I Crimini Informatici

Sapevate che partendo da una email di spamming si può arrivare all'indirizzo di chi l'ha spedita? Che si può rintracciare il destinatario di una email anonima? Sapevate poi che, anche cambiando data a un file, in realtà, la data "vera" della sua creazione rimane impressa e può essere rilevata? O che una chat rimane quasi sempre nella memoria di un computer? O che si può risalire all'autore di un virus? Che esistono delle "impronte digitali" anche in un disco fisso e che possono essere rivelate? Ma, soprattutto, sapevate che analisi di questo tipo possono essere effettuate anche da chi è a digiuno dell'argomento, attraverso programmi piuttosto semplici da utilizzare o, meglio ancora, attraverso veri e propri "tool" utilizzati dalla Polizia informatica? Questo libro è un viaggio che spiega in modo semplice e un po' romanzato, ma molto focalizzato sull'aspetto pratico, gli strumenti e le tecniche per fare indagini informatiche in modo facile facile. Perché la computer forensic è utile, anche al "semplice cittadino".

Dei quindici anni più caldi mai avvertiti sul nostro pianeta quattordici si sono registrati nel xxi secolo. L'inquinamento da carbonio ha portato i gas serra ai picchi più alti dalla fine del Cretaceo. Una crisi finanziaria globale ha lasciato senza parole i cervelli meglio pagati al mondo. E ancora l'11 settembre, gli attacchi terroristici da Montreal a Manchester, la Brexit, i collassi nucleari, gli tsunami e gli uragani: di ragioni per pensare che tutto stia crollando ce ne sono parecchie. Eppure Ian Goldin e Chris Kutarna sono sicuri: questa è la Nuova età dell'oro. Proprio come nel Rinascimento, nella nostra epoca c'è un terreno estremamente fertile per la fioritura del genio, perché in nessun altro momento storico il rapporto tra scienza e tecnologia è stato così stretto. Vincere le sfide del presente e superare lo shock continuo prodotto dalla collisione tra realtà e aspettative significa allora strutturare una strategia che, presupponendo il fattore rischio come elemento imprescindibile della natura del genio, attinga al passato per dirigere il presente e orientare il futuro. Goldin e Kutarna ripercorrono quindi la storia delle scoperte geografiche, delle rivoluzioni scientifiche e artistiche che hanno caratterizzato l'età moderna e le confrontano con l'attualità: come Gutenberg e la stampa, Zuckerberg e i social media contribuiscono a diffondere la conoscenza; il crollo del muro di Berlino e la globalizzazione hanno abbattuto barriere e consentito di varcare confini prima invalicabili in misura pari alla scoperta di Cristoforo Colombo; i flussi migratori di oggi, spesso determinati da movimenti geopolitici radicati nella religione, ricordano quelli provocati in Europa dalla scissione tra Chiesa cattolica e Chiesa riformata. Se è vero che il presente non è una ripetizione di quanto già accaduto, è pur vero che l'umanità non si reinventa a ogni generazione e che, a dirla con Machiavelli, per prevedere il futuro bisogna consultare il passato. Nuova età dell'oro è lo strumento necessario per conquistare una visuale più ampia, calibrare speranza e determinazione, promuovere un progresso finalmente sostenibile. Perché è tempo che economia e cultura entrino in un secondo Rinascimento.

262.23

L'ex hacker Kevin Poulsen si è costruito negli ultimi dieci anni una reputazione invidiabile come uno dei massimi giornalisti investigativi nel campo della criminalità digitale. In Kingpin riversa per la prima volta in forma di libro una conoscenza e un'esperienza diretta impareggiabili, consegnandoci la storia avvincente di un gioco del gatto col topo e una panoramica senza precedenti del nuovo e inquietante crimine organizzato del ventunesimo secolo. Nell'underground dell'hacking la voce si era diffusa come un nuovo virus inarrestabile: qualcuno – un cyber-ladro brillante e temerario – aveva appena scatenato il takedown di una rete criminale online che sottraeva miliardi di dollari all'economia statunitense. L'FBI si affrettò a lanciare un'ambiziosa operazione sotto copertura per scoprire questo nuovo boss del crimine

digitale; altre agenzie di tutto il mondo dispiegarono decine di talpe e agenti sotto copertura. Collaborando, i cyber-poliziotti fecero cadere nelle loro trappole numerosi hacker sprovveduti. La loro vera preda, però, mostrava sempre una capacità straordinaria di fiutare i loro informatori e cogliere le loro trame. Il bersaglio che cercavano era il più improbabile dei criminali: un brillante programmatore con un'etica hippie e la doppia identità di un supercattivo. Importante hacker "white hat", Max "Vision" Butler era una celebrità nel mondo della programmazione e in passato aveva addirittura collaborato con l'FBI. Ma nei panni di un "black hat", come "Iceman", trovava nel mondo del furto dei dati un'opportunità irresistibile di mettere alla prova le sue enormi capacità. Penetrò in migliaia di computer di tutti gli Stati Uniti, rubando a suo piacimento milioni di numeri di carte di credito.

Alanna Blake è un'adolescente in fuga che abbina ingegno a un gruppo di hacker estremisti in ANTIAMERICA. Disponibile in ebook, audiolibro e libro in brossura. L'AntiAmerica è al centro della più grande rivolta anarchica americana degli ultimi 100 anni. Quando il gruppo di hacktivisti AntiAmerica attacca le più grandi banche della nazione, il settore finanziario rimane in bilico sull'orlo del collasso. Il pirata informatico e adolescente in fuga Alanna Blake viene reclutata con forza dal governo per rintracciare l'unico collegamento con l'AntiAmerica, il suo ex fidanzato scomparso Javier. Si affida alla proprie abilità di ingegneria sociale per districarsi in una cospirazione di menzogne e inganni che mette in pericolo sia la vita di tutte le persone più vicine a lei sia i segreti di un passato che desidera rimanga segreto per sempre.

PUBLISHER: TEKTIME

Sicurezza informatica Leggi internazionali sui crimini informatici Proposta di progetto di ricerca di dottorato e / o dottorato di ricerca

A partire dagli anni novanta, l'avvento di internet ha suscitato l'incremento di nuove tipologie di reati commessi mediante strumenti informatici. I criminali virtuali, tramite il web, possono mettere in atto attacchi informatici, truffe e frodi telematiche, hacking, spionaggio informatico, produzioni di virus, cyberstalking, spamming, malware, net-strike, pirateria satellitare e far proliferare la pedofilia online. Questi sono solo alcuni dei crimini informatici che possono avvenire per mezzo di internet. Maggiori sono i pericoli riguardanti la "fascia debole" caratterizzata dai minori. Bambini e adolescenti più volte hanno dimostrato di essere inconsapevoli dei pericoli in cui si possono imbattere attraverso l'utilizzo della rete, in modo particolare mediante l'uso di chat o social network. I giovani di oggi sono definiti nativi digitali, nascono e crescono accompagnati dalle tecnologie. Alcuni di loro vivono il web come un mondo virtuale parallelo a quello reale. Il problema sussiste nel momento in cui i minori usano internet senza cautele, allo sbaraglio. La curiosità, la troppa libertà e la noia, sono elementi che delineano e penalizzano i bambini e gli adolescenti che, molto spesso, non sanno che la rete oltre ad avere finalità positive, nasconde insidie e persone malintenzionate. Il presente ebook illustra i pericoli che il web porta con se, partendo da una definizione generale di pedofilia e giungendo alle varie forme tramite le quali si manifesta. Esamina il tema dei pedofili, come siano divenuti cyberpedofili e come la cyberpedofilia sia strettamente

legata al mercato della pedopornografia online. Analizza l’adescamento dei minori nelle chat, approfondendo le sue fasi e le conseguenze che ne derivano; si è, metaforicamente, entranti nel mondo virtuale dei pedofili online per analizzare le dinamiche che lo caratterizzano. E’ stato illustrato ed esplicato il progredimento di un incontro offline e approfondito il nesso tra i minori e internet. Un mondo sommerso che ha basi solide e malate, un commercio che frutta milioni e milioni e che è divenuto un business vero e proprio. Chi si occupa di contrastare questo mercato? In che modo? Come viene fatta arrivare l'informazione preventiva ai minori? C'è in Italia una Legge che regola l'utilizzo del pc e della rete in modo sano e che punisce il crimine informatico? Tale testo tenta di esaurire le risposte a queste domande attraverso interviste alla Polizia Postale e delle Comunicazioni e mediante dati di analisi statistiche. Il libro segue un percorso che si districa tra “muri” giudiziari dando uno sguardo sociologico e psicologico ad una società “sconvolta”, coinvolta e spesso complice nell'utilizzo errato della e nella rete.

I crimini informaticilibreriauniversitaria.it EdizioniI crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioniHALLEY EditriceI crimini informatici. Storia, tecniche e difeseI crimini informatici, il dark web e web roomSicurezza informatica Leggi internazionali sui crimini informatici Proposta di progetto di ricerca di dottorato e / o dottorato di ricercaHumayun Bakht

PARTE I - PIRATERIA E SICUREZZA NEI MARI Il contrasto alla pirateria marittima: l`impegno delle istituzioni comunitarie e internazionali, di A. Tajani. Briganti e avventurieri: incursioni nei mari degli antichi, di C. Petrocelli. Roma e la pirateria, di S. Tafaro. La pirateria nella storia del Mezzogiorno, di F. Mastroberti. Operazione antipirateria dell`Unione Europea ATALANTA, di G. Guimero. Periodo di guida italiana della Forza marittima - EUNAVFOR - in mare. La pirateria marittima: diritto consuetudinario, diritto convenzionale e norme nazionali, di U. Leanza. La pirateria nei mari: un`analisi geopolitica, di N. Carnimeo. L`azione delle organizzazione internazionale in materia di pirateria marittima, di A. Leandro. Note minime in tema di responsabilità civilistica del vettore marittimo nell`abbandono del carico per fatti di pirateria, di D. Caterino. Assicurazione marittima ed assicurabilità del rischio pirateria, di F. Moliterni. La pirateria quale evento esonerativo della responsabilità del vettore marittimo, di S. Prete. PARTE II - PIRATERIA E CONTRAFFAZIONE. Frode e contraffazione nel settore agroalimentare: aspetti merceologici, di P. Giuncato e B. Notarnicola. Agro-pirateria: analisi del problema e proposte di soluzioni nell'ottica della legislazione alimentare, di D. Pisanello. La contraffazione nella black economy, di C. Coco. La normativa a tutela della proprietà industriale, di C. Ciavarella PARTE III - LA PIRATERIA INFORMATICA. Pirateria informatica e rischio democratico, di G. Dammacco. Noterelle sulla pirateria informatica, di U. Patroni Griffi. La sistematica dei reati connessi alla pirateria informatica, di P. De Felice. La competenza giurisdizionale in materia di criminalità informatica transnazionale, di G. Pizzolante. Pirateria informatica e prospettive di tassazione della rete, di A. Uricchio. Le patologie dell`informazione: profili costituzionali, di F. Perchinunno. L`intermediario in internet: nuove frontiere e nuove responsabilità, di C. Sacchetto Pirateria informatica e open source, di O. Carrieri. PARTE IV - LA PIRATERIA AMBIENTALE. La \"pirateria ambientale\" da traffico illecito dei rifiuti: tecniche risarcitorie e sottosistemi normativi, di F. Parente. Problematiche ambientali e gestione dei rifiuti in ambito portuale, di A. Bonomo. Il traffico illegale dei rifiuti e l`intensificazione dei controlli

ambientali, di V. F. Uricchio. Profili penali del traffico dei rifiuti, di N. Selvaggi. Attività d`indagine sui rifiuti transfrontalieri, di N. Candido.
Alex è un giovane povero nella città di Mandala. Alex è in realtà un bravo ragazzo che è costantemente sotto la pressione dei problemi finanziari e dell'oppressione della gente di Mandala City. Alex è stato truffato molte volte da truffatori online. E apprende le tecniche di frode studiando la chat di persone che si ingannano e iniziano a praticarla sugli altri. La sua vita cambia in meglio come artista della truffa. Impara ad hackerare i sistemi informatici e con il suo duro lavoro commette hacking e altri crimini informatici. La sua vita si arricchisce con la sua nuova professione e riceve più sesso da varie donne della sua città. Le avventure di Alex da bravo ragazzo a criminale più ricercato della città sono piene di avventure sessuali di molte donne e crimini informatici che ha fatto tanto da essere soprannominato lo Squartatore.
L’opera, che vede la collaborazione di diversi studiosi e professionisti specializzati nel settore, approfondisce la complessa tematica del rapporto fra diritto e nuove tecnologie, privilegiando un approccio di carattere operativo anche se non viene risparmiato spazio ad importanti riferimenti di carattere dottrinario. Grande rilevanza assume la giurisprudenza, spesso decisiva per risolvere le particolari questioni giuridiche sorte con l’avvento della tecnologia. Il libro si suddivide in 4 macroaree: civile, penale, amministrativa e tecnologie emergenti, proprio per evidenziare l’evoluzione che negli ultimi tempi ha contraddistinto la materia, da intendere ormai come comprensiva sia dell’informatica del diritto, che del diritto dell’informatica e dove ormai lo stesso riferimento alla sola informatica appare limitato. Proprio per questo motivo si è ritenuto di affrontare le principali ed emergenti tematiche dell’informatica giuridica: la contrattualistica, la protezione dei dati personali, i reati, la cybersecurity, la digitalizzazione della PA, l’IA, l’IoT, la blockchain, i big data.
Il lavoro, di taglio manualistico, rappresenta una corretta e coerente trattazione di tutti gli aspetti criminologico-giuridici inquadrati in una parte generale-espositiva e 4 sezioni di parte speciale sino a trattare i singoli reati in chiave criminologica. Questa distinzione concettuale consente di operare un continuum, una progressione nell’apprendimento e nell’approfondimento della criminologia giuridica, mantenendo però una completa autonomia nella trattazione dei singoli argomenti affrontati. Il manuale ha un taglio scientifico ma anche pratico: una soluzione volutamente onnicomprensiva che l’autore ha ritenuto indispensabile per il criminologo giurista.
Il trattato approfondisce, in modo completo ed esaustivo, le principali questioni del diritto penale e processuale penale legate alle tecnologie informatiche. Ha una destinazione scientifica e professionale ed è suddiviso in 4 parti: - Parte I - DIRITTO PENALE SOSTANZIALE. Questioni e prospettive di fondo: una visione d'insieme sulla responsabilità penale dell’Internet Provider e degli enti per i reati informatici ex D.lgs. 231, sulle fonti internazionali ed europee e sulla validità nello spazio della legge penale. - Parte II - DIRITTO PENALE SOSTANZIALE. Tematiche di carattere specifico: ad esempio, Cyberterrorismo, istigazione a delinquere via Web, tutela dei minori e pedopornografia telematica, Cyberstalking, Cyberbullismo, tutela della libertà e della riservatezza della persona, falsità informatiche, furto di identità digitale, diffamazione via web, frodi informatiche e truffe on line, Cybericiclaggio, riservatezza e diritto alla Privacy, diritto d’autore, indebita utilizzazione di carte di credito. - Parte III - DIRITTO PENALE SOSTANZIALE. Le nuove frontiere: robotica, biorobotica, potenziamento cognitivo, profili penali dell'Internet of Things. - Parte IV - DIRITTO PROCESSUALE PENALE. Documento informatico, prove atipiche, Convenzione di Budapest, ispezioni, perquisizioni e sequestri di dati e sistemi, misure atte a garantire la ripetibilità dell'atto di indagine “informatica”, indagini di digital forensics, competenza della procura distrettuale, data retention, collaborazione internazionale tra autorità investigative e giudiziarie,

intercettazioni a mezzo del c.d. captatore informatico, il caso “Apple-F.B.I.”, indagini informatiche in relazione al cloud computing, indagini informatiche per i reati commessi a mezzo del deep web.

Informatica Generale

L’espressione white collar crimes, coniata dal criminologo americano Sutherland, si riferisce ai delitti perpetrati dalla “persona rispettabile, appartenente alla classe superiore, che commette un reato nel corso dell’attività professionale, violando la fiducia formalmente o implicitamente attribuitagli”. Ad oggi, la criminologia si rimanda ad essa per spiegare in chiave soggettivistica le più svariate forme di criminalità economica, che negli anni hanno assunto contorni incerti e ondivaghi. Si tratta, infatti, di un insieme di condotte illecite difficilmente inquadrabili, diramate su scala planetaria, attraverso prassi speculative sistemiche e manovre di massimazione dei profitti basate su processi di infiltrazione in attività imprenditoriali lecite. La criminalità di tipo economico si fonda su fatti delittuosi facilmente mimetizzabili e misconosciuti, che si celano sotto l’apparenza di transazioni o affari legali, o si perdono nella rete dei traffici aterritoriali e anonimi del cyber spazio. I white collar criminals agiscono sfruttando la posizione sociale e imprenditoriale ricoperta e tessendo rapporti con i centri politici o con l’associazionismo criminale organizzato, in vista di un’illecita implementazione degli utili e del perseguimento anticoncorrenziale degli obbiettivi prefissati. I mille volti della criminalità economica ricomprendono attività illegali di tipo eterogeneo: si va dai crimini informatici, agli occupational crimes, ai delitti compiuti dai vertici imprenditoriali. E ormai da tempo gli studi sulla cd. “delinquenza delle classi superiori” evidenziano le difficoltà di circoscrizione e repressione del fenomeno, incardinato in realtà organizzate, lecite e non, che si muovono agilmente sia a livello territoriale, che su scala mondiale, anche sulla base delle garanzie offerte dalla mediazione tecnologica. La perpetrazione di crimini all’interno delle strutture imprenditoriali ha inoltre fatto emergere l’idea di una colpa d’impresa, connessa all’assenza di idonei ed effettivi strumenti di autoregolamentazione in grado di prevenire comportamenti criminosi e contenere il pericolo di attività illecite compiute da soggetti comunque inseriti nel circuito aziendale. Di qui anche la necessità di adeguare l’impianto penalistico moderno alla nuova realtà criminale, attraverso l’elaborazione di tecniche di contenimento dei cd. corporate crimes, e l’opportunità di costituire appositi Compliance Programs per il controllo del potenziale criminogeno societario e l’esclusione di profili di colpa per comportamenti devianti tenuti da sottoposti o vertici imprenditoriali. La varietà di fenomenologie criminali coinvolte, ci ha indotti a un costante approfondimento criminologico delle questioni connesse alla delinquenza di tipo economico. In più occasioni ci siamo occupati di contesti criminali legati al circuito dell’economia. Il riferimento è alla corruzione sistemica imprenditoriale – che da anni domina indisturbata le strategie aziendali e i meccanismi di mercato – ai crimini informatici – ricondotti, pur nella loro eterogeneità, alla macro categoria dei white collar crimes – e alla cd. responsabilità d’impresa – condizionata all’elusione di idonei modelli di governance predisposti per la regolamentazione dell’attività aziendale e la conseguente prevenzione di focolai criminali al suo interno. E la trattazione nasce proprio dalla volontà di ricomporre in modo unitario i nostri studi sul tema, in modo da tracciare un quadro criminogenetico e criminodinamico più ampio, che consenta al lettore una consapevole maturazione delle principali tematiche criminologiche riconducibili al fenomeno della cd. delinquenza

economica.
Negli ultimi tempi la tecnologia ha compiuto progressi eccezionali in campo informatico. La diffusione capillare delle applicazioni web ha sviluppi sempre più rapidi in molteplici settori, ma tanto più saranno i dispositivi connessi al web tanto più la pirateria informatica troverà terreno fertile per scoprire e individuarne i punti deboli. L'autrice analizza le maggiori possibilità di truffe su Internet auspicando che l'avanzamento della tecnologia insieme ai sistemi di sicurezza "giochino d'anticipo" contrastando le truffe in tempo reale.
Sicurezza informatica . Crimini informatici per affari non etici Proposta di progetto di ricerca di dottorato e / o dottorato di ricerca
Un contributo aggiornato alla conoscenza dei profondi mutamenti normativi che hanno interessato, negli anni, la procedura penale, in funzione della sua applicazione sul campo delle indagini difensive e di quelle tecnico scientifiche.
Il mondo del web viene qui trattato in modo organico e completo. Dopo le fonti del diritto dell'informatica si entra nel vivo della rete del monitoraggio ai fini di giustizia e sicurezza. Poi: Cyberspazio, Tempo, Diritto di accesso, diritti e doveri nell'uso di Internet, i beni e loro tutela, soggetti, responsabilit DEGREES, tutela della persona, regolamentazione, libert DEGREES e censura nella Rete. Spazio agli aspetti penali con i crimini informatici. Spazio ad una parte tecnica sui bit coin, ransomware, modalit DEGREES di riscatto per la decriptatio e le macchine infettate, i big data e la captazione. Sotto il profilo della comunicazione vengono trattati il terrorismo, le perquisizioni informatiche, la comunicazione in Rete, il commercio elettronico, la contrattazione informatica, telematica e virtuale e il controllo internazionale sull'esportazione di software per intrusioni. Infine privacy e tutela dati personali, diritto all'oblio, giochi on line, telelavoro, PA Digitale e documento informatico, firme elettro