Adriana Iuliana STANCU

NOI TENDINȚE ÎN CRIMINALITATEA CIBERNETICĂ – TERORISM CIBERNETIC

PRO UNIVERSITARIA 2024 BUCUREȘTI

Universul Juridic
București
2024

CUPRINS

Capitolul 1

TEHNOLOGIE ȘI CRIMINALITATE CIBERNETICĂ

1.1. Introducere

Internetul, computerele și tehnologiile mobile au remodelat dramatic societatea modernului. În urmă cu trei decenii, majoritatea indivizilor nu dețineau un telefon mobil, oamenii nu trimiteau mesaje, e-mailurile erau neobișnuite, iar computerele personale erau încă echipamente oarecum scumpe. Conectivitatea la internet a avut loc în general prin modemuri dial-up lente în care persoanele plăteau pentru accesul la internet pe oră. Sistemele de jocuri video foloseau grafică pe 16 biți și nu se conectau la alte dispozitive pentru a permite jocurilor să fie o activitate comună. Indivizii citeau cărți și ziare mai degrabă decât e-readere. Dacă foloseai sisteme de poziționare globală (GPS), probabil că nu conduceai vehiculul personal, ci mai degrabă operai un sistem militar. Astăzi, cea mai mare parte a lumii depinde de computere, internet și tehnologia celulară. Indivizii dețin acum laptopuri care sunt conectate prin Wi-Fi, smartphone-uri și unul sau mai multe sisteme de jocuri video care pot fi conectate în rețea. Telefoanele mobile au devenit o metodă preferată de comunicare pentru majoritatea oamenilor, în special mesajele text. În plus, oamenii au mai multe conturi de e-mail și profiluri de rețele sociale pe mai multe platforme atât pentru uz personal, cât și pentru afaceri. Este uimitor că lumea și comportamentul uman s-au schimbat atât de repede prin utilizarea tehnologiei. De fapt, există acum 4,57 miliarde de utilizatori de internet în întreaga lume, reprezentând 58,7% din populația lumii (Internet World Stats, 2020). Națiunile asiatice cuprind jumătate din utilizatorii Inter-net din lume, deși doar 53,6% din populația lor totală are acces online susținut (Internet World Stats, 2020). În schimb, națiunile nord-americane cuprind doar 7,6% din populația mondială de utilizatori de internet, deși 94,6% din populația lor totală are acces (Internet World Stats, 2020).

1.2. Importanța tehnologiei în societatea modernă

Proliferarea tehnologiei a dus la schimbări distincte în modul în care indivizii interacționează cu lumea din jurul lor. Oamenii fac acum cumpărături,

comunică și împărtășesc informații în formate digitale, ceea ce înainte era imposibil. Schimbările suplimentare de comportament vor continua probabil în fața inovațiilor tehnologice pe măsură ce acestea sunt dezvoltate și implementate. De fapt, sociologul Howard Odum s-a referit la acest proces de schimbare a comportamentului ca răspuns la inovația tehnologică (Odum, 1937; Parker, 1943; Vance, 1972). Din perspectiva lui Odum, căile tehnice înlocuiesc modelele de comportament existente și forțează schimbări instituționale în societate (Vance, 1972). De exemplu, dacă o persoană în urmă cu 30 de ani dorea să comunice cu alte persoane, putea să le sune, să le vadă personal dacă era posibil sau să trimită o scrisoare prin poștă. Acum, însă, acea persoană trimitea un mesaj text, scrie un e-mail sau trimite un mesaj direct pe rețelele de socializare, în loc să vorbească la telefon sau să trimită o scrisoare prin „poștă". Impactul căilor tehnice este evident în toate grupurile demografice din societatea modernă. De exemplu, 81% dintre americani dețin un smartphone începând cu 2019, cu acces majoritar în rândul populațiilor mai tinere: 96% dintre tinerii cu vârste cuprinse între 18 și 29 de ani au unul (Pew Research Center, 2019). Prin comparație, dovezile sugerează că 59,9% din populația Chinei și doar 25,3% din India au smartphone-uri (Newzoo, 2020). Pe măsură ce aceste rate continuă să crească, utilizarea internetului se va schimba și va avea un impact direct asupra vieții sociale și economice a indivizilor din fiecare țară și din toate regiunile lumii. Acest lucru este evident în faptul că mulți oameni din întreaga lume folosesc rețelele sociale ca mijloc de a se conecta și de a interacționa cu ceilalți în moduri diferite. De exemplu, 69% dintre adulții americani folosesc Facebook, deși a existat o creștere substanțială a utilizării Instagram și Linkedln ca mijloc de comunicare (Perrin și Anderson, 2019). În schimb, WhatsApp este mult mai popular într-un context global și este aplicația de mesagerie numărul unu în mare parte din America, Europa de Vest, Africa și unele părți ale Asiei (Iqbal, 2020). Alte servicii, cum ar fi QQ, au o populație de utilizatori mult mai specifică regiunii (Bucher, 2020). În ciuda variațiilor regionale de utilizare, tehnologia a avut un impact masiv asupra populațiilor tinere care nu au experimentat niciodată viața fără internet și comunicații (CIC), cum ar fi e-mailul și mesajele text. Astăzi, tinerii din Statele Unite își achiziționează primele telefoane mobile la aproximativ 11 ani, 20% dintre ei au unul până la vârsta de 8 ani (Robb, 2019). Modele de utilizare similare sunt evidente pe tot globul, copiii din Germania primind un telefon între 6 și 13 ani, în timp ce copiii din Coreea de Sud îl obțin chiar mai devreme.

Tehnologia nu a schimbat doar comportamentele tinerilor, ci le-a modelat comportamentul și viziunea asupra lumii încă de la început. Majoritatea oamenilor de la mijlocul anilor 1980 nu au trăit niciodată fără computere, internet sau telefoane mobile. În consecință, ei nu cunosc o lume fără aceste dispozitive și cum ar fi viața fără aceste resurse. Astfel, Prensky (2001) a susținut că acești tineri sunt nativi digitali, în sensul că au fost aduși într-o lume care era deja digitală, petrec mult timp în medii digitale și folosesc resurse tehnologice în viața lor de zi cu zi. De exemplu, aproape toată lumea (96%) cu vârste cuprinse între 16 și 34 de ani din Marea Britanie accesează internetul de pe un dispozitiv mobil (Office for National Statistics, 2018). Persoanele cu vârste cuprinse între 18 și 24 de ani din Statele Unite folosesc, de asemenea, aplicații de mesagerie unice la rate mult mai mari decât grupurile mai în vârstă, deoarece 73% folosesc Snapchat și 75% folosesc Instagram (Perrin și Anderson, 2019). În mod similar, 55% dintre toți bărbații indieni cu vârste cuprinse între 18 și 34 de ani folosesc WhatsApp aproape în fiecare zi (Steup, 2018). În schimb, imigranții digitali sunt cei care s-au născut înainte de crearea internetului și a tehnologiilor digitale (Prensky, 2001). Acești indivizi trebuie să se adapteze destul de des la mediul digital, care se schimbă mult mai repede decât ar fi pregătiți altfel. Acest lucru este valabil mai ales pentru multe persoane în vârstă care s-au născut cu zeci de ani înainte de crearea și apariția acestor tehnologii. În consecință, ei pot fi mai puțin dispuși să adopte imediat aceste resurse sau să le utilizeze în diverse moduri. De exemplu, unele resurse pot fi mai greu de înțeles pentru imigranții digitali din cauza tehnologiilor utilizate sau a utilității lor percepute. De exemplu, doar 31% dintre adulții americani cu vârsta de 50 de ani și peste au fost susceptibili să folosească o aplicație precum Instagram, iar 12% au folosit Snapchat (Perrin și Anderson, 2019). În mod similar, doar 28% dintre persoanele cu vârsta de 65 de ani și peste din Marea Britanie au folosit internetul pe un dispozitiv mobil (Office for National Statistics, 2018). Astfel, imigranții digitali au un model mult diferit de adoptare și utilizare a tehnologiilor în comparație cu nativii digitali. Proliferarea tehnologiei în societatea modernă a avut un impact masiv asupra comportamentului uman. Lumea este restructurată în jurul utilizării CIC (comunicarea prin intermediul calculatorului), afectând modul în care interacționăm cu guvernele, companiile și unii cu alții. În plus, utilizarea tehnologiei creează o diviziune între generații bazată pe modul în care indivizii folosesc tehnologia în viața lor de zi cu zi. În același timp în care tehnologia modifică modul în care ne trăim viața de zi cu zi, indivizii adaptează diverse

tehnologii, cum ar fi computerele și internetul, pentru a submina proiectele și aplicațiile lor benefice originale pentru a comite forme modificate și noi de infracțiuni.

Evoluția continuă a comportamentului uman ca urmare a inovațiilor tehnologice a creat oportunități de neegalat pentru infracțiuni și abuzuri. În ultimele trei decenii, a existat o creștere substanțială a utilizării tehnologiei de către infractorii de stradă și noi aplicații ale tehnologiei pentru a crea noi forme de criminalitate care nu existau anterior. World Wide Web și Internetul oferă, de asemenea, un loc pentru persoanele care se săvârșesc infracțiuni și contravenții pentru a comunica și a împărtăși informații, fapt care nu este posibil în lumea reală. Ca urmare, este vital să începem să înțelegem cum au loc aceste schimbări și ce înseamnă pentru infracționalitate în secolul XXI. Există trei modalități cheie prin care tehnologiile informatice și celulare pot fi abuzate sau subminate de infractori: 1 ca mediu de comunicare și dezvoltare a subculturilor online; 2 ca mecanism de direcționare a resurselor sensibile și de implicare în infracțiuni și contravenții și 3 ca dispozitiv adiacent pentru a facilita infracțiunea și a furniza dovezi ale activității infracționale atât online, cât și offline.

Diverse forme de tehnologie, cum ar fi telefonia (adesea văzută ca tehnologie care permite comunicarea vocală pe distanțe lungi), internetul și mass-media digitală, pot fi folosite ca mijloc pentru ca indivizii să comunice într-un mod rapid și descentralizat pe tot globul. Calculatoarele, telefoanele mobile și echipamentele tehnologice pot fi obținute la costuri minime și utilizate cu un grad ridicat de anonimat. La rândul lor, infractorii pot folosi aceste dispozitive pentru a se conecta cu alții și pentru a partaja informații care ar putea fi de interes. De exemplu, clienții prostituatelor folosesc forumuri web și camere de chat pentru a discuta unde se află prestatorii sexuali, serviciile furnizate, prețurile și prezența poliției într-o anumită zonă (Holt & Blevins, 2007; Holt et al., 2008; Sharp și Earle, 2003). Acest schimb de informații de primă mână este dificil de efectuat în lumea reală, deoarece nu există semne exterioare care să sugereze că cineva este interesat sau a vizitat o prostituată. În plus, există un grad ridicat de stigmatizare socială și rușine în jurul plății pentru sex, așa că este puțin probabil ca cineva să recunoască acest comportament altei persoane în public (McKeganey și Barnard, 1996; O'Connell Davidson, 1998). Cu toate acestea, natura anonimă și fără chip a internetului permite oamenilor să vorbească despre astfel de acțiuni cu risc redus de prejudicii sau represalii. Vânzarea de narcotice ilicite, cum ar fi cocaina, marijuana și metamfetaminele, s-a mutat, de asemenea,

online prin dezvoltarea piețelor, cum ar fi faimosul Drum al Mătăsii, unde indivizii cumpără și vând narcotice prin diferite metode. Resursa principală folosită de vânzători și cumpărători sunt forumurile care operează pe așa-numitul Dark Web, care este o porțiune a internetului care poate fi accesată numai prin utilizarea unui software specializat de criptare și protocoale de browser. Persoanele fizice pot accesa aceste forumuri numai prin utilizarea serviciului „The Onion Router" sau TOR, care este un proxy gratuit și un protocol de criptare care ascunde adresa IP și detaliile locației utilizatorului (Barratt et al., 2014; Dolliver, 2015). În plus, conținutul acestor site-uri nu poate fi indexat de Google sau alte motoare de căutare. Această tehnologie limitează capacitatea agențiilor de aplicare a legii de a elimina conținutul ilicit, deoarece sursa de găzduire nu poate fi identificată prin mijloace tradiționale (Dolliver, 2015). Natura distribuită a internetului și a CIC-urilor permite indivizilor să se conecteze cu alte persoane și grupuri care împărtășesc aprecieri, antipatii, comportamente, opinii și valori similare. Ca urmare, tehnologia facilitează crearea de subculturi între indivizi bazate pe comportamente și idealuri comune, indiferent de izolarea geografică sau socială. Dintr-o perspectivă sociologică și criminologică, subculturile sunt grupuri care au propriile valori, norme, tradiții și ritualuri care le diferențiază de cultura dominantă (Brake, 1980; Kornblum, 1997). Participanții la subculturi își generează propriile coduri de conduită pentru a structura modurile în care interacționează cu alți membri ai subculturii și cu diferite grupuri din societate (Foster, 1990). În plus, apartenența la o subcultură influențează comportamentul individual prin furnizarea de credințe, obiective și valori care aprobă și justifică activitatea (Herbert, 1998). De exemplu, o subcultură poate pune accentul pe dezvoltarea abilităților și abilităților care pot avea mai puțină valoare în cultura generală. Membrii unei subculturi au, de asemenea, propriul lor jargon sau argou pentru a comunica cu ceilalți și pentru a-și proteja discuțiile de străini (Bilgrei, 2017; Holt et al., 2010a). Utilizarea acestui limbaj poate servi ca o demonstrație practică a apartenenței la orice subcultură. Astfel, subculturile oferă membrilor o modalitate de a-și evalua reputația, statutul și aderența la valorile și credințele grupului. Există nenumărate subculturi în societatea modernă, multe implicând atât experiențe online, cât și offline. Cu toate acestea, nu toate subculturile sunt deviante. Indivizii pot fi, de asemenea, membri ai mai multor subculturi simultan. De exemplu, s-ar putea să aparții unei subculturi a fanilor echipelor sportive (fie fotbal, baschet sau orice atletism) dacă (1) îți place să le urmărești meciurile, (2) cunoști statisticile jucătorilor tăi preferați, (3) cunoști evenimentele istorice din

sezoanele anterioare ale echipei tale și (4) dezbați cu alții despre cine ar putea fi cei mai buni jucători pe anumite poziții. Există subculturi similare pentru grădinărit, modă, mașini, filme și alte comportamente. Găsirea altora care vă împărtășesc interesele poate fi benefică, deoarece permite conectivitatea socială și o modalitate de a vă canaliza interesele în moduri pozitive. În același mod, subculturile pot apărea online și offline pentru cei interesați de anumite forme de criminalitate și deviație (Quinn & Forsyth, 2005). Tehnologia permite indivizilor să se conecteze cu ceilalți fără teama de represalii sau respingere socială și chiar permite persoanelor care sunt curioase despre comportament sau activitate să afle mai multe într-un mediu online fără teama de a fi detectate (Blevins și Holt, 2009; Deshotels și Forsyth, 2020). Noile tehnologii permit, de asemenea, formarea și participarea la mai multe subculturi cu mai multă ușurință decât ar fi posibil offline. De fapt, indivizii pot comunica cu ușurință cunoștințe subculturale prin e-mail și alte CIC-uri, cum ar fi tehnicile de infracțiuni care pot reduce riscul de detectare de către victime și forțele de ordine (Aldridge & Askew, 2017; Souleymanov et al., 2021). Datorită importanței tehnologiei ca mijloc de comunicare cu ceilalți, această carte se va concentra pe rolul subculturilor online de a facilita criminalitatea și devianța în mediile virtuale și din lumea reală.

1.3. Tehnologia ca țintă sau mijloc de a se angaja în infracțiuni

Al doilea mod în care tehnologia poate fi folosită în mod abuziv este mult mai insidios – ca o resursă pentru ca indivizii să atace și să provoace daune indivizilor, companiilor și guvernelor atât online, cât și offline. Multe dispozitive din viața noastră de zi cu zi au capacitatea de a se conecta la Internet, de la televizoare la computere desktop, sisteme de jocuri video, termostate și sisteme de securitate. Aceste tehnologii conțin informații sensibile, de la obiceiurile noastre de cumpărături la nume de utilizator și parole pentru conturile bancare și de e-mail. Deoarece aceste dispozitive pot comunica între ele, persoanele pot obține acces la aceste informații prin diferite metode de hacking informatic.

În timp ce hacking-ul este adesea considerat a implica persoane cu înaltă calificare cu o înțelegere semnificativă a tehnologiei, simplul act de a ghici e-mailul sau parola computerului cuiva ar putea fi definit ca un hack (Bossier & Burruss, 2011; Skinner și Fream, 1997). De fapt, cercetările asupra studenților sugerează că între 10 și 25% dintre studenți au încercat să ghicească parola altcuiva (Holt et al., 2010c; Rogers et al., 2006; vezi și Donner, 2016). Obținerea accesului neautorizat la informații personale online este adesea cheia definițiilor

hacking-ului, deoarece o persoană încearcă să intre în sisteme sau date protejate (vezi Schell & Dodge, 2002; Steinmetz, 2015; Wall, 2001). La rândul lor, ei pot folosi informațiile obținute pentru a se angaja în diferite forme de fraudă sau furt în spații online și offline. În mod similar, unii hackeri vizează site-uri web și resurse pentru a provoca daune sau pentru a exprima un mesaj politic sau ideologic. Adesea, comunitatea de hackeri și activiști folosește desfigurarea web pentru a răspândi un mesaj și a provoca daune în același timp (Holt et al., 2017; Howell et al., 2019). Desfigurările web sunt un act de vandalism online în care o persoană înlocuiește codul HTML existent pentru o pagină web cu o imagine și un mesaj pe care le creează. De exemplu, o persoană ar putea încerca să desfigureze site-ul Casei Albe (www.whitehouse) și să înlocuiască conținutul cu un mesaj pe care vrea să-l vadă alții. Deși acest lucru este un inconvenient și o rușine pentru proprietarul site-ului, poate fi mai rău intenționat dacă defacerul alege să șteargă complet conținutul original. Defacementele au devenit un instrument obișnuit pentru hackerii și actorii motivați politic pentru a-și exprima opiniile și au fost folosite în jurul multor evenimente sociale fierbinți. De exemplu, comunitatea de hackeri turci a început o campanie pe scară largă de desfigurări ale web-ului după publicarea unei caricaturi cu o imagine a profetului Mahomed cu o bombă în turban (Holt, 2009; Ward, 2006). Mulți musulmani au fost profund ofensați de această imagine, iar hackerii turci au început să desfigureze site-urile deținute de ziarul danez care a publicat caricatura, împreună cu orice alt site care a repostat imaginea. Desfigurările au fost efectuate în sprijinul religiei islamice și pentru a-și exprima indignarea față de modul în care credința lor a fost portretizată în mass-media populară (Holt, 2009; Ward, 2006). Astfel, actorii motivați care doresc să facă rău sau să-și exprime opinia pot vedea diverse resurse online ca țintă.

Deoarece tehnologia poate fi folosită atât ca mediu de comunicații, cât și ca țintă pentru atacuri împotriva țintelor și infrastructurii digitale, este esențial să se delimiteze ceea ce constituie abuzul și utilizarea abuzivă a tehnologiei. De exemplu, termenul deviantă este folosit pentru a se referi la un comportament care poate să nu fie ilegal, deși este în afara normelor sau credințelor formale și informale ale culturii dominante. Există multe forme de deviantă, în funcție de normele sociale și de contextele sociale. De exemplu, trimiterea de mesaje text și utilizarea Facebook în timpul claselor, cinematografelor sau altor setări poate să nu fie ilegală, dar este perturbatoare și, în general, dezaprobată de profesori și administratori. Prin urmare, trimiterea de mesaje text și utilizarea Facebook ar

putea fi văzute ca fiind deviante în contextul anumitor situații și locații. Deoarece activitatea este generată de tehnologie, trebuie denumită deviație cibernetică. Un exemplu mai pertinent de devianță cibernetică este evident în crearea și utilizarea pornografiei. Internetul a făcut extrem de ușor pentru indivizi să vizualizeze imagini și videoclipuri pornografice, precum și să creeze aceste materiale prin utilizarea camerelor web, a camerelor de telefon mobil și a fotografiilor digitale. Este legal pentru oricine cu vârsta peste 18 ani fie să acceseze imagini pornografice, fie să joace în aceste filme și media. Dacă comunitatea mai largă împărtășește opinia că pornografia este greșită din punct de vedere moral, atunci vizionarea acestor materiale poate fi considerată deviantă în acea zonă. Prin urmare, nu este ilegal să te angajezi în această activitate; mai degrabă încalcă pur și simplu normele locale și sistemele de credințe, făcându-l un comportament deviant. Activitățile care încalcă legile legale codificate se schimbă de la a fi deviante la acte criminale. În contextul pornografiei, dacă o persoană are sub 18 ani în Statele Unite, nu are voie legal să creeze sau să vizualizeze imagini pornografice. Prin urmare, un astfel de act este considerat o infracțiune, deoarece implică sancțiuni legale. Legile penale din Statele Unite, atât la nivel de stat, cât și la nivel federal recunosc o varietate de infracțiuni în lumea reală. Cu toate acestea, adoptarea și utilizarea rapidă a tehnologiei pentru a facilita activitatea infracțională a dus la crearea mai multor termeni pentru a clasifica corect aceste comportamente. Mai exact, criminalitatea cibernetică și criminalitatea informatică au apărut în urmă cu câteva decenii pentru a se referi la modul unic în care tehnologia este folosită pentru a facilita activitatea criminală. Criminalitatea cibernetică se referă la infracțiunile „în care făptașul folosește cunoștințe speciale despre spațiul cibernetic", în timp ce infracțiunile informatice au loc deoarece „făptuitorul folosește cunoștințe speciale despre tehnologia informatică" (Furnell, 2002, p. 21; Wall, 2001). În primele zile ale calculatoarelor, diferența dintre acești termeni a fost utilă pentru a clarifica modul în care tehnologia a fost încorporată în ofensivă. Faptul că aproape fiecare computer este acum conectat la Internet într-un fel sau altul a diminuat nevoia de a segmenta aceste două acte (Wall, 2007). În plus, au devenit aproape sinonime atât în cercurile academice, cât și în mass-media populară. Ca urmare, această carte va folosi termenul de „criminalitate cibernetică" din cauza gamei de infracțiuni care pot apărea prin utilizarea mediilor online și a numărului masiv de computere și dispozitive mobile care sunt conectate la Internet. Folosind exemplul pornografiei, este legal să produci și să accesezi acest conținut în

Statele Unite și în majoritatea celorlalte părți ale globului. Cu toate acestea, națiunile majoritar islamice, cum ar fi Iranul și Arabia Saudită, au interzis și au făcut ilegal accesul la pornografie din cauza credințelor lor religioase (Shishkina și Issaev, 2018). Alte țări, cum ar fi Suedia, impun restricții minime asupra producției de conținut pornografic, inclusiv imagini cu animale sau „bestialitate". Deși este ilegal să creezi sau să vizualizezi acest conținut în Statele Unite și în majoritatea celorlalte națiuni, indivizii pot accesa materiale pornografice bestiale, violente sau neobișnuite din întreaga lume, indiferent de legile națiunii lor, datorită conectivității oferite de Internet (Brenner, 2008; Wall, 2007). Astfel, este dificil să restricționezi sau să aplici legile locale privind comportamentul individual din cauza capacității de a accesa conținut la nivel global. Intersecția dintre criminalitatea cibernetică și devianța cibernetică este, de asemenea, legată de problema emergentă a terorismului cibernetic. Acest termen a apărut la mijlocul anilor 1990, când tehnologia a început să joace un rol din ce în ce mai important în toate aspectele societății (Britz, 2010; Denning, 2001). Nu există o definiție unică acceptată pentru terorismul cibernetic, deși mulți recunosc acest comportament ca fiind utilizarea tehnologiei digitale sau a CIC-urilor pentru a provoca daune și a forța schimbări sociale bazate pe convingeri ideologice sau politice (Brenner, 2008; Britz, 2010). Atacurile cibernetice determinate de o agendă ideologică sau politică au fost observate în ultimele două decenii, cu indivizi care vizează informații sensibile, sisteme informatice și rețele din întreaga lume (Holt et al., 2021). Infractorii pot, de asemenea, să atace aceste ținte folosind tactici similare, ceea ce face dificilă separarea actelor de terorism cibernetic de criminalitatea cibernetică (Brenner, 2008; Holt et al., 2021).

Pentru a clasifica mai precis aceste fenomene online, este necesar să se ia în considerare atât motivul atacatorului, cât și amploarea vătămării cauzate. De exemplu, actele criminale vizează adesea persoane individuale și pot fi motivate de obiective economice sau de altă natură, în timp ce atacurile teroriste sunt adesea determinate de un motiv politic și sunt concepute nu numai pentru a răni sau ucide nevinovați, ci și pentru a stârni frică în populația mai largă (Britz, 2010; Jarvis și Macdonald, 2015). Nu este întotdeauna posibil să se identifice în mod clar natura anumitor acte ca fiind deviante, criminale sau teroriste doar pe baza naturii evenimentului (Holt et al., 2021). Este nevoie de context suplimentar pentru a evalua motivația potențială a acțiunii, inclusiv ținta atacului și modul în care atacatorii își exprimă motivele incidentului. De exemplu, o încălcare a datelor care vizează o companie ar putea fi efectuată dintr-o motivație economică,

cum ar fi utilizarea datelor cardurilor de credit ale clienților pentru a se angaja în fraude. Cu toate acestea, poate fi de natură ideologică dacă ținta se încadrează în convingerile ideologice ale unui anumit grup extremist sau radical și postează comentarii publice pentru a sugera că a efectuat atacul pentru a dăuna sau a face de rușine compania (Britz, 2010; Jordan și Taylor, 2004). Astfel de hack-uri au fost raportate de grupuri de extremă stânga precum Animal Liberation Front încă de la mijlocul anilor 2000 și sunt exemple de criminalitate cibernetică efectuată în sprijinul unui sistem de credințe ideologice care poate fi considerat acte de terorism cibernetic (vezi Holt et al., 2021).

În plus, capacitatea de comunicare oferită de Internet creează o intersecție interesantă între devianța cibernetică și terorismul cibernetic. De exemplu, membrii grupurilor extremiste și de ură folosesc rețelele sociale și aplicațiile criptate pentru a se conecta cu alții din întreaga lume. De fapt, diverse grupuri extremiste de extremă dreapta depind acum de instrumente precum Telegram ca mijloc de comunicare în moduri mai ascunse, precum și de a-și promova agenda. Legile unei anumite țări pot să nu permită un astfel de limbaj, cum ar fi în Germania, unde este ilegal să postezi conținut legat de nazism (Shishkina & Issaev, 2018). În Statele Unite, totuși, un astfel de discurs este protejat de Primul Amendament al Constituției; Prin urmare, actul de a folosi forumurile online pentru a exprima o opinie în mare parte nesusținută de societate este un comportament deviant, mai degrabă decât ilegal.

1.4. Atractivitatea criminalității cibernetice și devianța

Creșterea devianței, a criminalității cibernetice și a terorismului cibernetic i-a determinat pe mulți să se întrebe de ce unii oameni aleg să se angajeze în nereguli în medii virtuale. Există mai mulți factori unici care pot explica infracțiunile online, inclusiv, dar fără a se limita la, disponibilitatea tehnologiei în lumea modernului, ușurința de a comite anumite forme de criminalitate cibernetică, tehnologia care acționează ca un multiplicator de forță, capacitatea de a reduce detectarea de către forțele de ordine prin anonimat online și provocările în extrădările internaționale. Fiecare dintre aceste probleme este discutată mai jos și pe tot parcursul manualului ca teme recurente. În primul rând, omniprezența tehnologiei facilitează accesul persoanelor la instrumentele necesare pentru a comite infracțiuni cu relativă ușurință. Prețurile computerelor au scăzut substanțial în ultimul deceniu, ceea ce face foarte ușoară achiziționarea unor astfel de echipamente. Computerele portabile mai mici, cum ar fi iPad-ul și