جرایم سایبری یا اینترنتی

به دنبال برگزاری کلاس های آموزشی ضمن خدمت قضات در دادگستری استان تهران، از مهرماه ۸۲ دو عنوان درسی-آموزشی در برنامه های این دوره گنجانیده شد. این عناوین عبارتند از: الف؛ جرایم اینترنتی (یا به تعبیر درست تر جرایم سایبری؛ جرایم علیه تکنولوژی اطلاعات) برای قضات کیفری. ب؛ دعاوی اینترنتی (یا به تعبیر درست تر حقوق سایبر؛ حقوق تکنولوژی اطلاعات) برای قضات حقوقی. در دوره جرایم سایبری این مباحث به صورت مقدماتی و در ۵ جلسه درسی ارائه می شود: ۱-کلیات شامل ادوار زمانی استفاده از کامپیوتر و مسائل جزائی و حقوقی ناشی از هر دوره زمانی، رشته های جدید حقوق و جرایم سایبری و ...، ۲-ماهیت جرایم سایبری، ۳ و ۴-تقسیم بندی و شرح مختصر دسته های جرایم سایبری. ۵-آیین دادرسی جرایم سایبری و صلاحیت سایبری. نیز در دوره حقوق سایبر (دعاوی اینترنتی به تعبیر مذکور در برنامه دوره) این مباحث با توجه به اندازه ۵ جلسه درسی طرح می شود: ۱-کلیات (مشترک با دوره کیفری)، ۲ و ۳-قراردادهای انفورماتیک، ۴-مسئولیت مدنی در محیط دیجیتال، ۵-مالکیت فکری در فضای سایبر. از آن جا که مطالب کلاس بسیار کلی و در حد بیان فهرست و ذکر مشکلات و مباحث حقوقی است، برآنیم در ماهنامه قضاوت برخی مباحث را به طور جزئی تر مطرح کنیم تا قضات، حقوقدانان، وکلا و دانشجویان حقوق بتوانند بسته به علایق خود به مطالعات تفصیلی روی آورند. به طور طبیعی مطالب طرح شده در این سلسله مقالات شامل موضوعات مختلف اما مطرح در حقوق سایبر و جرایم سایبری است. خوانندگان محترم در صورت تمایل به پیگیری مطالب به صورت منظم و حسب ترتیب و توالی منطقی، تئوریک و تاریخی می توانند به جزوه های درسی این مرقومات و مقالات منتشره در خبرنامه انفورماتیک (شورای عالی انفورماتیک) مراجعه کنند. آن چه می آید قسمت اول این موضوع است که توسط محمد حسن دزیانی تهیه و به نگارش درآمده است.

■ پیشگیری از جرایم سایبری

قواعد نت اسمارت برای حمایت از کودکان در اینترنت:

به کاربران خردسال، نوجوان و جوان توصیه می شود:

۱ - هرگز آدرس خانه، شماره تلفن، اسم مدرسه و ... خود را از طریق اینترنت به هیچ کس ندهید، مگر با اجازه و آگاهی اولیاء و سرپرستان قانونی خود.

۲ - هرگز عکس، مشخصات کارت اعتباری یا جزئیات حساب بانکی یا هر مطلب شخصی و خصوصی خودتان را از طریق اینترنت به کسی ندهید، مگر با اجازه و آگاهی اولیاء و سرپرستان قانونی خود.

۳ - هرگز گذرواژه (password) خودتان را به هیچ کس حتی بهترین دوستانتان ندهید.

۴ - هرگز از طریق اینترنت با دیگران و افراد ناشناس قرار ملاقات نگذارید، مگر اینکه والدین و سرپرستان قانونی شما مطلع باشند. در صورت انجام نخستین ملاقات، بلافاصله اولیای خود را آگاه و مطلع کنید. باید ملاقات ها، همیشه، در مکان های عمومی باشد.

۵ - هرگز در اتاق گفتگو و مکالمه (چت) یا کنفرانس های اینترنتی شرکت نکنید. زمانی مطالب مکتوب یا مطروحه در آن باعث آزار شما می شود یا موجب بی اعتمادی شما می شود. همیشه این موارد را به اولیاء یا سرپرستان قانونی خودتان اطلاع دهید.

۶ - هرگز به پست الکترونیک یا بسته های پستی حاوی مطالب زشت و زننده یا غیر اخلاقی جواب ندهید، خواه در گروه های خبری باشد یا یوزنت و ...

۷ - هرگاه در حال کار آن لاین و ارتباط اینترنتی با تصاویر زننده و مستهجن یا پیام های بد و غیر اخلاقی مواجه شدید، اولیاء خود را مطلع سازید.

۸ - همیشه مطالب درستی از خود منعکس کنید (راست بگویید) و هیچ گاه اطلاعات گمراه کننده یا غلط به کسی ندهید.

۹ - هرکس صدای زیبایی دارد لزوما سیرت زیبایی ندارد. اگر پیشنهاد، مطالب و حرف های کسی ظاهرا خوب و مطمئن است، ممکن است در واقع منفی، مضر و گمراه کننده باشد.

توضیحات:

- مطالب فوق بسیار سودمند است و در پیشگیری از وقوع جرایم سایبری و مبارزه با آن نقش مهمی ایفا می کند.
- به حکایت آمار و اطلاعات، کودکان و نوجوانان از اولیا، معلمان و اولیای خود بیشتر با تکنولوژی اطلاعات مانوس و آشنا هستند. از طرفی این نکته نشان دهنده ارتقای سطح کمی و کیفی دانش فنی کودکان، نوجوانان و جوانان است. از سوی دیگر حاکی از عقب ماندن اولیاء و . . . از کودکان و فرزندان خود و بالطبع افزایش میزان بزه‌دیدگی و . . . است. آشنایی هرچه بیشتر کودکان و نوجوانان با تکنولوژی اطلاعات، موجب آلودگی و بزه‌دیدگی آن‌ها خواهد شد، اگر هشدارهای تربیتی-قضایی را نادیده بگیرند یا اصولا چنین هشدارهایی را دریافت نکنند.
- دسته ای از جرایم سایبری، جرایم علیه کودکان و نوجوانان در دسته جرایم علیه محتوا است.

■ اقسام جرایم سایبری

جرایم سایبری - کامپیوتری دارای چند دسته یا طبقه کلی هستند که عبارتند از: ۱ - جرایم کلاسیک با توصیف سایبری شامل جعل سایبری، کلاهبرداری سایبری و . . . ، ۲ - جرایم علیه محتوا شامل جرایم علیه کودکان و نوجوانان، افتراهای اینترنتی، پورنوگرافی، ترویج ایدئولوژی‌های مضر و . . . ، ۳ - جرایم صرف تکنولوژی اطلاعات شامل جرایم دستیابی غیر مجاز، شنود و . . . ، ۴ - جرایم مخابراتی شامل جرایم ماهواره، شنود مخابراتی، جرایم موبایل و . . . ، ۵ - جرایم با مبنای غیر جزایی شامل جرایم مالکیت فکری، جرایم بانکداری الکترونیک، جرایم تجارت الکترونیک، جرایم حمایت از داده و . . .

- افرادی که از آن‌ها به عنوان شاهین شکاری یاد می‌شود با استفاده از اتاق های گفتگوی اینترنتی (چت) یا استفاده از گروه‌های خبری و . . . با اتخاذ ماهیت کذب و غالبا مثبت، خود را افرادی درستکار، هنرمند و . . . نشان می دهند و کودکان یا نوجوانان و حتی بزرگسالان مخاطب آن‌ها بدون آگاهی از ماهیت این افراد، به راحتی با آن‌ها گفتگو می کنند، اطلاعات مختلفی به آن‌ها می‌دهند و حتی قرار ملاقات می گذارند. شاهین‌ها معمولا در کار قاچاق کودکان، نوجوانان و زنان برای مقاصد غیر اخلاقی و فروش اعضای بدن، قاچاق مواد مخدر و . . . هستند.
- اطلاعات کارت اعتباری یا جزئیات حساب بانکی با کار مجرمان مالی به‌ویژه کلاهبرداران سایبری، جاعلان سایبری و . . . می آید. گذرواژه‌ها، آدرس ها و . . . با کار غالب مجرمان می آید، از جمله کسانی که به تخریب سایبری، نفوذیابی، دستیابی غیر مجاز و . . . اقدام می کنند.
- عکس خواه کامل یا فقط مربوط به چهره، یکی از بهترین ابزار سوء استفاده مجرمین اخلاقی (پورنوگرافرها) است.

این افراد عکس ها را می گیرند در حالی که صاحب عکس از نیت این افراد آگاهی ندارد و حتی برای این کار پوشش موجه و قانونی به شکل سایت حاوی مطالب هنری، آموزشی یا . . . درست می کنند و درصدد تهیه عکس از کاربر و بازدید کننده بر می آیند. این کار در واقع برای افزودن عکس به بدن عریان و . . . صورت می گیرد.

برنامه هایی مانند فتوشاپ که برای گرافیک استفاده می شود قادر به خلق تصاویر کاذب یا نیمه کاذب به صورت عریان، نیمه عریان یا در حال انجام اعمال غیر اخلاقی هستند. البته فتوشاپ یکی از برنامه های ارزشمند گرافیک است اما از آن سوء استفاده نیز می شود.

اولیاء در صورت برخورد با پیام‌های زشت یا تصاویر مستهجن می توانند به مقامات قضایی و پلیسی اطلاع دهند تا آنان با توجه به توان فنی که دارا هستند به راحتی مجرم یا مجرمان را دستگیر کنند

ارسال عکس برای کسی که نمی شناسیم، دادن شماره تلفن و . . . به افراد ناشناس خطر قرار گرفتن در لیست های منفی و مجرمانه را دارد. پاسخ به پست الکترونیک ناشناس یا غیر ضروری موجب شناسایی آدرس پست الکترونیک آن فرد می شود و آن گاه این فرد در معرض دریافت ای‌میل هایی با محتوای مضر یا غیر اخلاقی قرار می گیرد.

- والدین در صورت برخورد با پیام‌های زشت یا تصاویر مستهجن می توانند به مقامات قضایی و پلیسی اطلاع دهند تا آنان با توجه به آموزش‌ها و توان فنی که دارا هستند به راحتی مجرم یا مجرمان را دستگیر کنند.
- در غالب کشورها، نهادهای غیر رسمی اما تحت الحمایه دولت تشکیل شده‌اند که به آن‌ها هات لاین یا خط آتش می گویند. این خطوط، معمولا پیام های حاوی مخاطرات در زمینه های مختلف مالی، اخلاقی و . . . را از افراد دریافت و به پلیس یا مقام قضایی اطلاع می دهند و در کار تعقیب مجرمان مشارکت و نظارت دارند.
- هشدارهایی که در متن برای کودکان و نوجوانان آمده، از آن جا که بسیار ارزشمند است، بنا به توصیه ارگان‌های ذی ربط بین المللی باید به نحو مقتضی به اطلاع مدیران مدارس، مدیران کافی نت‌ها، مسئولان سایت‌ها، اولیاء و تهیه کنندگان خدمات اینترنت برسد تا از این طریق کاربران و کودکان مطلع شوند و درصد مخاطرات کاهش یابد و از میزان و امکان بزه‌دیده شدن این قشر سنی کاسته شود.

■ راهنمای پژوهشگران

حقوق تکنولوژی اطلاعات: در هر شماره در این بخش سعی می شود با شاخه‌های جدید حقوق و جرایم سایبری و نیز برخی منابع مفید آشنا شویم.

پیشنهاد ۲ واحد درس کشف علمی جرایم سایبری؛

معرفی ماخذ:

Searching and seizing computer and obtaining electronic evidence in criminal investigation

تفتیش و توقیف کامپیوترها و تحصیل ادله الکترونیک در تحقیقات جنائی.

با پیدایش جرایم کامپیوتری شکی نماند که تمامی مباحث حقوق جزا از جمله حقوق جزای ماهوی-شکلی و بین الملل دچار چالش شده و بایستی همانند فضای فیزیکی-فضای سایبر نیز از نظر جزایی قاعده‌مند شود. از این رو کوشش هایی توسط او ای سی دی، شورای اروپا و سازمان ملل در سطح جهانی و کشورها در سطح منطقه‌ای و محلی صورت گرفت. از جمله متون منتشره که بیانگر این کوشش ها است نشریه سیاست جنایی سازمان ملل در زمینه جرایم کامپیوتری است.

یکی از متون منتشره شورای اروپا نیز حاوی لیست و توضیح چالش ها برای آیین دادرسی و . . . است.

در سطح کشورها دادگستری آمریکا جهت آموزش قضات، ماموران اف بی آی و سایر علاقه مندان اقدام به ارائه متن تفتیش و توقیف کامپیوترها و . . . کرد. این متن در طول چند سال اخیر چند بار اصلاح شده و نسخه ۲۰۰۲ آن که روی سایت قرار گرفته نسخه جدید آن محسوب می شود. این کتاب برای دانشجویان حقوق، علوم انتظامی، کارآموزان قضایی و کارآموزان وکالت و نیز کسانی که به صورت حرفه‌ای به جرایم کامپیوتری می پردازند یا با پرونده های مرتبط با آن سر و کار دارند، متن مفید و سودمندی است.

حتی از این متن به عنوان دو واحد درسی در کنار دو واحد درس کشف علمی جرایم در دوره های کارشناسی و کارشناسی ارشد می توان در بحث کشف علمی جرایم کامپیوتری استفاده کرد.

در این کتاب پس از یک مقدمه، مباحث تفتیش و توقیف کامپیوترها بدون حکم، تفتیش و توقیف کامپیوترها با حکم، قانون حریم خصوصی ارتباطات الکترونیک، نظارت (دیده بانی) الکترونیک در شبکه های ارتباطی، ادله و ضمایم توضیح داده شده است.

تفتیش و توقیف کامپیوترها بدون حکم شامل دلیل نقض حریم خصوصی، استثنائات الزام به وجود حکم (رضایت شرایط اضطراری)، تفتیش ویژه محل کار (بخش عمومی / بخش خصوصی) و . . . است. تفتیش و توقیف کامپیوترها با حکم شامل برنامه ریزی و طراحی تفتیش (استراتژی مبنا و پایه اجرای تفتیش کامپیوتر، قانون حمایت از حریم خصوصی. اسناد ممتازه و . . .)، پیش بینی حکم و مسائل قبل از توقیف است.

در قانون حریم خصوصی ارتباطات الکترونیک

بر عکس حقوق جزا که در مواجهه با تکنولوژی اطلاعات دچار تنش صددرصد شده مباحثی مانند جرم‌شناسی، بزه‌دیده‌شناسی، روان‌شناسی جنایی و جامعه‌شناسی جنایی سایبری با تنش کمتری مواجه شده است

به تهیه کنندگان خدمات ارتباط الکترونیکی از جمله خدمات راه دور، تقسیم بندی انواع اطلاعات نگه‌داری شده توسط تهیه کنندگان خدمات، افشای اجباری و افشای اختیاری و . . . پرداخته شده است. در مباحث نظارت الکترونیک و ادله نیز مطالب سودمندی ذکر شده است. برای دیدن متن و استفاده از آن به آدرس زیر مراجعه نمایید:

www.cybercrime.gov

پیشنهاد ۲ واحد درس جرم‌شناسی جرایم سایبری:

معرفی ماخذ:

social learning theory and A moral disengagement analysis of criminal computer behavior, an explaratory study

By: Marcus. Rogers

در اثر پیدایش و تکامل جرایم سایبری یکی از شاخه ها یا رشته های مهم در این دکترین سایبری، یعنی جرم‌شناسی واجد یا درگیر مباحث جدیدی شده است. بر عکس حقوق جزا که در مواجهه با تکنولوژی اطلاعات دچار تنش صددرصد شده مباحثی مانند جرم‌شناسی مجرمان سایبری، بزه‌دیده‌شناسی سایبری، روان‌شناسی جنایی سایبری و جامعه شناسی جنایی سایبری با تنش کمتری مواجه شده و فقط برخی مباحث آن تغییر کرده است. برای مثال در جرم‌شناسی سایبری صحبت از خرده فرهنگ هکری، علل ارتکاب جرایم سایبری، تطبیق تئوری ها و نظریه های جرم‌شناسی با رفتارهای جدید غیر قانونی یا منحرفانه در فضای سایبر است. رشته ها یا شاخه هایی نیز مانند سیاست جنایی جرایم سایبری، پیشگیری جرایم سایبری و کشف علمی جرایم سایبری به مانند حقوق جزا با تنش کامل مواجه شده‌اند. بحث این کتاب ها ناظر به آنالیز مجرمین کامپیوتری بر اساس تئوری یادگیری اجتماعی است.

تئوری یادگیری اجتماعی منشعب از تئوری معاشرت های ترجیحی ساترلند است. در این تز در بخش مقدمه بحث قانون‌گذاری، بررسی اصطلاح هکر، تئوری یادگیری اجتماعی و به تبع آن تئوری معاشرت های ترجیحی ذکر شده است. با ارائه برخی توضیحات و تعاریف، مولف در سه فاز مطالعه خود را انجام داده است. آن گاه مولف و محقق هیپوتز خود را که حاصل گذر از سه مرحله و تلفیق یافته ها و تئوری ها است، ارائه کرده است.

متد تحقیق نامبرده بر اساس مصاحبه ها، پرسشنامه ها، سنجش منطقی و مهارتی و . . . است. در کنار بررسی مجرمان عمومی و عادی. مجرمان اینترنتی بررسی و نتیجه این بررسی تجزیه و تحلیل شده است. مولف سپس جزئیات و مباحث ریز و جزئی موجود در تئوری یادگیری اجتماعی را در کنار آنالیز رفتار مجرمان کامپیوتری به چالش کشیده است. در بخش ضمایم نیز برخی مستندات و ابزارهای کار مؤلف ارائه شده است.

برای ملاحظه متن فوق می توان به آدرس زیر مراجعه نمود:

www.cerias.purdue.edu/homes/mkr/cybercrime-thesis.pdf