrime

What is cybercrime?
Key issues

Phishing and other forms of identity theft

Obtaining identity information

Illegal access, Illegal interception, Data interference, System interference, Misuse of devices

Possessing, transferring, use

Attempt, aiding, abetting

Fraud and other offences

Siber suç nedir?
Temel konular

Oltalama ve diğer kimlik bilgileri hırsızlıkları

Kimlik bilgilerinin elde edilmesi

Yasadışı erişim, yasadışı müdahale, verilere müdahale, sisteme müdahale, cihazların kötü amaçlı kullanımı

Elde etme, aktarma,kullanma

Teşebbüste bulunma, yardım ve yataklık etme

Dolandırıcılık ve diğer suçlar

11

11

Council of Europe | I. About cybercrime

What is cybercrime?
Key issues

Cybercrime and organised crime

- Offenders increasingly organising for cybercrime
- Botnets an important tool
- ICT facilitate offences by OC groups and networks, in particular economic crime
- ICT creates vulnerabilities -> exploited by OC
- ICT facilitate logistics, anonymity and reduce risks of OC
- ICT facilitate global outreach of OC
- ICT shape OC -> networks

Siber suç nedir?
Temel konular

Siber suç ve organize suç

- Suçlular giderek daha çok siber suç için organize olmaktadırlar
- Botnet'ler önemli bir araç olarak kullanılmaktadır
- Bilgi ve İletişim Teknolojileri (BİT) organize suç (OS) grup ve şebekelerinin özellikle ekonomik suçlarını kolaylaştırmaktadır
- BİT, OS tarafından yararlanılan zaafları yaratmaktadır
- BİT OS unsurlarına lojistik, kimliklerini gizleme imkanı vermekte ve risklerini azaltmaktadır
- BİT OS unsurlarının tüm dünyaya erişimini kolaylaştırmaktadır
- BİT, OS şebekelerine yön vermektedir

12

12

What is cybercrime?
Key issues

Terrorist use of the internet/ICT

- Possible attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interests, including loss of life
- Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism, recruitment or training
- Use of ICT by terrorists for logistical purposes such as internal communication, gathering intelligence, target analyses

Siber suç nedir?
Temel konular

Internet'in ve BİT'in teröristlerce kullanımı

- Cana yönelik saldırılar da dahil olmak üzere, kritik öneme sahip bilgi altyapısına ve diğer çok önemli altyapı, bilgisayar sistemleri ve yasal menfaatlere muhtemel saldırılar
- Terör saldırısı tehditleri, terör eylemlerine teşvik ve bunların yaygınlaştırılması, teröre eleman sağlama ve eğitim sağlama da dahil olmak üzere, yasadışı içeriğin yayımlanması
- BİT'nin dahili iletişim, istihbarat toplama ve hedef analizi gibi lojistik amaçlarla teröristlerce kullanılması

13

13

II. The Convention on Cybercrime as a response

II. Siber suç sözleşmesinin saldırılara bir cevap olarak kullanılması

www.coe.int/cybercrime

14

14

Cybercrime: the criminal law response

- Criminalise certain conduct ▶ substantive criminal law
- Give law enforcement/criminal justice the means to investigate, prosecute and adjudicate cybercrimes (immediate actions, electronic evidence) ▶ criminal procedure law
- Allow for efficient international cooperation ▶ harmonise legislation, make provisions and establish institutions for police and judicial cooperation, conclude or join agreements

15

15

Siber suç: ceza hukukunun buna cevabı

- Belirli eylemlerin suç sayılması ▶ maddi cezai hukuku önlemleri
- Kolluk kuvvetlerine/ceza yargı organlarına siber suçları soruşturma, kovuşturma ve yargı önüne çıkarma (ani önlemler, elektronik kanıtlar) vasıtalarını sağlama ▶ ceza usulü kanunu
- Etkili uluslararası işbirliğini mümkün kılma ▶ mevzuatın uyumlaştırılması, polis-yargı işbirliği için tedbirler alınması ve kurumlar ihdas edilmesi, anlaşmalar yapılması veya bunlara dahil olunması

15

16

A response to this challenge:

The Convention on Cybercrime

- Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA
- Opened for signature in Budapest in November 2001
- In force since July 2004

The Protocol on Xenophobia and Racism Committed through Computer Systems

- Opened for signature in January 2003
- In force since March 2006

16

Bu soruna gösterilen reaksiyon:

Siber Suç Sözleşmesi

- Kanada, Japonya, Güney Afrika ve ABD'nin katılımıyla Avrupa Konseyi tarafından oluşturulmuştur
- 2001 Kasım ayında Budapeşte'de imzaya açılmıştır
- 2004 Temmuz ayından beri yürürlüktedir

Bilgisayar Sistemleri Üzerinden Gerçekleştirilen Aşırı Milliyetçilik ve Irkçılığa İlişkin Protokol

- 2003 Ocak ayında imzaya açılmıştır
- 2006 Mart ayından beri yürürlüktedir

16

Structure and content of the Convention

Chapter I: Definitions

Chapter II: Measures at national level
- Section 1 - Substantive criminal law
- Section 2 - Procedural law
- Section 3 - Jurisdiction

Chapter III: International cooperation
- Section 1 - General principles
- Section 2 - Specific provisions

Chapter IV: Final provisions

Sözleşmenin yapısı ve içeriği

Bölüm I: Tanımlar

Bölüm II: Ulusal Düzeyde Alınacak Önlemler
Kısım 1 – Maddi Ceza Hukuku
Kısım 2 – Usul Hukuku
Kısım 3 – Yargı Yetkisi

Bölüm III: Uluslararası İşbirliği
Kısım 1 - General ilkeler
Kısım 2 – Özel hükümler

Bölüm IV: Nihai hükümler

17

17

Criminalising conduct

Chapter II – Measures at national level

Section 1 – Substantive criminal law

- Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices)
- Title 2 – Computer-related offences (forgery, fraud)
- Title 3 – Content-related offences (child pornography)
- Title 4 – Infringements of copyright and related rights
- Title 5 – Ancillary liability and sanctions (attempt, aiding, abetting, corporate liability, sanctions and measures)

Bazı eylemlerin suç sayılması

Bölüm II – Ulusal düzeyde alınacak eylemler

Kısım 1 – Maddi Ceza Hukuku

- Madde 1 - Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar (yasadışı erişim, yasadışı müdahale, verilere müdahale, bilgisayar sistemlerine müdahale, cihazların kötüye kullanılması)
- Madde 2 – Bilgisayarlarla ilişkili sahtecilik fiilleri (sahtecilik, sahtekarlık)
- Madde 3 – İçerikle ilgili suçlar (Çocuk pornografisi)
- Madde 4 – Telif Hakları ve benzer hakların ihlali
- Madde 5 – İlave yükümlülük ve yaptırımlar (teşebbüste bulunmak, yardım ve yataklık etmek, kurumsal yükümlülükler, yaptırım ve önlemler)

18

18

Procedural tools

Section 2 – Procedural law

- Title 1 – Common provisions (scope of procedural provisions, conditions and safeguards)
- Title 2 – Expedited preservation of stored computer data (and traffic data and partial disclosure)
- Title 3 – Production order
- Title 4 – Search and seizure of stored computer data
- Title 5 – Real-time collection of computer data (traffic data, interception of content data)

These apply to all criminal offences involving a computer system!

Usule ilişkin araçlar

Kısım 2 – Usul hukuku

- Madde 1 – Genel Hükümler (usule ilişkin hükümlerin kapsamı, şartları ve önlemler)
- Madde 2 – Saklanan Bilgisayar verilerinin korunmasının kolaylaştırılması (Trafik Bilgilerinin Korunmasının Kolaylaştırılması ve Kısmen Açıklanması)
- Madde 3 – Üretim Talimatı
- Madde 4 – Saklanan bilgisayar verilerinin aranması ve bunlara el konulması
- Madde 5 – Bilgisayar bilgilerinin gerçek zamanlı olarak toplanması (trafik bilgiler, içerik bilgilerine el konması)

Bunlar bilgisayar sistemlerine ilişkin tüm suçları kapsamaktadır!

19

19

Art 15 Common provisions

Scope of procedural provisions

- Apply to all offences involving a computer system

Conditions and safeguards

- powers and procedures to be subject to conditions and safeguards provided for under domestic law, which shall provide for the adequate protection of human rights and liberties
- principle of proportionality
- judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure

Madde 15 Genel hükümler

Usul hükümlerinin kapasmı

- Bilgisayar sistemini içeren tüm suçlar için geçerlidir

Şartlar ve Önlemler

- Yetki ve usuller insan hak ve özgürlüklerinin yeterli bir biçimde korunmasını sağlayacak olan iç hukuk şart ve önlemlerine tabi olacaktır
- Orantılılık ilkesi
- Adli veya başka nitelikli bağımsız denetim, söz konusu usul ve şartların uygulanmasını gerekli kılan şartlar ve bu yetki ve usullerin kapsam ve süresinin sınırlı olması

20

20

Chapter III - International cooperation

Section 1 – General principles

Section 2 – Specific provisions

- Art 29 - Expedited preservation of stored computer data
- Art 30 - Expedited disclosure of preserved computer data
- Art 31 - Mutual assistance re accessing stored computer data
- Art 32 - Trans-border access to stored computer data
- Art 33 - Mutual assistance in real-time collection of traffic data
- Art 34 - Mutual assistance re interception of content data
- Art 35 - 24/7 network

Bölüm III – Uluslararası işbirliği

Kısım 1 – Genel ilkeler
Kısım 2 – Özel hükümler
•Madde 29 - Saklanan Bilgisayar Verilerinin Korunmasının Kolaylaştırılması
•Madde 30 – Saklanan Bilgisayar bilgilerinin açıklanmasının kolaylaştırılması
•Madde 31 – Saklanan bilgisayar bilgilerine erişimde karşılıklı yardım
•Madde 32 – Saklanan bilgisayar bilgilerine sınır ötesinde erişim
•Madde 33 - Trafik bilgilerinin gerçek zamanlı olarak toplanmasında karşılıklı yardım
• Madde 34 – İçerikle ilgili bilgilere müdahale edilmesinde karşılıklı yardım
•Madde 35 – 7 gün 24 saat boyunca elverişli ağ

21

21

Article 35 – 24/7 Network

Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance … Such assistance shall include facilitating, or … directly carrying out the following measures:

- the provision of technical advice;
- the preservation of data pursuant to Articles 29 and 30;
- the collection of evidence, the provision of legal
- information, and locating of suspects.

Based on the G8 experience

Madde 35 – 7 gün 24 saat boyunca elverişli ağ

Taraflardan her biri, en kısa sürede yardım temin edilmesini sağlamak üzere haftanın 7 günü 24 saat boyunca temas kurulabilecek bir irtibat noktası belirleyecektir. Söz konusu yardım, aşağıdakilerin kolaylaştırılması ya da ulusal yasa ve uygulamaların uygun görmesi halinde doğrudan yapılması ile olacaktır:
➢Teknik bilgi sağlanması;
➢Madde 29 ve 30 uyarınca verilerin korunması ;
➢Delil toplanması, yasal bilgilerin verilmesi, şüphelilerin yerlerinin bulunması .

G8 deneyimine dayalı olarak

22

22

Chapter III - International cooperation

Art 37 Convention is open for accession by third countries

- Global scope of the Convention

Bölüm III – Uluslararası İşbirliği

Madde 37 Sözleşme üçüncü ülkelerin katılımına açıktır

- Sözleşmenin global kapsamı

23

23

Supervision of the treaty

Art 46 Consultation of the Parties (Cybercrime Convention Committee, T-CY)

- Facilitate effective implementation of the treaty and identify problems
- Facilitate information exchange
- Consider possible amendments or supplements to the treaty

Sözleşmenin denetlenmesi

Madde 46 Tarafların istişaresi (Siber suç Sözleşme Komitesi, T-CY)

- Sözleşmenin etkili bir şekilde uygulanmasını kolaylaştırma ve sorunları belirleme
- Bilgi alışverişini kolaylaştırma
- Sözleşmede muhtemel değişiklikler ve ilaveler yapılması

24

24

Implementation – current status

➢The Convention entered into force in July 2004

➢23 ratifications + 22 signatures

➢Signed by Canada, Japan, South Africa, ratified by USA

➢Costa Rica, Mexico, Philippines have been invited to accede

➢Legislative amendments adopted or underway in many other countries and accession to the Convention under consideration

= Major global trend towards better cybercrime legislation

= Convention provides a global standard

Uygulama – mevcut durum

➢Sözleşme 2004 Temmuz ayında yürürlüğe girmiştir

➢23 ülke kabul etmiş + 22 ülke imzalamıştır

➢Kanada, Japonya, Güney Afrika imzalamış, ABD kabul etmiştir

➢Kosta Rika, Meksika, Filipinler katılmaya davet edilmişlerdir

➢Diğer pekçok ülkede yasal değişiklikler kabul edilmiş veya kabul edilme sürecindedir ve sözleşmeye katılma konusu değerlendirilmektedir

➢= Daha iyi siber suç mevzuatı konusunda büyük bir global eğilim mevcuttur

= Sözleşme global bir standart sağlamaktadırConvention provides a global standard

25

25

III. Implementation of the Convention by Turkey

Turkey has not yet signed nor ratified the Convention on Cybercrime …

III. Sözleşmenin Türkiye tarafından uygulanması

Türkiye Siber suç sözleşmesini henüz imzalamamış ve kabul etmemiştir …

26

26

Council of Europe | III. Implementation by Turkey

Substantive law: How does Turkey criminalise:

- Art 2 Illegal access to a computer system
- Art 3 Illegal interception
- Art 4 Data interference
- Art 5 System interference
- Art 6 Misuse of devices
- Art 7 Computer-related forgery
- Art 8 Computer-related fraud
- Art 9 Child pornography
- Art 10 Copy-right violations

Maddi hukuk: Türkiye söz konusu eylemleri nasıl suç kapsamına almaktadır:

- Madde 2 Bilgisayar sistemlerine yasadışı erişim
- Madde 3 Yasadışı müdahale
- Madde 4 Verilere müdahale
- Madde 5 Sisteme müdahale
- Madde 6 Cihazların kötüye kullanımı
- Madde 7 Bilgisayarlarla ilişkili sahtecilik
- Madde 8 Bilgisayarlarla ilişkili dolandırıcılık
- Madde 9 Çocuk pornografisi
- Madde 10 Telif hakları ihlalleri

27

27

Council of Europe | III. Implementation by Turkey

Procedural law: does Turkish legislation provide for:

- Art 16 + 17 Expedited preservation
- Art 18 Production order
- Art 19 Search and seizure
- Art 20 Real-time collection of traffic data
- Art 21 Interception of content data

Usul Hukuku: Türk hukukunda aşağıdakiler sağlanmakta mıdır:

- Madde 16 + 17 Korunmanın kolaylaştırılması
- Madde 18 Üretim emri
- Madde 19 Arama el koyma
- Madde 20 Trafik bilgilerinin gerçek zamanlı olarak toplanması
- Madde 21 İçerik bilgilerine el koyma

28

28

Conclusions

- Most provisions of the Convention are probably covered in Turkish legislation already
- Amendments to the criminal law should be undertaken to close gaps
- Turkey could sign the Convention on Cybercrime already now
- It is important for Turkey and for other countries that Turkey becomes a party to the Convention as soon as possible

Sonuçlar

- Sözleşmedeki hükümlerin çoğu muhtemelen Türk hukukunda halen yer almaktadır
- Boşlukları kapatmak için ceza hukukunda değişiklikler yapılmalıdır
- Türkiye şimdiden Siber Suç Sözleşmesini imzalayabilir
- Türkiye'nin sözleşmeye en kısa zamanda taraf olması Türkiye ve diğer ülkeler için önemlidir

29

29

Teşekkürler

Thank you

Alexander.seger@coe.int

30

30