**Program specijalističke obuke iz oblasti kibernetičkog (Cyber) kriminala za tužioce[[1]](#footnote-1)**

**Uvod**

Posljednjih godina u mnogim društvima u svijetu učinjen je ogroman napredak ka informatizaciji društva. Danas informacijske i komunikacijske tehnologije (IKT) prodiru u gotovo sve sfere života.

Zbog sve većeg oslanjanja na ove tehnologije, a time i ovisnosti o njima, društvo postaje podložno prijetnjama kao što su kibernetički kriminal, tj. krivična djela protiv kompjuterskih podataka ili sistema ili učinjena upotrebom kompjuterskih podataka ili sistema.

Kriminalno ponašanje brzo se mijenja iskorištavajući razvoj tehnologija i rupe u zakonu. Kriminalci će i ubuduće biti kreativni i primjenjivati sofisticirane napade da zarade više novca, a mi moramo držati korak s njima. Stoga osposobljavanje tužilaca i predstavnika agencija za sprovođenje zakona direktno pomaže u toj borbi.

U izvještaju Evropskog centra za kibernetički kriminal[[2]](#footnote-2) za 2013 godinu navodi se sljedeće:

Trenutno oko 2,5 milijardi ljudi diljem svijeta ima pristup internetu te se procjenjuje da će još oko 1,5 milijardi ljudi dobiti pristup u sljedeće četiri godine. Budući da će naš internetski život, sa svim svojim neizmjernim prednostima, i dalje rasti, rast će i naša izloženost internetskom kriminalu. Buduće prijetnje i kretanja u kibernetičkom kriminalu, kako se predviđa, će biti:

***Broj kriminalaca u porastu.*** *Prag za ulazak u posao s kibernetičkim kriminalom postaje vrlo nizak. Sve vrste kibernetičkog kriminala mogu se obaviti čak i bez tehničkih vještina – razbijanje lozinke, upadi u računarski sustav, prilagođeni zlonamjerni napadi ili DdoS napadi.*

***Veća potražnja.*** *Očekuje se da će se potražnja za uslugama kibernetičkog kriminala i njegovo korištenje povećati što će dovesti do još jačeg rasta razvoja, testiranja i distribucije zlonamjernih programa; izrade i primjene „botneta”; krađe akreditiva za plaćanje i trgovanja njima te usluga pranja novca.*

***Veća sofisticiranost.*** *Očekuje se razvoj agresivnijih i otpornijih vrsta zlonamjernih programa. To uključuje „ransomware” s naprednijim i složenijim šifriranjem; otpornije „botnete”; zlonamjerne programe za bankarstvo i napredne, sofisticirane trojanske viruse u cilju izbjegavanja zaštitnih mjera financijskih institucija.*

***Prelazak na mobitele.*** *U razvoju zlonamjernih programa očekuje se pomak prema djelovanju i distribuciji preko mobilnih uređaja.*

***Pametnija distribucija.*** *U narednim godinama očekuju se novi načini distribucije agresivnih i otpornih vrsta zlonamjernih programa. U porastu je i zabrinjavajuća pojava gdje se dječja pornografija nudi uživo preko interneta.*

***Povećana potreba za pranjem novca.*** *Kriminalci će tražiti jednostavne načine za unovčenje i pranje dobiti. Dodatno će porasti potražnja za e-valutama i drugim anonimnim sustavima platnog prometa.*

***Usluge „u oblaku“*** *[[3]](#footnote-3)* ***na meti.*** *Upadi u usluge u oblaku (cloud service) kriminalcima su sve zanimljiviji. Očekuje se da će kriminalci sve više upadati u takve usluge radi špijuniranja, pronalaženja akreditiva i iznude.*

Imajući u vidu navedeno, osim velikog broja krivičnih djela protiv ili upotrebom IKT-a, sve je veći broj drugih predmeta koji završavaju na sudu a u kojima se pojavljuju elektronski dokazi pohranjeni u kompjuterskom sistemu ili nekom drugom uređaju.

Zbog svega toga i tužioci moraju biti spremni da se bave kibernetičkim kriminalom i elektronskim dokazima. Značaj IKT-a u današnjem društvu je takav da sudije i tužioci moraju posjedovati barem osnovno poznavanje tih tehnologija i s njima povezanih problema.

Cilj: Specijalistička edukacija ima za cilj da sa njenim završetkom tužioci steknu osnovno[[4]](#footnote-4) i napredno[[5]](#footnote-5) znanje o tome šta su kibernetički kriminal i elektronski dokazi, kako postupati u vezi s tim, koji materijalni i procesni zakoni se primjenjuju, koje tehnologije, te koliko hitne i efikasne mjere treba provesti, kao i u kojem obimu treba da bude međunarodna saradnja.

Ciljna grupa:

Predviđeno je da se ova specijalistička edukacija održi za grupu od 20 odabranih tužilaca iz tužilaštava u BiH koji se bave ovom ili sličnom vrstom predmeta ili koji imaju potencijal za stručno usavršavanje u oblasti kibernetičkog kriminala i prenošenje specijalističkog znanja koje steknu tokom edukacije na kolege u svojoj matičnoj instituciji.

Koncept: Cjelokupni program obuke će trajati 9 dana: tri trodnevna treninga (Modula) po podijeljenim oblastima. Edukacija je će obavljati preko entitetskih centara koji će ovo obuku vršiti zajedno.

Vremenski rok: Predviđeno je da se ove edukacije održe u 2016 i 2017. godini.

Očekivani rezultati:

Nakon ovee obuke tužioci bi trebalo da mogu:

- Povezati kriminalnu radnju sa odredbama domaćeg zakona

- Odobriti istražne radnje

- Ishoditi naredbu za pretres i oduzimanje kompjuterskih sistema i davanje elektronskih dokaza

- Ubrzati međunarodnu saradnju

- Ispitati svjedoke i vještake

- Iznijeti/ocijeniti elektronske dokaze.

**Pregled programa po modulima**

**Modul 1**

Naziv kursa: **Uvod u kibernetički kriminal**

Trajanje: 3 dana

**Oblast: Uvod u kibernetički kriminal**

*Tematski pregled sadržaja:*

- Opasnosti kibernetičkog kriminala

- Šta je kibernetički kriminal i njegove karakteristike

- Kako kompjuteri komuniciraju

- Informacije na internetu

-Razvoj i suzbijanje kibernetičkog kriminala u Evropi

- Izazovi za sudije i tužioce

- Funkcioniranje interneta (osnovni pojmovi)

- Rad informacijske i komunikacijske tehnologije i internet infrastrukture

- Protokoli i tehnologije

- Rječnik pojmova

**Oblast: Kibernetički kriminal i sigurnosni rizici**

- Trendovi u kibernetičkom kriminalu

- Tipologije: Posebni tipovi i tehničke kibernetičkog kriminala (npr. phishing, botnet i drugih malware, dječja pornografija)

- Kako kriminalci koriste informacije i komunikacijske tehnologije

- Prestupnici (profil, trendovi itd.)

- Uticaj kibernetičkog kriminala

- Kako povećati sigurnost informacijskih i komunikacijskih tehnologija

- Praktični primjeri i simulacije

- Korištenje (skrivenih) internet baza podataka

- Profili socijalnih mreža

- Korištenje društvenih (socijalnih) mreža kao sredstvo za ciljane napade;:

* ranjivosti društvenih mreža,
* korištenje ciljanih napada
* sposobnosti socijalnih mreža da odgovoriti na takve prijetnje.

- Načini komunikacije

- Načini anonimnosti

- Otkrivanje/identifikacija lokacije i identiteta kompjutera, kompanija i osoba na internetu

- Studije slučaja

**Modul 2**

**Naziv kursa: Kibernetički kriminal u domaćim zakonima i Međunarodna saradnja**

**Trajanje: 3** dana

**Oblast: Kibernetički kriminal u domaćim zakonima**

*Tematski pregled sadržaja:*

- Domaći pravni okvir za borbu protiv cyber kriminala

- Krivična djela usmjerena protiv kompjuterskih podataka i sistema

- Kompjuterska prevara i kompjutersko krivotvorenje

- Krivična djela u vezi sadržaja (dječja pornografija, ksenofobija, krivična djela motivisana mržnjom)

- Populacija osjetljiva na napade

- Krivična djela u vezi intelektualne svojine

- Sudske odluke/sudska praksa

**Oblast: Međunarodna saradnja**

- Konvencija o kibernetičkom/cyber kriminalu i dodatni protokoli

- Implementacija Konvencije o kibernetičkom/cyber kriminalu u pravni okvir Bosne i Hercegovine

- Konvencija o kibernetičkom kriminalu kao okvir za međunarodnu saradnju

- Opći principi

- Privremene mjere i uloga kontakt mjesta dostupnih 24/7

- Uzajamna pravna pomoć i uloga nadležnih organa

- Međunarodna saradnja u pretraživanju mreže

- Studije slučaja

**Modul 3**

Naziv kursa: **Procesni zakon/istražne radnje i elektronski dokazi**

Trajanje: 3 dana

**Oblast: Procesni zakon/istražne radnje**

*Tematski pregled sadržaja:*

- Stvarna i mjesna nadležnost

- Hitno očuvanje kompjuterskih podataka

- Izdavanje naredbi/naloga za dostavljanje podataka

- Pretres i oduzimanje kompjuterskih podataka

- Presretanje prometa i sadržaj podataka

- Zaštita podataka

- Istraga o IP-u i elektronskim dokazima – brojevi i kompjuterska imena

- Pozitivno „hakiranje“

- Preventivno pretraživanje interneta za otkrivanje organiziranog kriminala,

terorizma, teškog kriminala, pranja novca, itd.

- Pretraživanje interneta za pronalaženje osoba koje iskazuju nagli nekontrolirani

bijes (škole, itd.)

- Pretraživanje interneta radi otkrivanja dječje pornografije

**Oblast: Istraga i elektronski dokazi**

- O elektronskim dokazima: definicije i karakteristike

- Elektronski dokazi

- Tragovi/otisci na kompjuterima, internetu, digitalnoj komunikaciji

- Radnje pretraživanja, oduzimanja i očuvanja elektronskih dokaza

- Kompjuterska forenzika

- Karakteristike forenzičkog softwarea

- Identifikacija osumnjičenih

- Praćenje kriminalnog novca

- Zaštita i uslovi

- Upravljanje predmetima/priprema

- Iznošenje elektronskih dokaza na sudu

- Organizacija provođenja propisa u vezi sa kibernetičkim kriminalom i elektronskim dokazima

- Studije slučaja

**Oblast: Saradnja sa privatnim sektorom**

- Komunikacija sa dobavljačima internet usluga/privatnim sektorom

- Primjeri partnerstva javnog i privatnog sektora u Bosni i Hercegovini

-

- Provođenje zakona – saradnja sa dobavljačima internet usluga (ISP) u istrazi o kibernetičkom kriminalu: smjernice

- Rasprava: provođenje zakona – saradnja sa dobavljačima internet usluga (ISP): iskustva u BiH

- Studije slučaja

1. Nacrt obuke iz oblasti kibernetičkog kriminala djelomično je zasnovan na Konceptu obuke za sudije i tužioce Vijeća evrope uz dopune sa relevantnim i aktuelnim temama. [↑](#footnote-ref-1)
2. http://europa.eu/rapid/press-release\_IP-14-129\_hr.htm [↑](#footnote-ref-2)
3. *Cloud Service ili Cloud Computing* je koncept korištenja i funkcionisanja računara koji je zasnovan na internetu, gdje su dijeljeni resursi, softver i informacije i koji se dostupni na zahtjev. [↑](#footnote-ref-3)
4. „Osnovno znanje“ znači da treba da razumiju sljedeće:

- Kompjutere i mreže: kako funkcioniraju, osnovne pojmove rada interneta, ulogu dobavljača internet usluga, posebne izazove za sudije i tužioce

- Kibernetički kriminal: kako se informacijske i komunikacijske tehnologije koriste za izvršenje krivičnog djela

- Zakoni o kibernetičkom kriminalu: domaći zakoni (uključujući i sudsku praksu) i menunarodni standardi

- Stvarna i mjesna nadležnost

- Elektronski dokazi: tehnička procedura i zakonska pitanja. [↑](#footnote-ref-4)
5. Napredno znanje” znači da bi tužioci trebali imati praktično razumijevanje i biti sposobni da primjenjuju znanje iz osnovnih oblasti. [↑](#footnote-ref-5)