

Projekt o kibernetičkom kriminalu

www.coe.int/cybercrime

i

Lisabonska mreža

www.coe.int/lisbon-network



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Odjel za informatičko društvo i borbu protiv kriminala
Opća direkcija za ljudska prava i pravne poslove
Strasbourg, Francuska

8. oktobar 2008.

Bosnian version

Obuka za sudije i tužioce o kibernetičkom kriminalu: koncept

Projekt finansiran sredstvima Rumunije, Microsoft-a i McAfee-a, te Vijeća Evrope

Ovaj dokument je pripremila radna grupa sastavljena od različitih sponzora u okviru Projekta o kibernetičkom kriminalu i Lisabonske mreže institucija za edukaciju sudija i tužilaca Vijeća Evrope.

Kontakt:

Za dodatne informacije kontaktirati:

*Odjel za informatičko društvo i borbu protiv
kriminala
Opća direkcija za ljudska prava i pravne poslove
Vijeće Evrope
Strasbourg, Francuska
Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int*

Napomena:

Ovaj tehnički izvještaj ne sadrži nužno službene stavove Vijeća Evrope ili donatora koji finansiraju ovaj projekt ili stranaka potpisnica instrumenata koji se navode u ovom dokumentu.

Sadržaj

1	Izvršni rezime	4
2	Uvod	7
3	Institucije i sistemi obuke	9
4	Vještine i znanje koji se traže od sudija i tužilaca	12
4.1	Osnovno znanje	12
4.2	Napredno znanje	14
4.3	Specijalističko znanje	17
5	Sadašnja obuka o kibernetičkom kriminalu i elektronskim dokazima	18
5.1	Početna obuka	18
5.2	Obuka na radnom mjestu	19
6	Prijedlog pristupa	23
6.1	Cilj	23
6.2	Institucionaliziranje početne obuke	23
6.3	Institucionaliziranje obuke na radnom mjestu	23
6.4	Standardizirani i obnovljivi kursevi odnosno moduli	24
6.5	Pristup nastavnom materijalu ili materijalu za samostalno učenje	24
6.6	Pilot-centri za osnovnu i naprednu obuku	25
6.7	Povećanje znanja kroz međusobno povezivanje	25
6.8	Saradnja između javnog i privatnog sektora	26
7	Podrška realizaciji ovog koncepta	27
8	Dodatak	28
8.1	Lisabonska mreža: linkovi sa institucijama za obuku sudija i tužilaca	28
8.2	Primjeri osnovnog kursa obuke: struktura i teme koje se obrađuju	29
8.2.1	Primjer Holandije	29
8.2.2	Primjer Njemačke (Njemačka pravosudna akademija)	29
8.2.3	Primjeri Vijeća Evrope	30
8.3	Primjeri naprednog kursa obuke: struktura i teme koje se obrađuju	32
8.3.1	Primjer Holandije	32
8.3.2	Prijedlog Holandije za održavanje obuke s vodećim ekspertom	33

1 Izvršni rezime

Budući da se društva u cijelom svijetu oslanjaju na informacijske i komunikacijske tehnologije, sudije i tužioći moraju biti spremni da se bave kibernetičkim kriminalom i dokazima u elektronskoj formi. Dok su u mnogim zemljama organi za provođenje zakona uspjeli da se zadovoljavajuće osposobe za istragu u slučaju kibernetičkog kriminala i osiguravanje elektronskih dokaza, čini se da je to manje slučaj sa sudijama i tužiocima. Iz iskustva vidimo da u mnogim slučajevima sudije i tužioći imaju problema u suočavanju sa novim realnostima kibernetičkog svijeta. Zbog toga je potreban poseban napor da bi se sudije i tužioći osposobili za krivično gonjenje i suđenje u predmetima kibernetičkog kriminala i korištenje elektronskih dokaza putem edukacije, povezivanja i specijalizacije.

Ovaj koncept ima za cilj podržati takva nastojanja. Koncept su razvili Projekat Vijeća Evrope o kibernetičkom kriminalu i Lisabonska mreža institucija za obuku sudija i tužilaca u saradnji sa radnom grupom sastavljenom od više sponzora, u toku 2009. godine.

Svrha ovog koncepta je pomoći institucijama za obuku sudija i tužilaca da izrade programe o kibernetičkom kriminalu i elektronskim dokazima za sudije i tužioce i da ih uvrste u redovne početne programe i programe stručnog usavršavanja (tj. da ih institucionaliziraju). Na taj način će se dodatno olakšati povezivanje među sudijama i tužiocima u cilju povećavanja znanja, kao i dobijanja konzistentne – umjesto povremene – podrške za prijedloge obuke od strane zainteresiranih partnera.

Navedeni koncept se sastoji od sljedećih elemenata:

Ciljevi

Sadašnji početni programi i programi stručnog usavršavanja generalno ne pružaju sudijama i tužiocima onaj nivo znanja koji im je potreban za rješavanje kibernetičkog kriminala i rukovanje elektronskim dokazima.

Stoga bi koncept obuke za sudije i tužioce trebalo da ima sljedeće ciljeve:

- Omogućiti institucijama za obuku da provode početne programe i programe stručnog usavršavanja zasnovane na međunarodnim standardima.
- Opremiti najveći mogući broj budućih i sadašnjih sudija i tužilaca osnovnim znanjem o kibernetičkom kriminalu i elektronskim dokazima.
- Pružiti naprednu obuku jednom ključnom broju sudija i tužilaca.
- Podržati kontinuirano specijaliziranje i tehničku obuku sudija i tužilaca.
- Doprinijeti povećanju znanja putem povezivanja i saradnje među sudijama i tužiocima.
- Omogućiti pristup različitim programima i mrežama za obuku.

Sljedeće mjere mogu pomoći postizanju navedenih ciljeva:

1. Institucionaliziranje početne obuke

- U zemljama u kojima je početna obuka zapravo praktična obuka na radnom mjestu, preporučuje se da se barem jedan dio obuke posveti kibernetičkom kriminalu i elektronskim dokazima.
- U zemljama u kojima početnu obuku drže institucije za obuku sudija i tužilaca program obuke treba da obuhvati najmanje jedan modul osnovnog nivoa o kibernetičkom kriminalu i elektronskim dokazima. Ove teme treba, dodatno, uvrstiti u obavezne module koji obuhvataju materijalno i procesno pravo. Potrebno je ponuditi i opcionalne module za napredno znanje o kibernetičkom kriminalu i elektronskim dokazima.

- Posebne module obuke treba standardizirati u toj mjeri da budu obnovljivi i omogućće kandidatima da napreduju sa osnovnog ka naprednijim nivoima.

2. Institucionaliziranje stručnog usavršavanja

- Institucije koje pružaju stručno usavršavanje treba da imaju najmanje jedan osnovni modul o kibernetičkom kriminalu i elektronskim dokazima da bi oni koji su već na dužnosti sudije ili tužioca, a nisu to slušali u okviru početne obuke, prošli najmanje jedan osnovni modul o kibernetičkom kriminalu i elektronskim dokazima.
- Ove institucije bi trebalo još dodatno da nude kurseve naprednog nivoa.

3. Standardizirani i obnovljivi kursevi ili moduli

- Treba razviti standardizirane kurseve ili module koji se mogu ponavljati u širem obimu i racionalno u pogledu troškova, koji će omogućiti budućim i sadašnjim sudijama i tužiocima da napreduju sa osnovnog na napredne nivoe.
- Potrebno je izvršiti ocjenjivanje postojećih osnovnih kurseva koji se mogu uvrstiti u program početne obuke ili stručnog usavršavanja. Jedan standardni kurs se kasnije može preporučiti institucijama za početnu obuku i stručno usavršavanje.
- Slično ocjenjivanje treba izvršiti za kurseve naprednog nivoa, tako da se kasnije može preporučiti jedan standardni kurs naprednog nivoa.
- Predavači treba da budu obučeni za držanje takvih kurseva u tolikoj mjeri da ih mogu držati domaći predavači na svom jeziku, uz samo ograničenu potrebu za angažmanom međunarodnih predavača.

4. Pristup obuci i materijalu za samostalno učenje

- Nastavni materijal treba da bude pripremljen tako da odražava zajedničke međunarodne standarde i dobru praksu. Takava materijal treba da bude dostupan institucijama za obuku bez velikih troškova i s ciljem da se distribuira na lokalnom nivou.
- Iako sudije i tužiocima treba da dobiju obuku, prije svega, kako primjenjivati domaći zakon, bez obzira na to moguće je izraditi standardizirane materijale za obuku na takav način da se ostavi dovoljno mjesta za domaće sisteme i propise.
- Potrebno je izraditi i učiniti dostupnim kurseve koji se pohađaju putem interneta.

5. Pilot centri za osnovnu i naprednu obuku

- Potrebno je osnovati nekoliko pilot-centara za osnovnu i naprednu obuku sudija i tužilaca o kibernetičkom kriminalu i elektronskim dokazima gdje bi se mogli testirati i dalje razvijati standardizirane kurseve i materijale, širiti dobru praksu, provoditi istraživanja o podučavanju, voditi registar predavača, provoditi obuku predavača i držati obuku u drugim zemljama sa sličnim sistemima i jezikom.
- Pilot-centri treba da koordiniraju rad jedni s drugima uz podršku Vijeća Evrope.
- Sudije i tužiocima koji su spremni da postanu specijalisti treba da razmotre mogućnost da dobiju obuku putem učestvovanja u obuci putem centara izvrsnosti za agencije za provođenje zakona i kompanije iz ove oblasti.

6. Povećanje znanja putem međusobnog povezivanja

Iz tog razloga:

- Dok početna obuka i stručno usavršavanje daju sudijama i tužiocima jedan temelj, komunikacija sa kolegama, povezivanje sa drugim sudijama i tužiocima, ali i sa čitavim nizom drugih subjekata u ovoj oblasti od ključnog je značaja.
- Sudije i tužiocima treba da koriste postojeće mreže za sudije i tužioce (kao što je GPEN).

- Treba razgovarati o tome da Vijeće Evrope formira jednu međunarodnu mrežu za sudije koji sude u predmetima kibernetičkog kriminala odnosno „sudije za elektronski kriminal“ (slično kao GPEN za tužioce).
- Umrežavanje evropskih institucija koje nude obuku o kibernetičkom kriminalu i elektronskim dokazima treba da podrže Vijeće Evrope i Evropska mreža za obuku sudija i tužilaca.
- Da bi olakšali pristup sudijama i tužiocima ovim i mnogim mrežama vezanim za kibernetički kriminal, Vijeće Evrope treba da predoči inicijative i mreže i uspostavi portal sa linkovima, kratkim informacijama i kontakt-informacijama o različitim mrežama, čime će se omogućiti koordinacija među mrežama. Na taj način će se dodatno omogućiti pristup postojećim materijalima i inicijativama.

7. Saradnja javnog i privatnog sektora

- Korisna bi bila podrška privatnog sektora obuci sudija i tužilaca, imajući na umu da privatni sektor raspolaže potrebnim stručnim znanjem o ovoj temi. U isto vrijeme, sudije i tužioći moraju ostati nezavisni i nepristrasni.
- Institucije za obuku sudija i tužilaca mogu koristiti ekspertizu koja postoji u privatnom sektoru kada osmišljavaju programe obuke, izrađuju materijale za obuku i drže kurseve.
- Podrška privatnih organizacija institucijama za obuku ne smije se posmatrati tako kao da će se putem nje doći do nekih povoljnih sudskih odluka ili da će donijeti posao, nego kao način da sudije i tužioći dobiju adekvatne informacije koje im omogućavaju da donesu informirane odluke.
- Privatni sektor može na transparentan način dati podršku međunarodnim ili domaćim organizacijama, akademijama, inicijativama za obuku ili ostalim trećim stranama koje će zatim podržati nezavisne institucije za obuku.
- Iako je važno da sudije i tužioći imaju pregled o internetu i kibernetičkom kriminalu, isto tako je važno da im se daju informacije koje se odnose samo na konkretnu platformu. Kompanije koje se bave ovom djelatnošću mogu dati materijal za posebne module (umjesto čitavog kursa) o tome kako rade platforme od značaja za razumijevanje.

Lisabonska mreža Vijeća Evrope usvojila je ovaj koncept u septembru 2009. godine i preporučila da se distribuira i usvoji na što više institucija za obuku sudija i tužilaca. Mreža je takođe odlučila da ovaj koncept iznese pred Konsultativno vijeće Evropskih sudija i Konsultativno vijeće Evropskih tužilaca, kao i Evropsku komisiju za efikasnost pravosuđa (CEPEJ) kako bi ostvarila naširu moguću podršku ovom konceptu.

2 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.

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 sudije i tužiocima moraju biti spremni da se bave kibernetičkim kriminalom i elektronskim dokazima. Kako navodi Konsultativno vijeće Evropskih sudija¹, "neophodno je da sudije, nakon što su završili sve potrebne nivoe studija prava, dobiju opsežnu, raznovrsnu obuku kako bi mogli na zadovoljavajući način obavljati svoju funkciju" (stav 3.), a u obuci bi "trebalo da se uzme u obzir potreba za socijalnom svijesti i obimno razumijevanje različitih tema koje održavaju složenost života u društvu" (stav 27.). Značaj IKT-a u današnjem društvu je takav da sudije i tužiocima moraju posjedovati barem osnovno poznavanje tih tehnologija i s njima povezanih problema.

Dok su u mnogim zemljama organi za provođenje zakona uspjeli da se osposobe za istragu u oblasti kibernetičkog kriminala i da rade sa elektronskim dokazima, čini se da to nije bilo tako i sa sudijama i tužiocima koji, ipak, imaju ključnu ulogu u krivičnom procesu. Iz iskustva je jasno da u mnogim slučajevima sudije i tužiocima nailaze na teškoće u suočavanju sa novim realnostima kibernetičkog svijeta.

Zbog toga su potrebni posebni napor da se sudijama i tužiocima omogući da krivično gone i sude u predmetima kibernetičkog kriminala i da koriste elektronske dokaze, i to u vidu obuke, povezivanja i specijalizacije.

Stručno znanje i kapaciteti privatnog sektora u pogledu novih tehnologija ključni su za obuku organa za provođenje zakona. Oni će takođe biti korisni i za obuku sudija i tužilaca², ali ovaj potencijal do sada nije bio dovoljno iskorišten. A u isto vrijeme se mora očuvati nezavisnost i nepristrasnost sudija i tužilaca. Zbog toga su potrebni inovativni pristupi kojima će se osigurati nezavisnost sudija i tužilaca, a istovremeno da im se omogući pristup stručnom znanju privatnih kompanija i sticanje znanja o tome kako radi ta industrija i tehnologija. Koncept koji se ovdje predlaže pokazuje kako institucije za obuku sudija i tužilaca mogu imati koristi od podrške iz akademskih institucija i privrednih subjekata korištenjem standardiziranih programa obuke i drugih metoda.

Svrha koncepta koji se predstavlja u ovom radu je pomoći institucijama za obuku sudija i tužilaca da izrade programe za obuku o kibernetičkom kriminalu i elektronskim dokazima za sudije i tužioce i da tu obuku uvrste u redovne programe početne obuke i stručnog usavršavanja (tj. da je institucionaliziraju).

¹ Mišljenje br. 4 o odgovarajućoj početnoj obuci i stručnom usavršavanju za sudije na nivou država i evropskom nivou (CCJE (2003.) Op no 4)

² Vidjeti studiju objavljenu u martu 2009. god.: "[Co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel](#)" (Saradnja pravnih eksperata, privatnog sektora i akademske zajednice na provođenju dugoročne i održive obuke za ključno osoblje za kibernetički kriminal)

Ovaj koncept se zasniva na informacijama koje su dale institucije za obuku sucija i tužilaca u Belgiji, Hrvatskoj, Gruziji, Njemačkoj, Francuskoj, Holandiji, Poljskoj, Portugalu, Rumuniji, Španiji, „Bivšoj Jugoslovenskoj Republici Makedoniji“ i Velikoj Britaniji (odgovori na upitnik pristigli u junu 2009. godine), radionici održanoj u Portugalu u julu 2009. godine na kojoj su bili predstavnici iz Belgije, Irske, Portugala, Holandije i Velike Britanije, kao i privatnog sektora i radionici održanoj u Strasbourgu, 3. i 4. septembra 2009. god., uz učešće predstavnika institucija za obuku sudija i tužilaca navedenih zemalja, privatnog sektora, kao i Evropske mreže za obuku sudija i tužilaca i Lisabonske mreže Vijeća Evrope³.

Ovaj proces koji je uključio brojne i različite učesnike doveo je do izrade – po prvi put – koncepta za obuku sudija i tužilaca o pitanjima kibernetičkog kriminala i elektronskih dokaza. Participatorna priroda ovog procesa sigurno će doprinijeti boljoj saradnji različitih učesnika i objedinjavanju znanja i stručnosti u ostvarivanju ovog koncepta.

Lisabonska mreža Vijeća Evrope odobrila je ovaj koncept u septembru 2009. god. i preporučila da ga institucije za obuku sudija i tužilaca distribuiraju i provedu. Odlučeno je da se ovaj koncept dostavi Konsultativnom vijeću Evropskih sudija i Konsultativnom vijeću Evropskih tužilaca, kao i Evropskoj komisiji za efikasnost pravosuđa (CEPEJ) kako bi se osiguralo da koncept dobije što širu podršku.

³ Lisabonska mreža za razmjenu informacija između fizičkih i pravnih osoba zaduženih za obuku sudija

3 Institucije i sistemi obuke⁴

U Evropi – a slično je i u drugim regijama – sistemi obuke sudija i tužilaca se prilično razlikuju⁵.

Što se tiče početne obuke, sistem se obično sastoji od jednog od sljedećih ili njihove kombinacije⁶:

- Sistem A: Kandidati – nakon što završe pravni fakultet (univerzitetska diploma) i često nakon to su položili prijemni ispit – dobijaju posebnu obuku u centru za obuku sudija da bi mogli postati sudije i/ili tužioci. Ponekad se budući sudije i tužioći zajedno obučavaju, a ponekad u različitim institucijama.
- Sistem B: Kandidati – nakon što su završili pravni fakultet (univerzitetska diploma) – skupljaju praktično iskustvo kroz rad (ponekad u vidu formalnog pripravništva) u tužilaštvu, sudu, advokatskim uredima ili drugim institucijama – prije polaganja ispita koji će im omogućiti sticanje kvalifikacije za advokata, tužioca ili sudiju. U ovom slučaju nema centralizirane posebne institucije za njihovu obuku⁷.

Obuku na radnom mjestu, tj. stalno stručno usavršavanje sudija i tužilaca koji obavljaju tu dužnost, nude javne institucije za obuku sudija i tužilaca, koje su takođe zadužene za početnu obuku (npr. u Francuskoj, Gruziji, Holandiji, Poljskoj, Portugalu, Rumuniji, Španiji, „Bivšoj Jugoslovenskoj Republici Makedoniji“, Hrvatskoj) institucije za obuku koje su posebno osnovane za stručno usavršavanje (npr. u Njemačkoj) ili druge javne institucije, nevladine organizacije, međunarodne organizacije ili privatni sektor. U nekim slučajevima ovo je predviđeno godišnjim programima obuke ili se može organizirati na ad hoc osnovi. U većini slučajeva, stručno usavršavanje je opcionalno, osim ako sudije ili tužioći ne obavljaju svoju dužnost na posebnom sudu (npr. u Rumuniji).

Plan i program obuke za početnu obuku i usavršavanje u većini slučajeva zahtijeva formalni proces razmatranja i usvajanja, iako veća fleksibilnost postoji u slučajevima programa usavršavanja. Na primjer:

⁴ U ovom dokumentu pod izrazom "institucija za obuku" podrazumijeva se svaki subjekt koji je odgovoran za provođenje obuke.

⁵ Kako navodi Konsultativno vijeće sudija Vijeća Evrope 2003. godine: "Postoje velike razlike među evropskim zemljama u pogledu početne obuke i stručnog usavršavanja sudija. Ove razlike se djelimično mogu ticati posebnih karakteristika različitih sudskih sistema, ali u nekim segmentima nisu neizbježne niti neophodne. Neke zemlje pružaju dugotrajnu formalnu obuku u specijaliziranim institucijama, nakon čega slijedi intenzivni nastavak obuke. U drugima je predviđena neka vrsta pripravništva uz mentorstvo iskusnog sudije, koji pripravnicima prenosi znanje i daje stručne savjete na osnovu konkretnih primjera, pokazuje im kakav pristup da zauzmu, a pri tom izbjegava moraliziranje i pridikovanje. Zemlje običajnog prava uvelike se oslanjaju na dugogodišnje stručno iskustvo, uobičajeno u advokaturi. Između ovih mogućnosti, postoji cijeli niz zemalja u kojima je obuka u različitoj mjeri organizirana i obavezna."

Broj 4. Konsultativnog vijeća Evropskih sudija (CCJE) dostavljeno Ministarskom komitetu Vijeća Evrope o odgovarajućoj početnoj obuci i stručnom usavršavanju za sudije na nivou države i Evropske unije (CCJE (2003.) Op. N° 4; novembar 2003. god).

⁶ Vidjeti Prilog za više informacija.

⁷ Potrebno je spomenuti specifičnosti sistema običajnog prava. U Velikoj Britaniji, na primjer, sudije se imenuju iz redova iskusnih praktičara. Takođe postoji mogućnost za praktičare koji nisu stalni sudije da budu privremeni sudije u trajanju od najmanje jednog mjeseca svake godine, nakon čega velika većina bude imenovana za stalne sudije. Osim toga, mnogo je laika imenovanih da budu članovi tribunala (građansko) i sudova (uglavnom krivično pravo). Postoje posebni programi obuke koja se vrši prije svakog imenovanja i u toku obavljanja funkcije.

- U Francuskoj se plan i program utvrđuje nakon konsultacija na nivou pravosudnih institucija, pravnika i odjela Ministarstva pravosuđa. Program obuke se nakon toga dostavlja Upravnom odboru obrazovne institucije na usvajanje.
- U Njemačkoj je Programska konferencija Njemačke pravosudne akademije – koju sačinjavaju predstavnici različitih administracija pravosudnog sistema, kao i stručna udruženja sudija i tužilaca – odgovorna za izradu plana i programa stručnog usavršavanja na ovoj akademiji.
- U Poljskoj do 30. aprila svake godine odjeli Ministarstva pravde, predsjednici sudova i tužilaštva dostavljaju prijedloge. Na osnovu tih prijedloga Direktor državne škole predstavlja Programskom odboru plan nastavnih aktivnosti za sljedeću godinu na odobrenje do 30. jula. Nakon odobrenja Ministarstva pravde, nastavni plan se šalje odgovornim odjeljenjima Ministarstva pravde, predsjednicima drugostepenih sudova i apelacionim tužilaštvima.
- U Rumuniji strategiju za početnu obuku i stručno usavršavanje usvaja Naučno vijeće Državnog instituta sudija i Više vijeće sudija.
- U Španiji planove i nastavne programe priprema pedagoška komisija koja se sastoji od stručnjaka za pravna pitanja u konsultaciji sa udruženjima sudija ili pojedinačno sudijama. Programe početne obuke i stručnog usavršavanja sudija na kraju odobrava Generalno vijeće za pravosuđe.
- U Portugau program obuke svake godine razmatra i priprema Centar za pravosudne sudije. Sadržaj programa početne obuke je utvrđen zakonom, dok se program stručnog usavršavanja mijenja svake godine u skladu sa potrebama utvrđenim u praksi. Program obuke se utvrđuje nakon konsultacija sa višim pravosudnim vijećima, poreznim i upravnim sudovima i tužilaštvom.
- U Belgiji opće i posebne formacijske programe izrađuje i nadzire „Institut de formation judiciaire“ svake godine. Ovaj institut je osnovan nedavno zakonom (31. 02. 2007. god.), a radi od početka 2009. godine. Kibernetički kriminal je uključen u (često opcionalno) stručno usavršavanje.
- U Holandiji Vijeće sudija i Vijeće glavnih tužilaca (koji zajedno formiraju instruktivnu organizaciju za instituciju za obuku SSR) odučuje da li postoje sredstva za predloženi program obuke. Prijedloge mogu davati, na primjer, tužioc i sudije ili predavači na SSR-u, i ako postoje raspoloživa sredstva, obuku će pripremiti odgovarajući stručnjaci sa SSR-a, iz tužilaštva, sudije ili ako je potrebno, treće strane, uključujući i privatni sektor.
- U Hrvatskoj se programi za početnu obuku i planovi za stručno usavršavanje utvrđuju u saradnji sa Savjetodavnim vijećem i Programskim vijećem Pravosudne akademije. Programsko vijeće utvrđuje prioritete obuke i dostavlja prijedlog nacrtu godišnjeg programa stručnog usavršavanja. Savjetodavno vijeće donosi ovaj akt i daje smjernice za utvrđivanje strategije stručnog usavršavanja. Članovi oba vijeća su ugledni pravni eksperti i predstavnici svih ciljnih grupa Pravosudne akademije.

Institucije za obuku mogu angažirati vanjske eksperte, naročito ako su predmeti specifični i tehničke prirode kao što je slučaj sa kibernetičkim kriminalom i elektronskim dokazima. Na primjer:

- U Njemačkoj državna pravosudna akademija stalno angažira vanjske predavače, koji su uglavnom pravni stručnjaci ili istraživači, ali ponekad su to i eksperti angažirani u privatnim i javnim kompanijama iz ove djelatnosti.
- U Holandiji, konsultanti i eksperti iz kompanija su uključeni u izradu kurseva obuke, a i drže obuku.
- U Rumuniji se Državni institut magistrata oslanja na vanjske trenere i predavače u specijaliziranim oblastima kao što su kibernetički kriminal (npr. Vijeće Evrope, Ministarstvo pravosuđa SAD-a, FBI, Tajnu službu SAD-a, kao i privatni sektor, kao što su eBay, VISA, American Express, Amazon, PayPal, Microsoft), a naročito u slučaju obuke trenera.
- U Španiji je Generalno vijeće za pravosuđe potpisalo sporazum sa kompanijama iz privatnog sektora (CYBEX, Logality) za održavanje obuke o kibernetičkom kriminalu i kibernetičkoj forenzici. Osim toga, eksperti iz privatnog sektora učestvuju u obuci sudija i tužilaca.

- U Portugalu su predavači na Centru za pravosudne studije uglavnom sudije i tužioći. Za stručno usavršavanje (npr. seminare ili kratke kurseve) mogu se angažirati treneri iz privatnog sektora i drugi eksperti.
- U Hrvatskoj su specijalisti iz policijski jedinica koji se bave suzbijanjem organiziranog i privrednog kriminala uključeni u izradu i provođenje obuke.
- U Belgiji se najveći postotak budžetskih sredstava predviđenih za obuku sudija i tužilaca izdvaja za obuku koju organiziraju univerziteti. Moguće je, međutim, angažirati i eksperte iz privatnog sektora za neke programe obuke.

Implikacije vezane za obuku sudija i tužilaca o kibernetičkom kriminalu odnosno elektronskim dokazima su sljedeće:

- Sudije i tužioći, u pravilu, počinju svoju edukaciju na studiju prava na univerzitetu. Može se pretpostaviti da, što se više problematika kibernetičkog kriminala i elektronskih dokaza bude uređivala zakonom, to će se ova oblast više uključivati u udžbenike i nastavne programe pravnog fakulteta. Međutim, može biti korisno dati određene prijedloge u tom pogledu onima koji su odgovorni za pripremu materijala za nastavu na univerzitetu.
- U zemljama u kojima početnu obuku vrše institucije za edukaciju sudija i tužilaca trebalo bi da je moguće u nastavni program uvrstiti i obuku o kibernetičkom kriminalu odnosno elektronskim dokazima.
- Tamo gdje se početna obuka odvija na radnom mjestu to je manje moguće.
- U većini zemalja postoje institucije za obuku sudija i tužilaca na radnom mjestu i trebalo bi da je moguće uvrstiti kibernetički kriminal odnosno elektronske dokaze u program te obuke.
- Iako je moguće organizirati *ad hoc* obuku na radnom mjestu (usavršavanje), potrebno je proći formalnu proceduru i dobiti odobrenje za uvrštavanje kibernetičkog kriminala odnosno elektronskih dokaza u formalni program i na taj način takvu obuku institucionalizirati.
- Obuka na radnom mjestu (usavršavanje) je obično fakultativna. Biće izazov uvjeriti sudije i tužioce da prođu takvu obuku iz jedne takve tehničke oblasti kao što je kibernetički kriminal odnosno elektronski dokazi⁸.
- Ekspertiza iz javnog i privatnog sektora je potrebna i može se angažirati za izradu kurseva obuke, obuku trenera i održavanje kurseva.

⁸ U Portugalu je stručno usavršavanje je obavezno (npr. svaki sudija i tužilac mora pohađati najmanje dva seminara godišnje), a u Rumuniji može biti obavezno u nekim slučajevima.

4 Vještine i znanje koji se traže od sudija i tužilaca

Očigledno je da će sve veći broj krivičnih predmeta, ali i mnogi predmeti iz građanskog ili upravnog prava koji dođu na sud biti na ovaj ili onaj način vezani za informacije i komunikacijske tehnologije, i da će se većina sudija u krivičnim predmetima i tužilaca suočiti sa, ako ne kibernetičkim kriminalom, onda sa stvarima koje se tiču elektronskih dokaza. Zbog toga nije dovoljno samo obučavati specijalizirane sudije i tužioce.

Znanje o kibernetičkom kriminalu i elektronskim dokazima je potrebno proširiti na što veći krug: svi ili što je više moguće sudija i tužilaca, zato, treba da stekne barem osnovna znanja o pitanjima vezanim za kibernetički kriminal i elektronske dokaze. To osnovno znanje treba pružiti kroz početnu obuku za buduće sudije i tužioce, a i u vidu stručnog usavršavanja za sudije i tužioce koji već obavljaju tu dužnost.

U isto vrijeme, ovdje se radi o veoma tehničkim pitanjima koja se konstantno razvijaju i ne može se očekivati da sudije i tužioc generalno mogu pratiti tehnološka dostignuća u svakom trenutku. Stoga je neophodno da se naprednije znanje prenese na jedan dovoljan broj sudija i tužilaca koji će postati specijalisti za kibernetički kriminal i elektronske dokaze.

4.1 Osnovno znanje

U većini pravosudnih sistema ne može se predvidjeti koji će sudija dobiti koji predmet (princip „prirodnog sudije“), tako da, na kraju, svi sudije, istražni sudije i tužioc treba da imaju osnovno znanje o pitanjima vezanim za kibernetički kriminal i elektronske dokaze. „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 međunarodni standardi
- Stvarna i mjesna nadležnost
- Elektronski dokazi: tehnička procedura i zakonska pitanja.

Nakon ove osnovne obuke, sudije i tužioc bi trebalo da mogu:

- Povezati kriminalnu radnju sa odredbama domaćeg zakona
- Odobriti istražne radnje
- Narediti pretres i oduzimanje kompjuterskih sistema i davanje elektronskih dokaza
- Ubrzati međunarodnu saradnju
- Ispitati svjedoke i vještake
- Iznijeti/ocijeniti elektronske dokaze.

U nastavku dajemo jedan primjer tipičnog osnovnog kursa obuke za sudije i tužioce.

Primjer: Obuka o kibernetičkom kriminalu i elektronskim dokazima – uobičajeni modul za sticanje osnovnog znanja

Cilj kursa	Do kraja ovog kursa sudije i tužioci treba da steknu osnovno znanje o tome šta su kibernetički kriminal i elektronski dokazi, kako postupati u vezi s tim, koji materijalni i procesni zakoni se primjenjuju, kao i koje tehnologije, te koliko hitne i efikasne mjere treba provesti, kao i u kojeg obima treba da bude međunarodna saradnja
Sesija 1	O kibernetičkom kriminalu
	<ul style="list-style-type: none"> ➤ Zašto se brinuti zbog kibernetičkog kriminala? ➤ Šta je kibernetički kriminal? ➤ Izazovi za sudije i tužioce ➤ Domaći zakoni i međunarodni standardi
Sesija 2	Tehnologija
	<ul style="list-style-type: none"> ➤ Funkcioniranje interneta (osnovni pojmovi) ➤ Rječnik pojmova ➤ Protokoli
Sesija 3	Kibernetički kriminal kao krivičnog djelo u domaćim zakonima
	<ul style="list-style-type: none"> ➤ Krivična djela usmjerena protiv kompjuterskih podataka i sistema ➤ Kompjuterska prevara i kompjutersko krivotvorenje ➤ Krivična djela u vezi sadržaja (dječja pornografija, ksenofobija, rasizam) ➤ Krivična djela u vezi intelektualne svojine ➤ Sudske odluke/sudska praksa
Sesija 4	Elektronski dokazi
	<ul style="list-style-type: none"> ➤ O elektronskim dokazima: definicije i karakteristike ➤ Zahtjevi za elektronskim dokazima ➤ Kompjuterska forenzika
Sesija 5	Procesni zakon/istražne radnje
	<ul style="list-style-type: none"> ➤ Stvarna i mjesna nadležnost ➤ Hitno očuvanje kompjuterskih podataka ➤ Izdavanje naredbi/naloga ➤ Pretres i oduzimanje kompjuterskih podataka ➤ Presretanje prometa i sadržaj podataka ➤ Zaštita
Sesija 6	Interakcija sa privatnim sektorom
Sesija 7	Međunarodna saradnja
	<ul style="list-style-type: none"> ➤ Konvencija o kibernetičkom kriminalu kao okvir međunarodne saradnje ➤ Opći principi ➤ Privremene mjere i uloga kontakt mjesta dostupnih 24/7 ➤ Uzajamna pravna pomoć i uloga nadležnih organa
Sesija 8	Ocjenjivanje i zaključivanje
Logistika i materijali	<p>Ova obuka se može provoditi putem interneta ili u učionici. Ako se provodi u učionici:</p> <ul style="list-style-type: none"> ➤ Dovoljna je učionica koja ima kompjuter i projektor za prezentacije (s obzirom da ovaj kurs ne sadrži praktične vježbe, kao što su demonstracija forenzičkog softvera ili istražnih radnji, nije potrebna kompjuterska laboratorija) ➤ Odgovarajući dijelovi domaćih materijalnih i procesnih zakona ➤ Budimpeštanska konvencija o kibernetičkom kriminalu, zajedno sa izvještajem s obrazloženjima ➤ Čitanka sa rječnikom pojmova i druge uvodne informacije ➤ Ako se predavanja drže na stranom jeziku, potrebno je predvidjeti prevodioca, a materijali treba da budu prevedeni.

4.2 Napredno znanje

Ponekad osnovno znanje nije dovoljno da se riješi sudski predmet kibernetičkog kriminala. Za takvu situaciju će biti potrebno da znatan broj sudija, istražnih sudija i tužilaca ima naprednije znanje da bi mogli provesti istragu, krivično goniti, odnosno suditi složene slučajeve koji se tiču kibernetičkog kriminala i elektronskih dokaza, ili dati pomoć drugim tužiocima i sudijama.

U nekim zemljama formirani su specijalizirani odjeli u tužilaštvu (npr. Rumunija, Srbija), u drugim, opet, velika tužilaštva raspolažu sa više specijaliziranih tužilaca. U Holandiji je u toku program "intensiveringsprogramma" kako bi se postiglo, između ostalog, da u svakom od jedanest velikih tužilačkih ureda ima najmanje po jedan specijalizirani tužilac. U Italiji, prema novom zakonu o kibernetičkom kriminalu, 29 tužilaštava je sada nadležno za kibernetički kriminal. U Portugalu Lisabonsko okružno tužilaštvo ima specijalni odjel o kompjuterskom kriminalu, kojem se dodjeljuju ove istrage.

U nekim zemljama određeni tužioci mogu nadgledati rad jedinica za visokotehnološki kriminal u okviru policije. U većini zemalja tužilaštva su tako hijerarhijski organizirana da viši tužilac može dodijeliti slučaj specijaliziranom tužiocu. Stoga je moguće odrediti tužioce koji će dobiti napredni stepen ovog znanja.

Što se tiče sudija, u nekim zemljama je moguće da se predmeti kibernetičkog kriminala dodijele specijaliziranom sudiji u sudu koji se bavi određenim vrstama kriminaliteta, kao što je organizirani kriminal. Takav primjer (vjerovatno jedini u Evropi) je Srbija, gdje se posebno odjeljenje okružnog suda u Beogradu bavi predmetima kibernetičkog kriminala. Međutim, s obzirom da je u većini pravosudnih sistema prisutan princip „prirodnog“ sudije, neophodan je drugačiji pristup. U Holandiji je, možda jedinstveno u svijetu) osnovano pet centara sa specijaliziranim sudijama koji služe kao resurs drugim sudijama. U Španiji se razmatra sličan prijedlog na nivou Općeg vijeća za pravosuđe, prema kojem bi grupa sudija specijaliziranih za kibernetički kriminal i elektronske podatke pomogla i savjetovala druge sudije. U Belgiji se zakonom ne zahtijeva specijalizacija, ali većina sudova ima mogućnost da traži da se jedan ili više njihovih članova specijaliziraju. Činjenica da se ti predmeti dodjeljuju ovim specijaliziranim sudijama, međutim, samo je pitanje unutrašnje organizacije suda. Ponekad je nadležnost za odlučivanje u nekim predmetima zakonom data određenim sudovima u zemlji (Brisel). Pa ipak, u većini slučajeva nadležnost se određuje prema mjestu izvršenja krivičnog djela, a tamo nema uvijek specijaliziranog sudije ili tužioca. U mnogim zemljama ima sudova koji možda češće od drugih imaju slučajeve kibernetičkog kriminala, zbog čega treba da imaju viši stepen specijalizacije od drugih.

"Napredno znanje" znači da bi sudije i tužioci trebali imati praktično razumijevanje i biti sposobni da primjenjuju znanje o sljedećem:

- Kompjuterima i mrežama:
 - Rječnik termina vezanih za kompjutere i kibernetički kriminal
 - Rad interneta
 - Protokole i tehnologiju
 - Ulogu dobavljača internet usluga
- Kibernetičkom kriminalu:
 - Trendovi u kibernetičkom kriminalu
 - Tipologije: posebne tipove i tehnike kibernetičkog kriminala (npr. *phishing*, *botnet* i drugi *malware*, dječja pornografija)
 - Praktični primjeri i simulacije
- Kibernetičkim zakonima i drugim propisima:
 - Domaći zakoni i sudska praksa
 - Međunarodna saradnja: međunarodni i bilateralni sporazumi, putevi pravosudne saradnje i praktične metode hitne saradnje

- Istraži i elektronskim dokazima:
 - Stvarna i mjesna nadležnost
 - Odredbe procesnog prava i njihova praktična primjena
 - Radnje pretraživanja, oduzimanja i očuvanja elektronskih dokaza
 - Karakteristike forenzičkog softvera
 - Identifikacija osumnjičenih
 - Praćenje kriminalnog novca
 - Zaštita i uslovi
 - Iznošenje elektronskih dokaza na sudu.

Primjer: Obuka o kibernetičkom kriminalu i elektronskim dokazima – tipičan modul naprednog znanja⁹

Cilj kursa	Do kraja kursa sudije i tužioce treba da steknu napredni stepen znanja koje se moe primijeniti u praksi o radu kompjutera i mreža, o tome šta je kibernetički kriminal, o zakonima i drugim propisima o kibernetičkom kriminalu, nadležnosti, istražnim radnjama i elektronskim dokazima, i međunarodnoj saradnji
Sesija 1	<p>Kompjuteri i mreže</p> <ul style="list-style-type: none"> ➤ Rječnik termina u vezi kompjutera i kibernetičkog kriminala ➤ Rad informacijske i komunikacijske tehnologije i internet infrastrukture <ul style="list-style-type: none"> - Protokoli i tehnologije - Kako kompjuteri komuniciraju - Istraga o IP-u i elektronskim dokazima – brojevi i kompjuterska imena - Uloga dobavljača internet usluga ➤ Informacije na internetu <ul style="list-style-type: none"> - Prikupljanje informacija - Korištenje (skrivenih) internet baza podataka ➤ Profili socijalnih grupa <ul style="list-style-type: none"> - Načini komunikacije - Načini anonimnosti ➤ Otkrivanje/identifikacija lokacije i identiteta kompjutera, kompanija i osoba na internetu
Sesija 2	<p>Kibernetički kriminal i sigurnosni rizici</p> <ul style="list-style-type: none"> ➤ 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 ➤ Uticaj kibernetičkog kriminala ➤ Kako povećati sigurnost informacijskih i komunikacijskih tehnologija ➤ Praktični primjeri i simulacije
Sesija 3	<p>Zakoni o kibernetičkom kriminalu: materijalno krivično pravo</p> <ul style="list-style-type: none"> ➤ Krivična djela protiv kompjuterskih podataka i sistema ➤ Kompjuterska prevara i krivotvorenje ➤ Krivična djela u vezi sadržaja (dječja pornografija, krivična djela počinjena iz mržnje) ➤ Krivična djela vezana za intelektualnu svojinu ➤ Sudske odluke/sudska praksa

⁹ Based on replies to the questionnaire and the example provided by the Netherlands.

Sesija 4	Istraga i elektronski dokazi
	<ul style="list-style-type: none"> ➤ Elektronski dokazi <ul style="list-style-type: none"> - Tragovi/otisci na kompjuterima, internetu, digitalnoj komunikaciji - Radnje pretraživanja, oduzimanja i očuvanja elektronskih dokaza - Karakteristike forenzičkog softwarea - Identifikacija osumnjičenih - Praćenje kriminalnog novca - Zaštita i uslovi - Upravljanje predmetima/priprema - Iznošenje elektronskih dokaza na sudu ➤ Organizacija provođenja zakona u vezi sa kibernetičkim kriminalom i elektronskim dokazima ➤ Studije slučaja
Sesija 5	Zakoni i drugi propisi o kibernetičkom kriminalu: procesno pravo
	<ul style="list-style-type: none"> ➤ Hitno očuvanje kompjuterskih podataka ➤ Naredba za dostavljanje podataka ➤ Pretraživanje i oduzimanje kompjuterskih podataka ➤ Presretanje prometa i sadržaja podataka ➤ Zaštita ➤ Komunikacija sa dobavljačima internet usluga/privatnim sektorom ➤ Studije slučaja
Sesija 6	Stvarna i mjesna nadležnost
	<ul style="list-style-type: none"> ➤ Opća načela ➤ Nadležnost za kibernetički kriminal - izazovi ➤ Odredbe o nadležnosti u Konvenciji o kibernetičkom kriminalu ➤ Studije slučaja
Sesija 7	Međunarodna saradnja
	<ul style="list-style-type: none"> ➤ Konvencija o kibernetičkom kriminalu kao okvir za međunarodnu saradnju ➤ Opća načela ➤ Privremene mjere, uloga kontaktnih tačaka dostupnih 24/7 i policijska saradnja ➤ Uzajamna pravna pomoć i uloga nadležnih organa ➤ Studije slučaja
Sesija 8	Evaluacija i zaključci
Logistika i materijali	<p>Ova obuka se može provoditi putem interneta ili u učionici. Ako se provodi u učionici:</p> <ul style="list-style-type: none"> ➤ Potrebna je učionica koja ima kompjuter i projektor za prezentacije ➤ Bilo bi korisno da polaznici imaju kompjuter s pristupom internetu (ali ovo nije uslov) ➤ Odgovarajući dijelovi domaćih materijalnih i procesnih zakona ➤ Budimpeštanska konvencija o kibernetičkom kriminalu, zajedno sa izvještajem s obrazloženjima ➤ Čitanka sa rječnikom pojmova i druge uvodne informacije ➤ Ako se predavanja drže na stranom jeziku, potrebno je predvidjeti prevodioca, a materijali treba da budu prevedeni.

Sudijam i tužiocima obično nije potrebna ta vrsta tehničkih vještina i znanja koja je potrebna za istražitelje visokotehnoloških krivičnih djela ili forenzičare. Pa ipak, mislimo da je korisno da se prisjetimo se napora koji su uloženi da bi se došlo do jednog sistematskog programa obuke za službenike agencija za provođenje zakona.

Projekt koji je vodila Garda Síochána iz Irske, finansiran sredstvima Evropske komisije (Program Falcone 2002.), i uz učešće eksperata iz deset zemalja članica EU, razvio je jedan standardizirani osnovni („Prvi nivo“) program obuke o kibernetičkom kriminalu za službenike agencija za

provođenje zakona. Od 2004. godine organizira se dvotjedni tečaj koji je već proveden u mnogim evropskim i izvanevropskim zemljama. Tečaj je dobio akreditaciju Univerzitetskog koledža u Dublinu 2006. godine ([University College Dublin](#)).

U okviru kasnijih projekata koje je vodila Garda iz Irske u partnerstvu sa UCD-om, pripremljeni su dodatni moduli srednjeg i naprednog stepena, u općem nastojanju da se pripremi jedan potpuno akreditirani magistarski program kompjuterske forenzike i istrage o kibernetičkom kriminalu za službenike agencija za provođenje zakona na globalnom nivou. Postojeći moduli srednjeg stepena za polaznike iz agencija za provođenje zakona obuhvataju:

- Istrage na internetu
- Istrage o mrežama
- Forenziku NTFS sistema
- Forenziku Linus
- Forenziku mobilne telefonije
- Bežične LANS i VOIP
- Napredno ispisivanje skupa podataka
- Forenziku živih podataka
- Forenziku Microsoft Vista-e.

Ovi moduli se stalno ažuriraju, a u pripremi su i dodatni moduli.¹⁰

Europol je u julu 2007. godine osnovao Grupu za usklađivanje obuke o kibernetičkoj krivičnoj istrazi čiji je primarni cilj uskladiti ove aktivnosti unutar Evropske unije a vezano za obuku o visokotehnoškom kriminalu, kako bi se utvrdio jedan certificirani kurikulum za istražitelje iz agencija za provođenje zakona i proširio i na zemlje izvan EU kao pomoć drugim agencijama za provođenje zakona koje žele da to isto urade. Partneri u ovoj aktivnosti su Evropska komisija, OLAF, Eurojust, CEPOL, Interpol, Vijeće Evrope, Ujedinjeni narodi, Centar za kibernetičke krivične istrage Univerzitetskog koledža u Dublinu, Univerzitet u Troju, Christchurch univerzitet iz Kenterberija, Univerzitet u Bolonji, kao i brojne kompanije.

4.3 Specijalističko znanje

Neki sudije i tužioći mogu steći specijalističko znanje na postdiplomskim studijima, samostalnim učenjem, učeći od kolega ili stičući iskustvo u struci. To znanje neće biti dio redovnih programa obuke. Sudije i tužioći koji imaju takvo specijalističko znanje predstavljaju dragocjen resurs za druge, a i kao predavači.

¹⁰ Ostali primjeri uključuju programe za visokotehnoški kriminal Agencije za unapređenje policijskih aktivnosti Velike Britanije ([UK National Policing Improvement Agency](#)).

5 Sadašnja obuka o kibernetičkom kriminalu i elektronskim dokazima

5.1 Početna obuka

“Početna obuka” podrazumijeva obuku koju dobiju kandidati, nakon što su završili studije prava na univerzitetu, kako bi postali sudije i/ili tužioc. U mnogim sistemima početnu obuku provodi institucija za obuku sudija i tužilaca u trajnju od jedne do tri godine. U nekim drugim početna se obuka sastoji od više ili manje formalizirane praktične obuke na radnom mjestu, bez posebnog nastavnog programa.

U većini zemalja kibernetički kriminal i elektronski dokazi ili nisu predviđeni kao dio početne obuke ili jesu u manjoj mjeri. Na primjer:

- U Francuskoj obuka iz oblasti procesnog prava na Ecole Nationale de la Magistrature (ENM) obuhvata trosatno predavanje specijaliste za informacijske tehnologije o pretraživanju u cilju pronalaska elektronskih dokaza i o tehnologiji; pitanja kibernetičkog kriminala se ne obrađuju.
- U Gruziji kibernetički kriminal nije predviđen u početnoj obuci za tužioce, ali je prisutan u obuci za sudije i sudsko osoblje kao poludnevni kurs u formi predavanja.
- U Njemačkoj kibernetički kriminal nije obavezan u praktičnoj obuci na radnom mjestu.
- U Hrvatskoj, Poljskoj i Rumuniji ove teme nisu uključene u početnu obuku.

Međutim, u nekim zemljama kibernetički kriminal i elektronski dokazi su uobičajeni u početnoj obuci. Na primjer:

- U Holandiji početna obuka sadrži osnovni jednodnevni kurs o kibernetičkom kriminalu koji predaje Institut za edukaciju tužilaca i sudija (SSR) u Utrehtu ili Zutphenu i uključuju i čitanku i drugi potreban materijal. Kurs sadrži interaktivne seminare i studije slučaja. Osim ovog osnovnog jednodnevnog kursa i dubinske četverodnevne obuke, nudi se i dvodnevni kurs koji drže eminentni stručnjaci.
- Španska pravosudna škola nudi početnu obuku o kibernetičkom kriminalu i elektronskim dokazima novoimenovanim sudijama, i kao obuka o materijalnom i procesnom pravu. To je dio obavezne obuke o procesnom pravu i uzimanju dokaza. Kibernetički kriminal i elektronski dokazi podučavaju se na seminarima u trajanju od četiri popodneva i uključuju domaće pravo, međunarodne instrumente saradnje, demonstraciju forenzičkog softvera i istražne radnje, oduzimanje elektronskih dokaza i studije slučaja. Osim toga, jednom godišnje organizira se posebni seminar o elektronskim dokazima i još jedan o materijalnom pravu (krivična djela počinjena upotrebom elektronskih sredstava). Ove seminare drže kako pravni stručnjaci i stručnjaci za IT. Uz to, sudije imaju pristup virtualnoj biblioteci o elektronskom kriminalu. Cilj ove početne obuke je da se pruži osnovno znanje.
- U „Bivšoj Jugoslovenskoj Republici Makedoniji“ Akademija za obuku sudija i tužilaca provodi početnu obuku o kibernetičkom kriminalu i elektronskim dokazima kao dio obuke o krivičnom pravu, informacijskim tehnologijama i pretraživanju. Za kibernetički kriminal i elektronske dokaze predviđeno je deset sati.
- U Portugalu kibernetički kriminal nije posebno izdvojen dio nastavnog programa. Međutim, u o oblasti krivičnih istraga postoji posebni seminar (jedan i po sat vremena obuke) o kibernetičkom kriminalu i digitalnim dokazima. Za vrijeme obuke o krivičnom zakonu i krivičnom postupku devet sati je posvećeno kompjuterkim krivičnim djelima i procesnim mjerama za prikupljanje digitalnih dokaza i devet sati za informacijske i komunikacijske tehnologije.

Kurseve drže stalni predavači, sudije, tužiocima ili pravnicima koji imaju iskustvo u toj oblasti, specijalizirani policajci, IT eksperti ili specijalisti iz kompanija iz privatnog sektora.

Iz raspoloživih informacija može se zaključiti sljedeće:

- S obzirom je cilj pružiti svim sudijama i tužiocima osnovni nivo znanja o kibernetičkom kriminalu i elektronskim dokazima, obuka koja se nudi je isuviše ograničena.
- Početna obuka, uz vrlo malo izuzetaka, obuhvata samo osnovni nivo, a nije predviđena dalja obuka.
- Obično nije dostupan standardizirani materijal za obuku koja se ponavlja.

5.2 Obuka na radnom mjestu

Obuku na radnom mjestu, to jest, dalje stručno usavršavanje sudija i tužilaca koji obavljaju tu dužnost nude javne institucije za obuku, ali to mogu biti i brojne druge organizacije. Na primjer:

- U Francuskoj se na Ecole Nationale de la Magistrature održava petodnevni napredni seminar u školskim prostorijama, a pored njega nudi se i dvodnevno pripravništvo u uredu za visokotehnološki kriminal Ministarstva unutrašnjih poslova (OLCTIC). Troškove (približno 5.000 eura po kursu) pokriva škola. Predavači su sudije, tužiocima, policajci, stručnjaci za IT ili odabrani eksperti iz kompanija.
- U Gruziji je Visoka pravosudna škola jedina institucija zadužena za stručno usavršavanje sudija. U njoj se održava osnovni dvodnevni kurs o kibernetičkom kriminalu, financiran iz državnog budžeta. Predavači su fakultetsko osoblje i sudije Vrhovnog i apelacionih sudova. Tužioce obučava jedinica za obuku u okviru Ministarstva pravde, ali do sada nisu organizirani kursevi na temu kibernetičkog kriminala i elektronskih dokaza.
- U Njemačkoj stručno usavršavanje sudija i tužilaca provodi Njemačka pravna akademija koja organizira nekih 150 edukativnih događaja godišnje. 2009. godine dva od njih su bila usmjerena na kibernetički kriminal i trajala su svaki po četiri dana. Predavači su obično tužiocima i sudije koji imaju iskustvo u pitanjima kibernetičkog kriminala, ali mogu biti i pripadnici policije, carine, poreznih organa ili drugi. Troškove dijele federalna i pokrajinske vlade. Ovi kursevi pružaju osnovni i napredni nivo znanja.
- U Holandiji, iako je stručno usavršavanje fakultativno, svaki sudija ima obavezu provesti određeni broj nastavnih sati godišnje. Svaki sudija može izabrati koji kurs ili kurseve će pohađati. Institut za edukaciju sudija i tužilaca, ali i nekoliko drugih institucija i postdiplomskih nastavnih kapaciteta nude stručno usavršavanje iz kibernetičkog kriminala i elektronskih dokaza koje obuhvata osnovni i napredni nivo. Ova institucija svake godine organizira tri osnovna i tri detaljnija kursa i jedan kurs koji vode eminentni stručnjaci. Predavači su specijalisti iz oblasti kompjuterskog kriminala iz domaćih tužilaštava, kao i eksperti iz privatnih kompanija i drugih organizacija koje se time bave. Međutim, Institut za edukaciju sudija i tužilaca nudi čitav niz drugih kurseva i obuhvata pravne i praktične aspekte (ukupno oko 400 kurseva). Tako obuka ih kibernetičkog kriminala mora da se takmiči sa svim ovim drugim kursevima.
- U Poljskoj Državna škola za sudije i tužioce nudi kurseve osnovnog i naprednog nivoa u obliku konferencije koji traju četiri do pet dana. U toku 2009. godine organizirana su dva takva događaja („Metodologija krivičnih djela počinjenih upotrebom informacijskih sistema“ i „Elektronski dokazi na sudu“).

- U Rumuniji Državni institut za sudije nudi stručno usavršavanje, ali samo na osnovnom nivou. Na primjer od 2006. do 2009. godine svake godine su organizirana po dva seminara, svaki za približno 25 sudija odnosno tužilaca, većinom iz budžeta Instituta, neki finansirani sredstvima Evropske komisije (PHARE), a neki (2006. godine) uz podršku eBay-a. Predavači su sudije i stručnjaci za IT iz Rumunije, kao i inostrani eksperti koje su finansirale organizacije kao što je Vijeće Evrope. Kibernetički kriminal je, štaviše, obavezni predmet decentralizirane obuke na nivou tužilaštava apelacionih sudova. Ovu obuku takođe koordinira Državni institut za sudije.
- U Španiji, Španska pravosudna škola pod Općim pravosudnim vijećem provodi stručno usavršavanje sudija o kibernetičkom kriminalu i elektronskim dokazima. Za tužioce ovakvu obuku nudi Centar za pravne studije pod autoritetom Ministarstva pravosuđa. U oba slučaja obuk se organizira u saradnji sa CYBEX-om, privatnom kompanijom specijaliziranom za ovu problematiku. Pravosudna škola ima budžet od približno 42.000 eura za obuku o kibernetičkom kriminalu. Moguće je finansiranje i podrška iz privatnog sektora. Stručno usavršavanje obuhvata osnovne nivoe, a kursevi traju tri do četiri dana i uključuju predavanja i analize praktičnih slučajeva. Materijali se objavljuju i obično su dostupni svakom sudiji. Iako se nekim pitanjima ova obuka detaljnije bavi, ne postoji sistematski program naprednog nivoa.
- U Portugalu stručno usavršavanje o kibernetičkom kriminalu provodi Centar za pravosudne studije koji organizira oko 30 nastavnih događaja godišnje. Dva od njih su redovno posvećena osnovnim pitanjima kibernetičkog kriminala. Ponekad se održavaju i drugi seminari na slične teme, kao što su autorsko pravo na internetu ili tehnologija i sudovi. Predavači su sudije i tužioci, pravnici, pripadnici policije i eksperti iz javnog i privatnog sektora. Seminari su dobro primljeni i pohađa ih veliki broj učesnika (uglavnom tužioci, ali i pravnici i sudije iz krivičnih sudova).
- U Belgiji je program stručnog usavršavanja još uvijek u procesu pripreme, zbog nedavnog osnivanja „Institut-a de Formation Judiciaire“. Svrha je očito organizirati pravosudnu obuku, uzimajući u obzir rezultate i preporuke nekoliko „trustova mozgova“, među kojima i zapažanja Vijeća Evrope. Učešće belgijskih sudija i tužilaca u obuci u inostranstvu može finansirati Institut na zahtjev magistrata (npr. jedan sudija i jedan tužilac su pohađali program Evropskog sertifikata o kibernetičkom kriminalu i e-dokazima koji je organiziran u Parizu u februaru 2009. godine).
- Trenutno u Hrvatskoj nema stručnog usavršavanja o kibernetičkom kriminalu i/ili elektronskim dokazima. Ova problematika se obrađivala samo zahvaljujući CARDS programu u kojem je učestvovala i Hrvatska.
- U „Bivškoj Jugoslovenskoj Republici Makedoniji“ nema stručnog usavršavanja.
- Obuka koju organizira Akademija evropskog prava (ERA), formalno osnovana na inicijativu Evropskog parlamenta 1992. godine ima za cilj omogućiti dubinsko znanje i analizu evropskog prava i prava Evropske zajednice tako što će organizirati praktično usmjerene seminare i kurseve za pravnike. Akademija je takođe i forum za razmjenu iskustava i mišljenja o evropskom pravu i javnim politikama. ERA redovno organizira otvorene događaje o kibernetičkom kriminalu koje pohađaju učesnici iz cijele Evropske unije. U periodu 2009-2010. godina ERA sarađuje i sa TAIEX-om, provodeći niz seminara u Rumuniji, Bugarskoj i zemljama kandidatima i budućim kandidatima koje će predstavljati glavne evropske i međunarodne instrumente za borbu protiv kibernetičkog kriminala.

Svi seminari su planirani kao platforma za diskusiju i ocjenu kako se primjenjuje evropsko zakonodavstvo u oblasti kibernetičkog kriminala u različitim zemljama članicama i kandidatima, kao i perspektive jedne djelotvorne kampanje u cijeloj Evropi protiv ilegalnog

korištenja interneta. Na njima se raspravlja o najskorijim evropskim zakonskim aktima i instrumentima, kao što je Konvencija Vijeća Evrope o kibernetičkom kriminalu (2001.), Okvirna odluka Vijeća 2005/222/JHA o napadima na informacijske sisteme i Okvirna odluka Vijeća 2004/68/JHA o suzbijanju seksualnog iskorištavanja djece i dječje pornografije. Stalna saradnja sa dobavljačima internet usluga i web društvima kao što su Google, Microsoft i Yahoo! takođe su predmet razgovora.

Svaki seminar nudi mješavinu nastavnih metoda, koje variraju od uvodnih i dubinskih predavanja do studija slučaja i drugih vrsta interaktivnog učenja. Posebna pažnja se posvećuje diskusiji u manjim radnim grupama. Predavanja i radionice drže EU i domaći eksperti.

- U nekoliko zemalja edukativne događaje podržavaju i kompanije iz ove oblasti. Na primjer:

U Njemačkoj eBay je podržao kurs obuke „Novi mediji i krivično pravo“ za sudije i tužioce koji je organizirala Njemačka pravna akademija tako što je osigurao govornika koji je predstavio tržište eBay-, s tim povezane krivične aktivnosti, mjere koje se poduzimaju za suzbijanje tih aktivnosti i kako eBay funkcioniše u vezi provođenja zakona. eBay je takođe učestvovao na nekoliko jednokratnih obuka koje je organizirao Berlinski pravosudni senat na kojima je svaki put učestvovalo oko 100 tužilaca.

U Rumuniji je eBay održao brojne obuke za sudije, tužioce i predstavnike agencija za provođenje zakona. Konkretno, ebay je radio sa Tajnom službom SAD-a pri Američkoj ambasadi na pružanju obuke za 25 tužilaca iz različitih ureda DIICOT-a (Direkcije za istragu o organiziranom kriminalu i terorizmu), 15 sudija i 20 policajaca u Sibiu. Osim toga, eBay je učestvovao i na dodatnim edukacijama za sudije u Targu Jiu, kao i za 60 sudija iz različitih sudova koji spadaju pod žalbeni sud Craiova.

Kako je već rečeno, u skoro svim slučajevima za izmjenu ili dopunu plana i programa institucionalne obuke za sudije i tužioce potrebno je provesti formalni postupak odobrenja i usvajanja.¹¹

Iako je jasno da je u toku mnogo inicijativa da bi se zadovoljila potreba za odgovarajućom obukom o kibernetičkom kriminalu za sudije i tužioce, evidentno je da nema usklađenosti među gore opisanim pristupima.

Čak i kad uzmemo u obzir nacionalne specifičnosti pravnog sistema i činjenicu da su obrazovni sistemi veoma različiti, pitanja vezana za kibernetički kriminal su po svojoj prirodi međunarodna i zahtijevaju minimalan nivo koordinacije i usklađenosti među zemljama. Ako bi među državama postojalo slično razumijevanje toga šta je to kibernetički kriminal, moguće bi svakako bilo unaprijediti dosljednost sudskih odluka i spriječiti stvaranje utočišta za kriminalce, a institucije za obuku bi dobile kvalitetan nastavni sadržaj za manje novaca.

Na osnovu dobivenih informacija može se zaključiti sljedeće:

¹¹ U vezi sa ovim informacijama, interesantan je projekt naziva [“European Certificate on the fight against cybercrime and the use of electronic evidence”](#) koji implementira CYBEX sredstvima Evropske komisije (JPEN). Ova obuka uključuju četverodnevni standardizirani kurs osnovnog nivoa za sudije, tužioce i druge pravnike. U periodu od 2009. i kraja 2010. god. kurs će biti testiran u 14 pilot-zemalja Evrope i Latinske Amerike. Učesnici će dobiti certifikat kao dokaz da su stekli teoretsko i praktično, pravno i tehničko znanje osnovnog nivoa o pitanjima vezanim za elektronske dokaze i kibernetički kriminal. Vijeće Evrope – u okviru Projekta o kibernetičkom kriminalu – takođe je počelo aktivnosti na izradi priručnika za obuku sudija i tužilaca za jedan dvodnevni kurs osnovnog nivoa, s naglaskom na zakonima o kibernetičkom kriminalu.

- Većina obuka na radnom mjestu koje se sada nude obuhvata osnovni nivo.
- Nudi se samo nekoliko kurseva, koji dopijaju samo do malog broja sudija i tužilaca.
- U većini slučajeva osnovni kurs nije standardiziran. Zbog toga se on ne ponavlja i ne dozvoljava sudiji ili tužiocu da napreduje sa osnovnog na naprednije nivoe na jedan sistematski način. Holandija je vjerovatno izuzetak u ovome.
- Nastavni materijal je neorganiziran i priprema se *ad hoc*.
- Budući da, u konačnom, svim sudijama i tužiocima treba najmanje osnovno znanje o kibernetičkom kriminalu i elektronskim dokazima, obuka koje se sada provodi je zaista nedovoljna, naročito imajući u vidu da sadašnja generacija sudija i tužilaca po svoj prilici nije imala nikakvu obuku niti je obrađivala ove teme za vrijeme studija.
- Osim nekoliko izuzetaka, nema obuke koja daje znanje na naprednijem nivo za sudije i tužioce.
- S obzirom na međunarodni karakter kibernetičkog kriminala, potreban je minimalan nivo koordinacije i usklađenosti među državama.

6 Prijedlog pristupa

6.1 Cilj

Kao što je prikazano u prethodnom dijelu, općenito gledajući, sadašnja početna obuka i stručno usavršavanje ne omogućavaju sudijama i tužiocima sticanje znanja potrebnog za postupanje u slučajevima kibernetičkog kriminala i elektronskih dokaza.

Stoga su ciljevi ovog koncepta obuke za sudije i tužioce sljedeći:

- Omogućiti institucijama za obuku da provode početnu obuku i stručno usavršavanje zasnovano na međunarodnim standardima
- Opremiti najveći mogući broj budućih i sadašnjih sudija i tužilaca osnovnim znanjem o kibernetičkom kriminalu i elektronskim dokazima
- Pružiti naprednu obuku ključnom broju sudija i tužilaca
- Podržati kontinuiranu specijalizaciju i tehničku obuku sudija i tužilaca
- Doprinijeti povećanju znanja kroz povezivanje sudija i tužilaca
- Omogućiti pristup različitim edukativnim inicijativama i mrežama.

Sljedeće mjere bi trebalo da pomognu ostvarenju ovih ciljeva.

6.2 Institucionaliziranje početne obuke

- U zemljama u kojima je početna obuka praktična obuka na radnom mjestu (vrsta pripravništva ili nekoliko perioda pripravničkog rada) bez formalnog nastavnog programa, preporučuje se da barem jedan dio te obuke (npr. jedno pripravništvo ili slično) bude na temu kibernetičkog kriminala i elektronskih dokaza.
- U zemljama gdje početnu obuku provode institucije za obuku sudija i tužilaca:
 - nastavni program te institucije bi trebao da minimalno sadrži jedan modul osnovnog nivoa o kibernetičkom kriminalu i elektronskim dokazima
 - ovu problematiku bi dodatno trebalo uključiti i u obavezne module o materijalnom i procesnom pravu
 - trebalo bi nuditi i opcionalne module za sticanje naprednog znanja o kibernetičkom kriminalu i elektronskim dokazima.

Posebne module obuke bi trebalo standardizirati do te mjere da se mogu ponavljati i omogućiti kandidatima da napreduju od osnovnog do naprednih nivoa. To znači da se mogu ponavljati najmanje u istoj državi za različite polaznike, tako da učesnici različitih edukativnih događaja imaju sličan nivo znanja. To takođe znači da su metodi za pružanje obuke standardizirani. Da bi se osiguralo da kvalitet obuke bude konstantno na visokom nivou, potrebno je provoditi ocjenjivanje na kraju svakog kursa.

6.3 Insitucionaliziranje obuke na radnom mjestu

- Institucije za obuku na radnom mjestu treba da ponude najmanje jedan modul osnovnog nivoa o kibernetičkom kriminalu i elektronskim dokazima kako bi se opremili osnovnim znanjem oni sudije i tužiocima koji već obavljaju tu dužnost, a nisu imali tu vrstu obuke u toku početne obuke.
- Potrebno je da i ove institucije nude kurseve naprednog nivoa znanja.
- Ponavljamo: posebni moduli obuke treba da budu standardizirani u toj mjeri da budu obnovljivi i da mogu omogućiti kandidatima da napreduju od osnovnog do naprednih nivoa. Stoga može biti neophodno da se usklade moduli obuke na radnom mjestu što je više moguće sa modulima početne obuke. Metode održavanja obuke treba takođe da budu standardizirane, uključujući kontrolu kvaliteta pomoću evaluacija na kraju svakog kursa.

- Za obuku specijaliziranih sudija i tužilaca može se predložiti uvođenje pripravništva u jedinice za visokotehnoški kriminal ili postdiplomskih kurseva ili studija.¹²

6.4 Standardizirani i obnovljivi kursevi odnosno moduli

- Potrebno je razviti takve standardizirane kurseve ili module koji se mogu ponavljati u širem obimu i efikasno sa stanovišta troškova, a i tako da se budućim i sadašnjim sudijama i tužiocima omogući napredovanje sa osnovnog na napredni nivo.
- Potrebno je izvršiti ocjenjivanje postojećih osnovnih kurseva¹³ koji bi se mogli uvrstiti u nastavni program početne obuke i program stručnog usavršavanja. Kasnije se institucijama za početnu obuku i stručno usavršavanje može preporučiti jedan standardni kurs.
- Slično ocjenjivanje se može izvršiti za kurseve naprednog nivoa i može se kasnije predložiti jedan standardni napredni kurs.
- Na kraju, predavači na ovim programima treba da su oni koji su osposobljeni za držanje ovakvih kurseva u toj mjeri da to mogu biti domaći predavači koji predaju na svom jeziku, uz vrlo malu potrebu za međunarodnim predavačima.¹⁴

6.5 Pristup nastavnom materijalu ili materijalu za samostalno učenje

- Potrebno je pripremiti nastavni materijal koji će odražavati zajedničke međunarodne standarde i dobru praksu. Materijal za obuku treba da bude na raspolaganju institucijama za obuku na način efikasan način u pogledu troškova i s ciljem da se obuka održava na lokalnom nivou. Jasno je da, iako je za obuku za agencije za provođenje zakona koje se fokusiraju na tehnologiju i forenziku potreban visok nivo standardizacije, to nije slučaj za obuku sudija i tužilaca koji treba da budu obučeni prvenstveno za primjenu domaćih propisa. Pa ipak, moguće je razviti standardiziran materijal za obuku na takav način da se ostavi dovoljno prostora za uključivanje domaćih sistema i zakonodavstva.
- U nekim zemljama nastavni materijali stoje sudijama i tužiocima na raspolaganju na internetu.¹⁵ Ovu praksu bi trebalo da slijede i druge zemlje.
- Potrebno je izraditi internetske kurseve i omogućiti njihovo korištenje.¹⁶
- Pristup kursevima obuke (domaćim i međunarodnim) treba što je više moguće olakšati, pojednostavljujućem procedura za odobrenje.

¹² Na primjer, osnovni dvosedmični kurs koji je pripremila Irska garda i Univerzitetški koledž u Dublin mogli bi biti od interesa i za sudije i tužioce.

¹³ Na primjer, ECCE kurs je pripremio i trenutno ga provodi kao pilot-projekt CYBEX.

¹⁴ UCD i Interpol su pripremili kurs "obuču edukatora" koji se može koristiti. Obuhvaćene su vještine obučavanja, izrada kursa, i tako dalje. To NIJE kurs samo za agencije za provođenje zakona i može se držati za svakoga.

¹⁵ Primjeri su Holandija i CYBEX-ova biblioteka elektronskih dokaza. Kao dio Projekta 2CENTRE, UCD će pripremiti internetske resurse za dostavljanje nekih od nastavnih materijala AGIS/ISEC-a.

¹⁶ Na primjer, UCD trenutno nudi dva MS programa, čiji dijelovi se u potpunosti drže putem interneta. CEJ iz Portugala namjerava organizirati jedan kurs putem interneta o Sudovima i informacijsko-komunikacijskim tehnologijama, sa modulima o kibernetičkom kriminalu i elektronskim dokazima. Taj kurs će biti na portugalskom jeziku i razmatra se mogućnost njegovog širenja i u druge zemlje u kojima se govori portugalski (npr. Brazil, Cape Verde, Angola, Mozambik, Guinea-Bissau, Sao Tome ili Timor).

6.6 Pilot-centri za osnovnu i naprednu obuku

- Potrebno je osnovati nekoliko pilot-centara za osnovnu i naprednu obuku sudija i tužilaca o kibernetičkom kriminalu i elektronskim dokazima. U tim centrima bi se moglo:
 - Testirati i dalje razvijati standardizirane kurseve i materijale
 - Širiti dobru praksu
 - Provoditi istraživanja o obučavanju
 - Voditi registar predavača
 - Provoditi obuku predavača
 - Davati obuku drugim zemljama sa sličnim sistemima i jezikom.
- Pilot-centri treba da usklađuju svoj rad jedni s drugima, uz podršku Vijeća Evrope.
- Sudije i tužioći koji su spremni da budu specijalisti treba da razmatraju mogućnost učestvovanja u obuci putem centara izvrsnosti za agencije za provođenje zakona i kompanije iz ove oblasti.¹⁷

6.7 Povećanje znanja kroz međusobno povezivanje

Dok početna obuka i stručno usavršavanje daju sudijama i tužiocima jedan temelj, komunikacija sa kolegama, povezivanje sa drugim sudijama i tužiocima, ali i sa čitavim nizom drugih subjekata u ovoj oblasti od ključnog je značaja.

Iz tog razloga:

- Sudije i tužioći treba da koriste postojeće mreže za sudije¹⁸ i tužioce (kao što je GPEN).¹⁹
- Treba razgovarati o tome da Vijeće Evrope formira jednu međunarodnu mrežu za sudije koji sude u predmetima kibernetičkog kriminala odnosno „sudije za elektronski kriminal“ (slično kao GPEN za tužioce).
- Umrežavanje evropskih institucija koje nude obuku o kibernetičkom kriminalu i elektronskim dokazima treba da podrže Vijeće Evrope i Evropska mreža za obuku sudija i tužilaca.
- Da bi olakšali pristup sudijama i tužiocima ovim i mnogim mrežama vezanim za kibernetički kriminal, Vijeće Evrope – na svojoj web-stranici: www.coe.int/cybercrime – treba da označi inicijative i mreže i uspostavi portal sa linkovima, kratkim informacijama i kontakt-

¹⁷ [2Centre initiative \(Cybercrime Centres of Excellence Network for Training Research and Education\)](#) (Inicijativa 2 centra – Mreža centara izvrsnosti za istraživanje i obrazovanje u kibernetičkom kriminalu) pokrenuta je u martu 2009. god. (za vrijeme Konferencije "Octopus" Vijeća Evrope). 2centra "proučava metode obuke za agencije za provođenje zakona i kompanije za oblast forenzičke informacijske i komunikacijske tehnologije i istrage o kibernetičkom kriminalu. Pregleda aktivnosti koje preduzimaju pripadnici agencija za provođenje zakona i osoblje kompanija za sticanje znanja i vještina u oblasti u kojoj je trenutno mnoštvo različitih vrsta i nivoa stručnog usavršavanja, obuke unutar institucije, obuke kombiniranjem različitih metoda i usavršavanja na radnom mjestu". Univerziteti u Troju postaću drugi 2010. godine.

¹⁸ Čini se da međunarodna mreža sudija koji rade na predmetima kibernetičkog kriminala i s elektronskim dokazima još ne postoji. Primjer jedne inicijative na nivou države je nešto što je razvila Holandija gdje je kreiran intranet resurs poput *wiki* (wikipedia, npr.) internet stranica.

¹⁹ Globalna mreža tužilaca za elektronski kriminal, GPEN, predstavlja inicijativu nastalu 2008. godine čiji je nosilac Međunarodno udruženje tužilaca (IAP). Ova mreža ima za cilj omogućiti razmjenu informacija i saradnju među tužiocima u predmetima koji se tiču elektronskog kriminala ili kibernetičkog kriminala, a u odnosu na Konvenciju o kibernetičkom kriminalu, za razvijanje i držanje programa obuke, te pružiti internet resurse tužiocima. GPEN je mreža specijaliziranih tužilaca za elektronski kriminalitet i svaki član Međunarodnog udruženja tužilaca je pozvan da imenuje najmanje jednog tužioca koji će se registrirati kao nacionalna kontakt-osoba za GPEN mrežu. Mrežom upravlja Odbor za razvoj GPEN-a koji čine članovi iz reda Međunarodnog udruženja tužilaca.

informacijama o različitim mrežama. Na taj način će se dodatno omogućiti pristup postojećim materijalima i inicijativama.

6.8 Saradnja između javnog i privatnog sektora

Organizirana i uređena saradnja agencija za provođenje zakona i privatnog sektora (područje IKT-a, uključujući dobavljače internet usluga) od suštinske je važnosti za istragu o kibernetičkom kriminalu i osiguranje elektronskih dokaza²⁰, a privatni sektor doprinosi ekspertizom i drugim vidovima podrške inicijativama za obuku agencija za provođenje zakona.

Korisna bi bila podrška privatnog sektora obuci sudija i tužilaca, imajući na umu da privatni sektor raspoložuje potrebnim stručnim znanjem o ovoj temi. U isto vrijeme, sudije i tužiocima moraju ostati nezavisni i nepristrasni.

Iz tog razloga:

- Institucije za obuku sudija i tužilaca mogu koristiti ekspertizu koja postoji u privatnom sektoru kada osmišljavaju programe obuke, izrađuju materijale za obuku i drže kurseve.
- Podrška privatnih organizacija institucijama za obuku ne smije se posmatrati tako kao da će se putem nje doći do nekih povoljnih sudskih odluka ili da će donijeti posao, nego kao način da sudije i tužiocima dobiju adekvatne informacije koje im omogućavaju da donesu informirane odluke.
- Privatni sektor može na transparentan način dati podršku međunarodnim ili domaćim organizacijama, akademijama, inicijativama za obuku ili ostalim trećim stranama koje će zatim podržati nezavisne institucije za obuku.
- Iako je važno da sudije i tužiocima imaju pregled o internetu i kibernetičkom kriminalu, isto tako je važno da im se daju informacije koje se odnose samo na konkretnu platformu. Kompanije koje se bave ovom djelatnošću mogu dati materijal za posebne module (umjesto čitavog kursa) o tome kako rade platforme od značaja za razumijevanje.

²⁰ Vidjeti, na primjer, Smjernice za provedenu zakona – saradnja sa dobavljačima internet usluga usvojene na Konferenciji "Octopus" Vijeća Evrope u aprilu 2008. godine.

7 Podrška realizaciji ovog koncepta

Realizacija ovog koncepta je prije svega u nadležnosti institucija za obuku sudija i tužilaca, ali trebalo bi da dobije podršku od javnih i privatnih institucija i partnera, uključujući i međunarodne organizacije. Imajući u vidu značaj informacijskih i komunikacijskih tehnologija za društvu, finansiranje ovakvih mjera obuke predstavljalo bi vrijednu investiciju i potrebno je učiniti svaki napor da institucije za obuku dobiju odgovarajuće resurse.

Vijeće Evrope i Evropska mreža za obuku sudija i tužilaca, kao i druga tijela, treba da zagovaraju i podstiču realizaciju ovog koncepta u cijeloj Evropi i šire.

Ova Evropska mreža i Vijeće Evrope bi mogli organizirati jednu zajedničku konferenciju o ovom konceptu u skoroj budućnosti.

Vijeće Evrope i Evropska mreža treba da redovno ocjenjuju ostvareni napredak.

Realizaciju ovog koncepta u praksi bi takođe trebalo da podrže donatori. Zainteresirani donatori i organizacije bi mogli da se udruže i kao partneri izrade projekte kako pomoći institucijama za obuku i drugim akterima koji su spremni da preuzmu odgovornost za mjere predložene u ovom konceptu.

Da bi se smanjio rizik sukoba interesa ili ugrožavanja nepristrasnosti sudija i tužilaca, donatori bi trebali da, umjesto da nude direktnu podršku, daju sredstva neutralnim trećim stranama, kao što su međunarodne organizacije, koje će onda komunicirati sa institucijama za obuku.

8 Dodatak

8.1 Lisabonska mreža: linkovi sa institucijama za obuku sudija i tužilaca

Četrdeset četiri od četrdeset sedam država članica Vijeća Evrope predstavljeno je u Lisabonskoj mreži. Članovi Lisabonske mreže su relevantne domaće institucije tih država zadužene za početnu obuku i stručno usavršavanje sudija i tužilaca. To takođe mogu biti, zavisno od slučaja, Škole za sudije i tužioce, Centri za obuku u pravosuđu ili odjeljenja za obuku sudija i tužilaca u Ministarstvu pravosuđa.

Za informacije o svakoj od država članica Mreže (uključujući i u nekim slučajevima slične programe obuke), pogledati:

- | | | |
|--|-----------------------------|---|
| Albania | Germany | Portugal |
| Andorra | Greece | Romania |
| Armenia | Hungary | Russian Federation |
| Austria | Iceland | Serbia |
| Azerbaijan | Ireland | Slovakia |
| Belgium | Italy | Slovenia |
| Bosnia and Herzegovina | Latvia | Spain |
| Bulgaria | Lithuania | Sweden |
| Croatia | Luxembourg | Switzerland |
| Cyprus | Malta | "the former Yugoslav Republic of Macedonia" |
| Czech Republic | Moldova | Turkey |
| Denmark | Montenegro | Ukraine |
| Estonia | Netherlands | United Kingdom |
| Finland | Norway | - England and Wales |
| France | Poland | - Scotland |
| Georgia | | |

Status posmatrača

- [UNMIK](#)

8.2 Primjeri osnovnog kursa obuke: struktura i teme koje se obrađuju

8.2.1 Primjer Holandije

Osnovna obuka – 1 dan

Program:

- 1 Opća orijentacija:
 - Šta je kibernetički kriminal?
 - Manifestacija kibernetičkog kriminala
 - Pravni okvir za agencije za provođenje zakona i tužilaštvo
- 2 Provođenje zakona:
 - Digitalno provođenje zakona kao svakodnevna praksa
 - Metodi provođenja zakona
- 3 Provođenje zakona (drugi dio):
 - internet i provođenje zakona prema zakonu o posebnim privilegijama za agencije za provođenje zakona

Zaključci i ocjenjivanje

8.2.2 Primjer Njemačke (Njemačka pravosudna akademija)

Osnovna obuka: „Pojavni oblici i strategija za borbu protiv kibernetičkog kriminala“ – 4 dana

Program:

Prvi dan:

- Materijalni krivični zakon Njemačke
- Primjena krivičnog zakona Njemačke u kontekstu kompjuterskog i internet kriminaliteta
- Problemi s kojima se svakodnevno susreću tužilaštvo i sud

Predavač je sudija Suda u Minhenu specijaliziran za finansijski i privredni kriminal, a prije nekoliko godina je bio tužilac koji je radio na predmetima kibernetičkog kriminala, špijuniranja podataka, korumpiranja podataka, i tako dalje.

- Problemi s kojima se svakodnevno susreću tužilaštvo i sud u Holandiji
- Razvoj i suzbijanje kibernetičkog kriminala u Evropi
- Problemi sa dobavljačima internet usluga u Holandiji i drugim evropskim zemljama
- Konvencija o kibernetičkom kriminalu Vijeća Evrope
- Značaj i važnost Konvencije o kibernetičkom kriminalu za Evropu i ostatak svijeta (Kina, SAD, Rusija)

Predavač je profesor dr Henri Kaspersen, Holandija

Drugi dan:

- Sabotaža kompjuterskih sistema
- Internetsko hakiranje
- Zaustavljanje internet naredbi
- Špijuniranje podataka
- Kompjuterske prevare s kreditnim karticama
- Napadi na bankovne podatke
- *Phishing* i nova vrsta kriminala na internetu
- *Botnet*
- Prevara na eBay-u ili drugim prodajnim platformama

Predavač je policajac Njemačkog policijskog štaba u Wiesbadenu

- 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 za otkrivanje dječje pornografije
- Međunarodna saradnja u pretraživanju mreže
- *Onlajn* pretraživanje (problemi sa ustavom)

Predavač je voditelj posebnog odjeljenja Štaba bavarske policije u Minhenu

Treći dan:

- Sigurnosno kopiranje i ocjenjivanje podataka u Njemačkoj ili drugim zemljama
- Pretraživanje podataka na internetu i mogućnost praćenja podataka na mreži
- Mogućnosti forenzičkog IT-a i ograničenja analize podataka
- Sistemi anonimiziranja podataka na mreži
- Korištenje kriptograma od strane kriminalnih osoba

Predavač je stručnjak iz Štaba policije Minhena

- Novi pravni problemi sa sigurnosnim kopiranjem i evaluacijom podataka sa interneta
- Nadležnost za sve zakonske mjere pretraživanja
- Nadležnost za pribavljanje dokaza za istragu i za sud
- Novi razvoj u provođenju zakona

Predavač je sudija Bavarskog krivičnog višeg suda u Bambergu

Četvrti dan:

- Ruska poslovna mreža
- *Intercage*
- Zaštita od sabotaže kompjutera i podataka
- Pozitivno „hakiranje“
- Uticaj i falsificiranje izbornih mašina
- Politički uticaj u novim zakonima
- Populacija osjetljiva na napade

Predavač je član čuvenog Kompjuterskog kluba haosa (Chaos Computer Club (CCC)) iz Hamburga, čiji članovi nastoje ući u kompjutere vlade, Bijele kuće, CIA-e. Ovaj klub pokazuje kako se može manipulirati vodosnabdijevanjem grada i slično.

8.2.3 Primjeri Vijeća Evrope

1. Radionica iz oblasti kibernetičkog kriminala za tužioce u Belo Horizonteu u Brazilu, 26. avgust 2008. godine (koju je organizio *Ministério Público Estadual Minas Gerais* u saradnji sa Vijećem Evrope)

Osnovna obuka – prvi dan

Program:

- 1 Uvodna sesija
 - Uvodne napomene
 - Sadašnja zakonodavna reforma
- 2 Kibernetički kriminal: pojave
 - Pregled sadašnjih prijetnji
 - Posebne prijetnje i slučajevi predmeti istrage u Brazilu
- 3 Materijalno pravo: koja krivična djela?
 - Međunarodni standardi
 - Tipologija, pravni instituti
 - Konvencija o kibernetičkom kriminalu

- Odredbe zakona Brazila
 - Sadašnje zakonske odredbe
 - Pravne reforme u toku
- 4 Istrage i međunarodna saradnja
 - Uloga tužilaca u istrazi o kibernetičkom kriminalu
 - Domaće procesno pravo
 - Procesne mjere i međunarodna saradnja prema Konvenciji o kibernetičkom kriminalu
- 5 Partnerstvo javnog i privatnog sektora
 - Primjeri partnerstva javnog i privatnog sektora u Brazilu
 - Provođenje zakona – saradnja sa dobavljačima internet usluga u istrazi o kibernetičkom kriminalu: smjernice
 - Rasprava: provođenje zakona – saradnja sa dobavljačima internet usluga: iskustvo u Brazilu

2. Kibernetički kriminal: obuka za sudije u Kairu u Egiptu, 9 – 10. juni 2008. god. (u organizaciji Microsoft-a, uz doprinos Vijeća Evrope)

Ovaj kurs je održan dva puta za različite grupe sudija sa trgovačkih sudova (i oni su takođe nadležni za rješavanje elektronskog kriminala)

Osnovna obuka – prvi dan

Program:

- 1 Uvodna sesija
- 2 Kibernetički kriminal: pojave
 - Pregled sadašnjih prijetnji
 - Posebne prijetnje
 - Prevarna upotreba identiteta i informacija na internetu: primjeri
 - Kreditne kartice i druge vrste prevare
- 3 Materijalno pravo: koja su krivična djela?
 - Međunarodni standardi (ekspert Vijeća Evrope)
 - Tipologija, pravni instituti
 - Konvencija o kibernetičkom kriminalu
 - Inkriminiranje krađe identiteta
 - Odredbe domaćih zakona
 - Sadašnje odredbe
 - Pravne reforme u toku

Drugi dio – Dokazi u postupku kibernetičkog kriminala

- 4 Istraga i krivični postupak
 - Procesne mjere prema Konvenciji o kibernetičkom kriminalu
 - Uloga policije, tužioca, sudije, specijalnih službi
 - Domaći procesni zakon
- 5 Međunarodna saradnja
 - Konvencija o kibernetičkom kriminalu
 - Odredbe domaćih zakona i bilateralnih sporazuma
 - Kontaktne tačke otvorene 24 sata 7 dana
 - Uloga sudije

6 Pribavljanje, zaštita, korištenje elektronskih dokaza

- Dokazi na kompjuteru okrivljene osobe: prisustvo digitalnih datoteka korištenih za kibernetički kriminal
- Dokazi kojima se potvrđuje lokacija mreže: IP adrese
- Dokazi pribavljeni od dobavljača internet usluga

7 Sudski postupak i sudska praksa: primjeri

8.3 Primjeri naprednog kursa obuke: struktura i teme koje se obrađuju

8.3.1 Primjer Holandije

Dubinska obuka – 4 dana

Program:

Prvi i drugi dan

Infrastruktura interneta

- Razumjeti kako internet funkcionira
- Kako kompjuteri komuniciraju?
- Šta su brojevi IP i imena kompjutera?

Informacije na internetu

- Kako prikupljati informacije sa interneta
- Pretraživanje (skrivenih) internet baza podataka

Profiliranje društvenih mreža

- komunikacija
- anonimnost
- odrediti lokaciju i identitet kompjutera, kompanija i osoba na internetu

Digitalni tragovi

- šta su "tragovi"?
- koji tragovi ostaju na kompjuteru?
- koji tragovi ostaju na internetu?
- koji tragovi se mogu naći u internetskoj komunikaciji?

Sigurnost

- opasnosti od interneta
- značaj dobre digitalne zaštite
- sigurno pohranjivanje informacija
- zaštita e-mejla

U toku ova dva dana svaki učesnik ima pristup kompjuteru povezanom na internet i stiče direktno iskustvo u vezi tema koje se obrađuju. Učesnici će dobiti ime određene osobe i zadatak da prikupe što je više moguće informacija o toj osobi iz internetskih izvora kojima je moguć slobodan pristup. Takođe će im biti zatraženo da prate porijeklo e-mejlova (pomoću e-mejl zaglavlja) ili da traže tragove u digitalnoj komunikaciji.

Treći i četvrti dan

Pravni okvir

- Koje nadležnosti ima policija i tužilaštvo u istrazi o kibernetičkom kriminalu
- Studija slučaja od strane tima za visokotehnološki kriminal

Organizacija istražnog postupka i krivičnog gonjenja kibernetičkog kriminala u Holandiji;

Presretanje (to neće biti u novom kursu, jer će biti dio osnovnog programa);

Digitalni odgovori na prigovor

- koji su poznati odgovori na prigovor
- sudska praksa vezana za te odgovore
- koje odgovore na prigovor treba očekivati u budućnosti i kako na njih odgovoriti
- studije slučaja

Svakom učesniku se osigurava nastavni materijal, čitanka koja sadrži sve teme koje se obrađuju na obuci i koje se mogu koristiti kao referentna literatura, odštampane prezentacije predavača i Udžbenik o digitalnom kriminalitetu autora Arjana Dasselaar-a.

8.3.2 Prijedlog Holandije za održavanje obuke s vodećim ekspertom

Izrada novog kursa o kibernetičkom kriminalu

'Intensiveringsprogramma Cybercrime' (Intenzivni program o kibernetičkom kriminalu), Državni tužilac za kibernetički kriminal i Holandski centar za obuku sudija i tužilaca pripremaju novi kurs o kibernetičkom kriminalu koji će obuhvatiti teme od „presretanja“ do obuke sa vodećim ekspertom na izabrane teme (*botnet*).

Još uvijek program nije u potpunosti završen, ali planirano da se prvi dan govori o osnovama presretanja (prislušivanje telefona i interneta), drugi dan će biti osnovni kurs o kibernetičkom kriminalu. Oba ova kursa će biti obavezna za sve tužioce u Holandiji kao dio njihovog stalnog stručnog usavršavanja. Drugi dio kursa je samo za specijaliste za kibernetički kriminal (primjenjivat će se strogi uvjeti za prijem na ovaj kurs) i sastoji se od jednog dubinskog kursa (2 do 4 dana) i dva dana „master“ kursa, tj. nastave sa vodećim ekspertom u oblasti (godišnje). Ovi kursevi će se držati u saradnji sa vanjskim partnerima kao što su Fox-IT, „Digital Intelligence Training“ i „Hoffman Bedrijfsrecherche“.

Razlog za pripremu ovakvog kursa nije nezadovoljstvo sadržajem dosadašnje obuke, nego da se osigura da dijelovi kursa budu bolje strukturirani i bolje prilagođeni jedan drugom, tako da ne dolazi do preklapanja. Imenovanje tužilaca za kibernetički kriminal u jedanaest velikih ureda Holandskog tužilaštva kao dio „Intenzivnog programa“ takođe je važan razlog za izradu odnosno prestrukturiranje obuke. Takođe je od vitalnog značaja za novi kurs da postoji postepeni napredak: od svakog učesnika se zahtijeva da prvo prođe dva osnovna kursa, a nakon toga pristupa dubinskom programu i „master“ kursu.

Jedna od mogućih novih karakteristika nove obuke biće info-grafikoni o radu i opasnostima od interneta. Ovi info-grafikoni su trenutno u završnoj fazi izrade i mogu se koristiti za probne prezentacije. U nastavku je dato nekoliko primjera kako će info-grafikoni izgledati.



Dalja obuka

Da bi se postiglo da tužioc koji rade na rješavanju slučajeva kibernetičkog kriminala u svom svakodnevnom radu budu sposobni pratiti najnovije događaje u svijetu kibernetičkog kriminala koji se razvija strahovitom brzinom, trenutno se pripremaju dva dodatna programa.

Prvi je uspostavljanje Centra znanja i ekspertize u Državnom tužilaštvu u Rotterdamu. Ovaj centar će dati odgovore na pitanja tehničke prirodi i iz oblasti pravosuđa, pratit će najnovije sudske slučajeve i distribuirati te i druge bitne informacije među profesionalcima koji rješavaju kibernetički kriminal, kako u policijskim snagama, tako i u Tužilaštvu (ovaj centar su zajednički uspostavile ove dvije organizacije).

Kao drugi program i dodatak ovom projektu pripremljena je „digitalna prostorija za saradnju“, koja se može porediti sa „sharepoint“ aplikacijom. U ovoj virtualnoj sobi profesionalci koji rješavaju kibernetički kriminal mogu razgovarati o pitanjima vezanim za svoj rad i pronaći sve vrste informacija koje se tiču njihovog rada. U oktobru ove godine napravit će se popis svega onoga što bi trebalo da bude sadržaj i (tehničke) mogućnosti takve digitalne sobe. Ovo je primjer kako prva stranica digitalne sobe može izgledati:

OPENBAAR MINISTERIE

OM Portal | Samenwerkingsruimte

Welkom Reinier van Loon | Mijn Site | Mijn Links

zoek...

Voorpagina | **Agenda** | **Mensen** | **Documenten** | **Discussie**

OM Portal > Samenwerkingsruimte > Cybercrime

Deelnemers samenwerkingsruimte

Naam:	Functie:
Jan Hoekman	
Reinier van Loon	
Danielle Laheij	

[Deelnemers toevoegen](#)

Laatste discussies / reacties

Discussie	Aantal reacties:
Cybercrime of niet? <i>Nieuw</i>	0
Is downloaden strafbaar?	10

[Deelnemers toevoegen](#)

Laatste documenten

Titel document:	Laatst bewerkt door:	Datum:
Samenvatting Plan van Aanpak Cybercrime <i>Nieuw</i>	Jan Hoekman	26 juni 2009 - 15:23
Plan van Aanpak Cybercrime	Reinier van Loon	19 mei 2009 - 08:42

[Document toevoegen](#)

RSS feed

Nu.nl (internet)

- Liever zonder televisie dan zonder internet *Nieuw*
- China blokkeert Google om porno *Nieuw*
- Reparatie site Brein duurt zeker etmaal
- Thuiskopie wil schadevergoeding uitblijven mp3-heffing

[RSS feeds toevoegen](#)

Agenda

Agenda punten:	Datum:
Brainstorm Cybercrime Samenwerkingomgeving	29 juni 2009 - 15:00
Kickoff Cybercrime officieren	06 september 2009 - 14:00

[Agenda item toevoegen](#)

Stvaranje osjećaja hitnosti: obuka na nivou rukovoditelja

S obzirom na relativno mali kapacitet holandske policije, neophodno je vršiti odabir krivičnih djela koja će biti predmet istrage i onih koja neće (napomena: Prema holandskom pravnom sistemu tužilaštvo može da ne vrši istragu i krivično gonjenje krivičnog djela, što se naziva „opportunitetsbeginsel“). Obično su ovo odluke koje donose rukovoditelji institucije.

Policija i Tužilaštvo priznaju da na ovom nivou nema dovoljno znanja o posljedicama kibernetičkog kriminala i značaju njegovog suzbijanja, tako da postoji opasnost da se važni slučajevi neće rješavati zbog toga što se druga (konvencionalna) krivična djela smatraju važnijim. Zbog toga se trenutno priprema program obuke za rukovoditelje policije i Tužilaštva. Prema planu, krajem ove godine održat će se jedan pilot-kurs. Cilj ovog kursa je stvoriti osjećaj hitnosti rješavanja ovih slučajeva i uglavnom će se polaznici suočiti sa realnošću kibernetičkog kriminala u današnjem društvu. Temama se neće baviti na nivou sadržaja (kao što se to čini u dubinskom programu), nego na strateškom, rukovodećem nivou.