A gépi tanulással kapcsolatos kutatás jogi kockázatai

Ram Shankar Siva Kumar*, *Microsoft, ramk@microsoft.com*
Jonathon Penney*, *Citizen Lab, University of Toronto, jon@citizenlab.ca*
Bruce Schneier, *Harvard Kennedy School, schneier@schneier.com*
Kendra Albert, *Harvard Law School, kalbert@law.harvard.edu*

Bevezetés

Az ellenséges gépi tanulás annak szisztematikus tanulmányozása, hogy motivált támadók hogyan veszélyeztethetik a gépi tanuló (ML) rendszerek titkosságát, integritását és rendelkezésre állását célzott vagy általános támadások révén. Az ML-rendszerek támadásának problémája olyannyira elterjedt, hogy a CERT, a támadások tanulmányozásával megbízott, szövetségi finanszírozású kutatási és fejlesztési központ egy átfogó sebezhetőségi jegyzetet adott ki arról, hogy a legtöbb ML-osztályozó sebezhető a támadói manipulációval szemben.[1] A vállalatok és a kormányok odafigyelnek. A Google, az [2]IBM, a [3]Facebook [4]és a Microsoft elkötelezte magát amellett, hogy befektet a gépi tanulási rendszerek védelmébe.[5] Az Egyesült Államok a mesterséges intelligencia szabályozásának meghatározásakor a mesterséges intelligencia rendszerek biztonságát és védelmét helyezi elsődleges prioritásként, az EU [6]pedig a Trustworthy AI kezdeményezés részeként nem kötelező érvényű ellenőrző listák teljes sorát tette közzé.[7]

A kutatás ezen a területen fellendülőben van. Mivel több 2014,mint tanulmányt2,000 tettek közzé az arXiv.[8] A kutatók ellenséges ML-technikákat használtak a Facebook mikrocélzási hibáinak azonosítására.

---

[1] https://kb.cert.org/vuls/id/425163/ (megjegyezve: "A gradiens süllyedésen keresztül képzett gépi tanulási osztályozók sérülékenyek a tetszőleges félresorolásos támadásra").
[2] https://ai.google/responsibilities/responsible-ai-practices/?category=security ("A biztonság és védelem magában foglalja annak biztosítását, hogy a mesterséges intelligencia rendszerek a szándékolt módon viselkedjenek, függetlenül attól, hogy a támadók hogyan próbálnak beavatkozni. ")
[3] https://www.ibm.com/cloud/architecture/architectures/securityArchitecture/watson-security
[4]https://spectrum.ieee.org/tech-talk/artificial-intelligence/machine-learning/facebook-ai-launches-its-deepfake-észlelési kihívás ("...a Facebook AI Red Team, amely elemzi az AI által a közösségi médiaóriás számára jelentett veszélyeket")
[5] https://docs.microsoft.com/en-us/security/engineering/securing-artificial-intelligence-machine-learning (megjegyezve, hogy "a mesterséges intelligencia tervezőinek mindig biztosítaniuk kell az érzékeny adatok titkosságát, sértetlenségét és rendelkezésre állását, azt, hogy a mesterséges intelligencia rendszer mentes legyen az ismert sebezhetőségektől, és hogy a rendszer vagy a felhasználó adatai elleni rosszindulatú viselkedés védelmére, észlelésére és az arra való reagálásra szolgáló ellenőrzéseket biztosítsanak").
[6]https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf (megjegyezve: "A mesterséges intelligenciával kapcsolatos politikák értékelésénél vagy bevezetésénél az ügynökségeknek szem előtt kell tartaniuk a potenciális biztonsági és védelmi kockázatokat, valamint a mesterséges intelligencia-alkalmazások esetleges rosszindulatú telepítésének és használatának kockázatát").
[7] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (megjegyezve: "A mesterséges intelligencia rendszereknek rugalmasnak és biztonságosnak kell lenniük. Biztonságosnak kell lenniük, biztosítva egy tartalék tervet arra az esetre, ha valami rosszul sülne el, valamint pontosnak,

megbízhatónak és reprodukálhatónak kell lenniük. Csak így biztosítható, hogy a nem szándékos károkat is minimalizálni és megelőzni lehessen").

[8] https://nicholas.carlini.com/writing/2019/all-adversarial-example-papers.html (lásd az összes dokumentumot tartalmazó txt fájlt)

* Egyenlő hozzájárulás

algoritmus.[9] Egy perturbációs támadás során a kutatók egyszerű matricákkal tudták letéríteni a Tesla önvezető rendszerét az autópályáról.[10] Az ilyen jellegű támadások különösen gyakoriak a kiberbiztonsági ipar által kifejlesztett védelmi eszközök ellen. A kutatók például képesek voltak becsapni a Cylance, egy kereskedelmi vírusirtó motor ML-rendszerét, hogy tévesen felismerje zsarolóprogramok jóindulatú szoftverként.[11] Egy másik példa szerint két biztonsági kutató megkerülte a Proofpoint, egy kereskedelmi e-mail védelem, azáltal, hogy először másolja a mögöttes ML modellt és offline, majd online támadást indítottak olyan e-mailekkel, amelyek kikerültek a rendszerből. Ez lett az első olyan sebezhetőség, amelyet egy ML-rendszeren kihasználtak, és amely bekerült a nemzeti sebezhetőségi adatbázisba.[12]

Ez a kutatás nem mentes a jogi kockázatoktól. Bármely operatív rendszer biztonságának tanulmányozása vagy tesztelése potenciálisan ütközik a Computer Fraud and Abuse Act (CFAA),[13] az Egyesült Államok elsődleges szövetségi törvényével, amely a hackelésért való felelősséget keletkezteti.[14] Eredetileg 1984-ben szűkített törvényként léptették hatályba, de azóta újabb és újabb tilalmakkal bővült.[15] A CFAA széles hatályát sok kritika érte, a biztonsági kutatók a leghangosabbak között vannak.[16] Érvelésük szerint a CFAA - merev követelményeivel és súlyos büntetéseivel - visszaszorítja a biztonsági kutatást.[17] Az ellenséges ML-biztonsági kutatás valószínűleg nem különbözik ettől.

A kontradiktórius ML-kutatással és a CFAA-val kapcsolatos korábbi munka azonban kevés. Egy 2018-as cikkben Ryan Calo et al. a CFAA szerinti ellenséges támadásokat vizsgálta, de csak az ellenséges ML-támadások három osztályát vizsgálta (kitérés, mérgezés és adat-inverzió).[18] A többi vonatkozó közzétett kommentár hasonlóan korlátozott. Egy nemrégiben megjelent tanulmány például csak a kitérő és a mérgező támadásokat vizsgálta, [19]míg egy másik a perturbációs, az extrakciós és a mérgező támadásokat vette figyelembe, de nem vizsgálta a bíróságok által a vonatkozó CFAA-rendelkezések alkalmazásában mutatkozó fontos következetlenségeket.[20] Mi itt ezt tesszük meg.

Ennek a dokumentumnak két célja van. A jogalkalmazók számára leírjuk a CFAA-nak a kontradiktórius ML-re való alkalmazásának összetett és zavaros jogi környezetét. A kontradiktórius ML-kutatók számára ismertetjük a kontradiktórius ML-kutatás potenciális kockázatait. Végezetül elemzést készítünk arról, hogy az Egyesült Államok Legfelsőbb Bírósága hogyan oldhatja fel a jelenlegi ellentmondásokat a

---

[9] Faizullabhoy, Irfan és Aleksandra Korolova. "A Facebook hirdetési platformja: New attack vectors and the need for interventions." *arXiv preprint arXiv:1803.10099* (2018).
[10] Xi, Bowei. "Ellenséges gépi tanulás a kiberbiztonság és a számítógépes látás számára: A jelenlegi fejlesztések és kihívások." *Wiley Interdisciplinary Reviews: Computational Statistics*: e1511.
[11] https://skylightcyber.com/2019/07/18/cylance-i-kill-you/
[12] https://nvd.nist.gov/vuln/detail/CVE-2019-20634
[13]18 U.S.C. § 1030.
[14] Kossoff, Jeff. (2019). Cybersecurity Law (Wiley, 2019) at 172.
[15] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, Minn94. L. Rev. (1561,20101561); Kossoff 172-173.
[16] Kosseff 212-213.
[17] Kosseff 213.
[18] Calo, Ryan, et al. "Is Tricking a Robot Hacking?". University of Washington School of Law Research Paper 2018-05 (2018);
[19] Shankar Siva Kumar, Ram, et al. "Law and Adversarial Machine Learning." *arXiv preprint arXiv:1810.10731* (2018).

[20] Natalie Chyi. (2020). A CFAA vizsgálata a kontradiktórius gépi tanulás kontextusában. https://www.legaltechcenter.net/a-i/commentary/.

A CFAA alkalmazása a *Van Buren kontra Egyesült Államok* ügyben,[21] amely fellebbezésről várhatóan a következő évben születik döntés. Úgy 2021.véljük, hogy a bíróság valószínűleg a CFAA szűk értelmezését fogja elfogadni, és ez hosszú távon valóban jobb kontradiktórius ML biztonsági eredményekhez fog vezetni.

CFAA és a kontradiktórius ML

A CFAA két szakaszát tekintjük különösen fontosnak az ellenséges gépi tanulás szempontjából. Először is, a számítógéphez való szándékos hozzáférés "engedély nélkül" vagy "az engedélyezett hozzáférést meghaladó módon", és ennek eredményeként "bármilyen információ" megszerzése egy "védett számítógépen" (1030(a)(2)(C) szakasz). Másodszor, szándékosan "kárt" okoz egy "védett számítógépnek" jogosulatlanul, "tudatosan" "program, információ, kód vagy parancs" továbbításával (1030(a)(5)(A) szakasz). Mindkettő büntetőjogi tilalom, de a CFAA magánjogi kereseti jogot is tartalmaz. Ez lehetővé teszi bármely személy számára, hogy pereljen, ha a CFAA megsértése miatt károkat vagy veszteségeket szenvedett el, beleértve ezt a két rendelkezést is.[22] Ezek a szakaszok nem merítik ki a CFAA szerinti lehetséges felelősséget, de lefedik a leggyakoribb ML-támadásokat.

Szándékos hozzáférés engedély nélkül vagy engedélyt meghaladóan -- 1030(a)(2) szakasz
A CFAA-t következetlenül alkalmazták. Az értelmezésével kapcsolatos ítélkezési gyakorlatot a következőképpen jellemezték
"széttöredezett" [23]és "nem egyértelmű", [24]a bíróságok "bizonytalanságot és zavart" fejeznek ki.[25] Az egyik
legvitatottabb ellentmondás a 1030(a)(2)(C) szakasz értelmezése, amely tiltja, hogy bárki "szándékosan jogosulatlanul hozzáférjen egy számítógéphez" vagy "túllépje az engedélyezett hozzáférést", és "ezáltal információt szerezzen bármely védett számítógépről".[26] Néhány ponton a bíróságok általában egyetértettek. Nagyon tágan értelmezték a "védett számítógép" kifejezést. Például magában foglal minden olyan számítógépet, amely az internethez csatlakozik.[27] Azt is általában úgy találták, hogy a "jogosulatlanul" az engedély nélküli hozzáférést jelenti. A "jogosultságot meghaladó hozzáférés" kifejezés jelentését illetően azonban jelentős nézeteltérések vannak. A megfogalmazás a bennfentesekre vonatkozik: olyan felhasználókra, akik már rendelkeznek jogosultsággal egy számítógépes rendszerhez -- például egy felhasználó, aki lekérdezési kéréseket küld egy ML-rendszerbe --, de valamivel *túllépik* ezt a jogosultságot a számítógépen lévő bármely információhoz való hozzáféréssel.

Mi jelenti az engedélyezett hozzáférés túllépését? Jelenleg 4-3 arányban oszlanak meg az Egyesült Államok fellebbviteli bíróságai. (A nem jogászok számára: a szövetségi fellebbviteli bíróságok az ország egyes régióit fedik le, és a Legfelsőbb Bíróság döntésének hiányában a szövetségi bíróságok jogértelmezését szabályozzák ezeken a területeken). Az Első, az Ötödik, a Hetedik és a Tizenegyedik Kerületi Bíróság, amelyek

[21] Van Buren v. United States, F940.3d (119211th Cir. 2019), petíciót nyújtottak be (U.S. Dec. 201918,) (No. 19-783) (a fellebbezésről szóló határozat függőben).
[22] Id. § 1030(g)
[23]Michael J. O'Connor, *The Common Law of Cyber-Trespass*, Brook85. L. Rev. (421,2020422)
[24]Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, Minn94. L. Rev. (1561,2010).1562

[25]Orin S. Kerr, *Norms of Computer Trespass*, Colum116. L. Rev. (1143,20161145).
[26]18 U.S.C. § 1030(a)(2)(C).
[27] *United States v. Kramer,* 631 F.3d 900, 902 (8th Cir. 2011) (megjegyezve, hogy a "számítógép" meghatározása "rendkívül tág", és megállapította, hogy egy közönséges mobiltelefon is számítógép); *United States v. Nosal (Nosal II),* 844 F.3d 1024, 1050 (9th Cir. 2016), cert. denied, 138 S. Ct. 314 (2017) (megjegyezve, hogy a "védett számítógépek" közé "gyakorlatilag minden internet-hozzáféréssel rendelkező számítógép tartozik...").

többek között Illinois, Massachusetts és Texas, tágabb értelmezést fogadtak el, megállapítva, hogy az "engedélyezett hozzáférés túllépése" magában foglalja a számítógépes rendszerben lévő információkhoz való "nem megfelelő célú" hozzáférést, ami általában valamilyen megállapodás, szabályzat vagy szolgáltatási feltételek megszegését jelenti. Néhány példa erre az volt, hogy a vádlott nem kezelte vagy felügyelte egy másik felhasználó fiókinformációit. Egy másik példa lehet egy távozó alkalmazott, aki a titoktartási megállapodásokkal ellentétesen töltött le vállalati információkat, vagy megsértette a hálózathasználati vagy hozzáférési szabályzatot. Az alábbi elemzésünkben ezt a 1030(a)(2) bekezdés "tágabb értelmezésének" fogjuk nevezni.

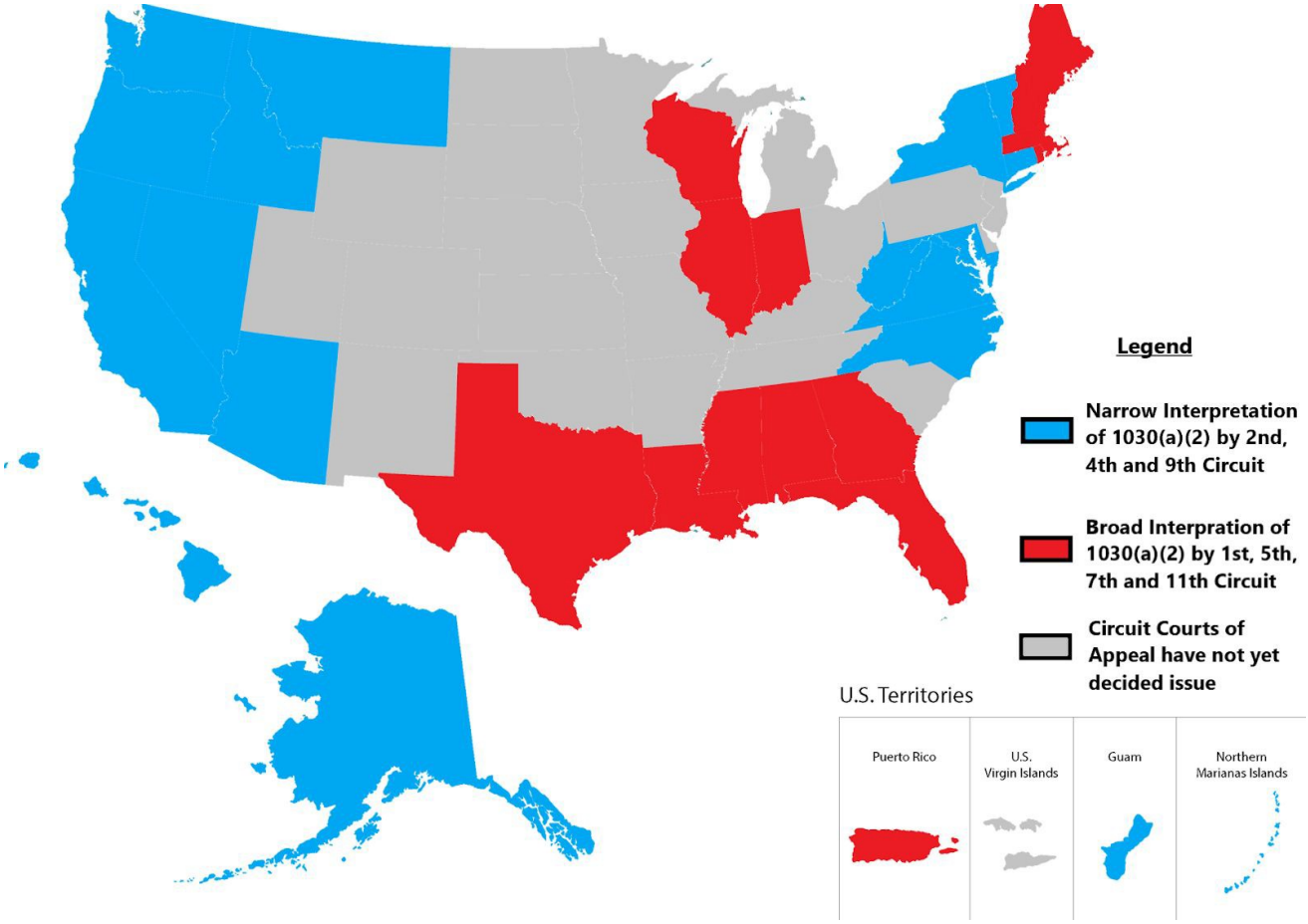
Ezzel szemben a New Yorkot és Kaliforniát is magában foglaló második, negyedik és kilencedik kerületi fellebbviteli bíróságok a fogalom szűk értelmezését fogadták el. Úgy ítélték meg, hogy az információkhoz való egyszerű, nem megfelelő célú hozzáférés nem minősül a 1030(a)(2) szakasz megsértésének. Inkább csak akkor "lépi túl az engedélyezett hozzáférést", ha egy személynek bármilyen okból tilos hozzáférnie az információkhoz. A gyakorlatban e szűkebb értelmezés szerint az alperes "túllépi az engedélyezett hozzáférést", ha a felhasználó (i) hozzáféréssel rendelkezik egy számítógépes rendszerhez; (ii) engedélyezett hozzáférése a rendszerben lévő bizonyos információkra korlátozódik; és (iii) a felhasználó megkerül vagy megkerül egy "technológiai hozzáférési korlátot" vagy "kódalapú" korlátozást, hogy további információkhoz férjen hozzá.[28] Az alábbi elemzésünkben ezt a 1030(a)(2) bekezdés "szűk értelmezésének" fogjuk nevezni.

A többi kerületi bíróság nem hozott végleges döntést ebben a kérdésben. Így az ország egyes régiói szűk értelmezést alkalmaznak; egyes régiók tágabb értelmezést alkalmaznak; és vannak olyan régiók, ahol még nem foglalkoztak ezzel az értelmezési kérdéssel, ami zavaros és bizonytalan helyzetet teremt a CFAA országos alkalmazásával kapcsolatban. A hatályos jog széttöredezett jellegét a következő térkép szemlélteti (**ábra1**):

[28] *Lásd* Brenda Sharton et al., "Key Issues in Computer Fraud and Abuse Act (CFAA) Civil Litigation", *Practical Law (Thomson Reuters)* 1, 4 (2018) (a szűkített olvasat összefoglalása); *United States v. Nosal I,* 676 F.3d 854, 863-864 (9th Cir. 2012) (en banc) ("szűkebb értelmezése egyben egy olyan jogszabály szövegének és jogalkotási történetének értelmesebb olvasata, amelynek általános célja a hackelés - a technológiai hozzáférési korlátok megkerülése - büntetése, nem pedig az üzleti titkok eltulajdonítása"). Kosseff, 175. o. ("A jogszabály szűk értelmezése arra a következtetésre vezethet, hogy csak akkor sérti meg

a CFAA-t, ha kódalapú jogsértést követ el").

1. ábra: A CFAA eltérő értelmezése a Circuit Court régió szerint



Ez a zavaros helyzet hamarosan véget érhet, mivel az Egyesült Államok Legfelsőbb Bíróságának lehetősége nyílik arra, hogy a *Van Buren kontra Egyesült Államok* ügyben foglalkozzon ezekkel a következetlenségekkel.[29] Ezt az ügyet és a kontradiktórius ML-hez való kapcsolódását e tanulmány utolsó részében tárgyaljuk.

Szándékos hozzáférés engedély nélkül vagy engedélyt meghaladóan -- 1030(a)(5) szakasz
Az 1030(a)(5)(A) szakasz megtiltja, hogy bárki "tudatosan" továbbítson "programot, információt, kódot vagy parancsot", és ezáltal szándékosan "kárt" okozzon egy "védett számítógépnek". A 1030(a)(2)(C) szakasszal ellentétben ez a kívülállókra és a bennfentesekre egyaránt vonatkozik. Bár a CFAA nem határozza meg a "továbbítás" fogalmát, a bíróságok általában úgy ítélték meg, hogy ez történhet az interneten keresztül vagy fizikai úton.
adathordozó, például egy USB-pendrive.[30] A felelősségre vonáshoz nem csak az szükséges, hogy az illető tudatosan továbbítsa, hanem az is, hogy
szándékosan károsítja a védett számítógépet. A CFAA meghatározása szerint a "kár" magában foglalja "az adatok, a program, a rendszer vagy az információ integritásának vagy rendelkezésre állásának bármilyen károsodását".[31]

[29] Van Buren v. United States, F940.3d (119211th Cir. 2019), petíciót nyújtottak be (U.S. Dec. 201918,) (No.

19-783) (a fellebbezésről szóló határozat függőben).
[30] Meridian Fin. Advisors, Ltd. kontra Pence, F763. Supp. 2d 1061-621046,). (S.D. Ind. 2011)).
[31] § 1030(e)(8).

A szolgáltatásmegtagadó (DOS) támadások - amikor kódot vagy parancsokat küldenek az interneten vagy más médiumon keresztül, és a fogadó rendszert túlterhelik vagy megzavarják - szintén e szakasz alapján kerültek büntetőeljárás alá. További példák közé tartozik a rosszindulatú kódok, köztük trójaiak vagy vírusok küldése; a címzett számítógépén lévő e-maileket törlő kódok; az elsősegélynyújtók kommunikációjára használt rádiós kommunikációs hálózaton keresztül küldött kódok, amelyek szándékosan zavarják a normál működést*;* [32]valamint a fogadó rendszert túlterhelő, a normál üzleti működést megzavaró tömeges vagy tömeges e-mailek.[33]

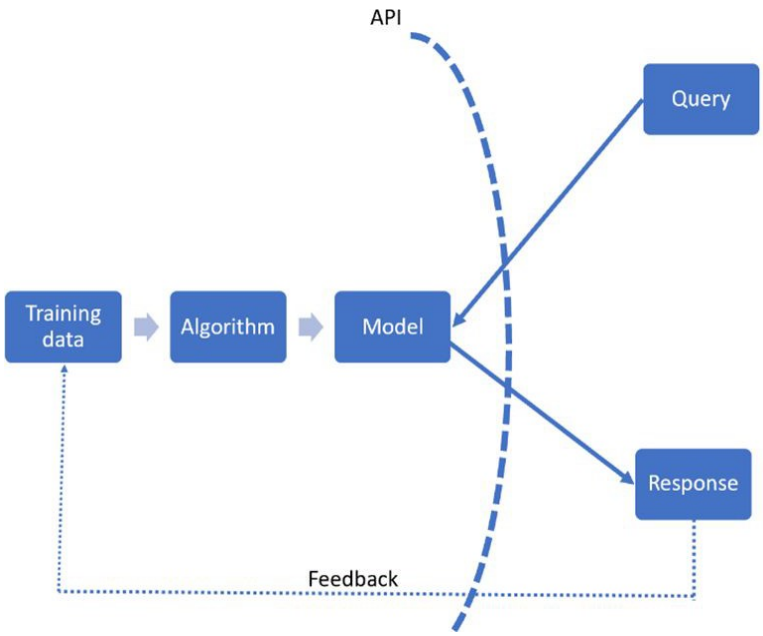
Hogyan befolyásolja a CFAA a gépi tanulással kapcsolatos kutatásokat

Hatályba lépése óta a CFAA-t alkalmazzák az operatív rendszereket tanulmányozó kutatókra. Az 1030(a)(2)(C) és az 1030(a)(5) szakaszok kivételesen széles alkalmazási köre hatással van az ML-kutatókra - és általában a biztonsági kutatókra -, akik büntetőjogi és polgári jogi felelősségre vonhatók a számítógéphez való jogosulatlan hozzáférésért. Az operatív rendszerek kutatása általában magában foglalja a rendszerek szondázását, vagy akár betörését is. Ez magában foglalja azokat is, akik jogos felhasználóként hozzáférhetnek egy rendszerhez, és akiknek a hozzáférését a szolgáltatási feltételek szabályozhatják. Pusztán a szolgáltatási feltételekkel ellentétes módon történő tesztelés, minden további nélkül, azt jelentheti, hogy a kutató túllépte az engedélyezett hozzáférést, és megsértette a CFAA-t. A CFAA súlyos szankciói azt jelentik, hogy az ilyen megállapítások visszatartó erővel hathatnak a biztonsági kutatásokra.[34] Ezen túlmenően az 1030(a)(2)(C) szakasz értelmezésével kapcsolatos bírósági megosztottság azt jelenti, hogy a kockázat mértéke attól függ, hogy a CFAA-követelést melyik joghatóságban lehet elbírálni.

Ebben a szakaszban bemutatjuk, hogy ezek a CFAA-rendelkezések hogyan hatnak konkrétan a gépi tanulással kapcsolatos kutatásra. Feltételezünk egy fizetős szolgáltatást, amely a felhasználóinak gépi tanulási szolgáltatást nyújt (mondjuk képfelismerést). A felhasználók úgy lépnek kapcsolatba ezzel a rendszerrel, hogy lekérdezést küldenek, és megkapják az osztályozás eredményét (lásd **az ábrát2**):

[32] United States v. Mitra, F405.3d (4927th Cir. 2005) (szintén megállapítva, hogy egy rádiórendszer számítógép).
[33] Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., F648.3d (295,6th 301Cir. 2011).
[34]https://www.theguardian.com/technology/2014/may/29/us-cybercrime-laws-security-researchers; https://www.eff.org/wp/protecting-security-researchers-rights-americas

2. ábra: Black Box beállítása



Elemzésünk során feltételezzük, hogy a támadónak nincs közvetlen hozzáférése a képzési adatokhoz, nem ismeri az algoritmust, és nem tud az algoritmusban használt jellemzőkről. Feltételezzük továbbá, hogy a támadó a rendszer legitim felhasználója, és a rendszer használatát a Google API szolgáltatási feltételein (TOS) alapuló szabályok szabályozzák.[35]

E feltételek szerint a felhasználók nem:

1. Visszafejteni vagy megkísérelni bármely API vagy bármely kapcsolódó szoftver forráskódjának kinyerését, kivéve, ha ezt a korlátozást az alkalmazandó jogszabályok kifejezetten tiltják.
2. az API-k vagy az API-kat biztosító szerverek vagy hálózatok zavarása vagy megzavarása.
3. Az ilyen tartalmakról adatbázist kaparni, adatbázisokat építeni vagy más módon állandó másolatokat készíteni, illetve a gyorsítótár fejléc által megengedettnél hosszabb ideig tárolni a gyorsítótárban tárolt másolatokat.
4. másolni, lefordítani, módosítani, származékos munkát létrehozni, eladni, bérbe adni, kölcsönadni, továbbadni, terjeszteni, nyilvánosan bemutatni vagy harmadik félnek allicencet adni.
5. A forrás vagy a tulajdonjog hamis feltüntetése

Feltételezve ezt a közös felállást, a következő szakaszban a CFAA fényében megvizsgálunk egy sor ellenséges ML-támadást, beleértve a 1030(a)(2)(C) szakasz értelmezésének megosztottságát. Az egyértelműség kedvéért, bár a különböző ellenséges ML-támadások minden egyes tágabb osztályára gyakran kínálunk példákat szemléltetés céljából, elemzésünk célja, hogy foglalkozzunk azzal, hogy ezek a CFAA

[35] https://developers.google.com/terms

a rendelkezések a különböző ellenséges ML-támadások minden egyes széles csoportjára vonatkoznának, szemben a támadás egyetlen példányával. Elemzésünket az **ábrán3** is ábrázoljuk.

Felderítő támadások: Támadások, amelyek csak lekérdezéseket küldenek és megfigyelik a válaszokat.

Kitérő támadás

A kikerülést célzó támadások során a támadó képes módosítani a lekérdezést, hogy a kívánt választ kapja meg, anélkül, hogy megkerülné az ML API mögött álló komponenseket. A kutatók például képesek voltak sajátos zajt hozzáadni a röntgenfelvételekhez, ami becsapott egy ML-rendszert, hogy a rendellenes röntgenfelvételeket tévesen normálisnak minősítse. [36] A Cylance vírusirtó motorokat érintő modellelkerülő támadásban a kutatók egyszerűen egy online játéktárból származó jóindulatú kódot csatoltak rosszindulatú zsarolóprogramhoz, ami arra késztette az ML-rendszert, hogy a kódot jóindulatú szoftverként tévesen minősítse.[37]

Az ilyen támadások nem valószínű, hogy az 1030(a)(2) vagy az 1030(a)(5)(A) szakasz alapján felmerülnének felelősségi aggályok. Az előbbi rendelkezés esetében a "jogosultságot meghaladó hozzáférés" szűk értelmezése alapján nem áll fenn a 1030(a)(2) szakasz megsértése, mivel a lekérdezésekkel nem kerül meg semmilyen technológiai hozzáférési korlát vagy hitelesítési kapu. Az ML-rendszert csak becsapják, hogy helytelen választ adjon. De a tágabb értelmezés szerint sincs jogsértés, mivel ez a támadás nem sérti a TOS-t: nincs visszafejtés, kaparás vagy származékos mű létrehozása. Az 1030(a)(5)(A) szakasz szerinti felelősségre vonás szintén nem valószínű. Még ha feltételezzük is, hogy a lekérdezés továbbított "programnak, információnak, kódnak vagy parancsnak" minősül, a kifejezés értelmében nincs "kár". Nem következik be a rendszer vagy a kapcsolódó adatok "integritásának" vagy "rendelkezésre állásának" "károsodása",[38] mivel nem történik "az elektronikus fájlok megsemmisítése, megrongálása vagy törlése", a rendszer "fizikai megsemmisülése", sem "a számítógépes rendszerben lévő adatok teljességének vagy használhatóságának bármilyen csökkenése".[39]

Modell lopás

A modelllopó támadások során a támadó képes a modell stratégiai lekérdezésével és a válasz megfigyelésével létrehozni az alapul szolgáló ML-modell másolt változatát, és ezáltal újrateremteni a szellemi tulajdont. A kutatók például képesek voltak olyan mély neurális hálókat újrateremteni, amelyeket az ML mint szolgáltató - például a Microsoft, a Face++, az IBM, a Google és a Clarifai - szolgáltatott, és amelyek nemcsak pontosak voltak (pontosságuk >80%), hanem olcsón fel is szerelhetők (kevesebb mint 3 dollárba kerültek).[40] A modelllopás egyik megközelítése a meglévő ML API orákulumként való felhasználása; azaz a támadó elegendő lekérdezést tesz az ML modell összes osztályára, megfigyeli a választ, és a (lekérdezés, válasz) párokból új függvényt tanul.[41]

---

[36] Paschali, Magdalini, et al. "Generalizability vs. robustness: investigating medical imaging networks using adversarial examples." (Általánosíthatóság vs. robusztusság: orvosi képalkotó hálózatok vizsgálata ellenpéldák segítségével). *International Conference on Medical Image Computing and Computer-Assisted Intervention (Nemzetközi konferencia az orvosi képfeldolgozásról és a számítógéppel segített beavatkozásról)*. Springer, Cham, 2018.
[37] I.d. 11
[38] § 1030(e)(8).
[39] TriTeq Lock & Sec. LLC kontra Innovative Secured Solutions, LLC, Civ. Action No. 10 CV 1304,

WL2012 at394229, 6; Kossoff at 197-198.

[40] Yu, Honggang, et al. "Cloudleak: Nagyméretű mélytanulási modellek lopása ellenséges példákon keresztül." *Proceedings of Network and Distributed Systems Security Symposium (NDSS)*. 2020.

[41] Tramèr, Florian, et al. "Stealing machine learning models via prediction apis". *25th {USENIX} Security Symposium ({USENIX} Security 16)*. 2016.

Az 1030. szakasz a) pontjának (2) bekezdése tekintetében a szűk értelmezés szerint valószínűleg nem áll fenn jogsértés, mivel nem kerül meg semmilyen technológiai hozzáférési korlát vagy kódalapú korlátozás. A lekérdezéseket csupán elküldik, és a megfigyelt válaszok alapján következtetéseket vonnak le. A 1030. a) pont (2) bekezdésének tágabb értelmezése alapján azonban jogsértésről lehet szó, ami attól függ, hogy a bíróság mennyire tágan értelmezi az ML-rendszerre és a bennfentes felhasználóra irányadó vonatkozó ÁSZF-et. Egyrészt valószínűtlennek tűnik, hogy egy bíróság úgy találja, hogy a jogos lekérdezési válaszokból *levezetett* információ a TOS alapján tiltott lehet, és CFAA felelősséget eredményezhet. Másrészt, ahogy az itt feltételezett TOS esetében is, az ilyen ML-használati korlátozások és irányelvek gyakran tiltják a visszafejtést vagy az adatbázisok létrehozását a lekérdezési válaszok alapján, még ha azok jogszerűek is. Így *lehetséges,* hogy egy bíróság a modelllopási támadást a modell "forráskódjának" "visszafejtésére" irányuló kísérletnek minősítené, ellentétben a TOS 1. záradékával, amelyek, mint említettük, meglehetősen tipikus használati vagy szolgáltatási feltételek. Ez "származékos mű" létrehozásának is minősülhet, ami szintén ellentétes az ÁSZF záradékával. 4.

Itt azonban nem valószínűsíthető az 1030(a)(5)(A) szakasz megsértése, mivel - az adóelkerülési támadásokhoz hasonlóan - a "kár" követelménye nem teljesül. Nincs a rendszer vagy a kapcsolódó adatok "integritásának" vagy "rendelkezésre állásának" "károsodása".

Modell inverzió és tagsági következtetés

A modell inverziós támadások során a támadók érzékeny információkat szereznek a privát képzési adatokról. Az egyik tanulmány bemutatta, hogy a személyre szabott orvoslásban használt ML-modellhez való akár feketedobozos hozzáféréssel a támadók vissza tudják szerezni a képzési adatok részét képező betegek privát genetikai markereit.[42] Az ilyen típusú támadásokat később kiterjesztették az ML API beállítására, ahol a kutatók megmutatták, hogy a támadók hogyan használhatják ki a válaszokban feltárt konfidenciaintervallumokat a privát képzési adatokban használt jellemzők rekonstruálására.[43] Az ilyen támadások komoly aggodalmakat vetnek fel, mivel a képzési adatok általában adatvédelmi szempontból érzékeny információkat tartalmaznak.[44]

A tagságra következtető támadások során a támadó stratégiai lekérdezéssel és a válasz megfigyelésével képes megállapítani, hogy egy adatpont része volt-e a képzési adatoknak. Például egy kórházi elbocsátási adatokon kiképzett és ML API-kban, például a Google Prediction API-ban elhelyezett modellben a kutatók megmutatták, hogy a támadók hogyan használhatják ezt a technikát arra, hogy egyszerű általános információk, például a résztvevő kora és neme révén rekonstruálják a képzési adatok részét képező résztvevők magáninformációit (például a páciens által elvégzett eljárást).

[42] Fredrikson, Matthew, et al. "Adatvédelem a farmakogenetikában: A személyre szabott warfarin adagolás végponttól végpontig tartó esettanulmánya." *23. {USENIX} biztonsági szimpózium ({USENIX} Security 14)*. 2014.

[43] Fredrikson, Matt, Somesh Jha és Thomas Ristenpart. "A bizalmi információt kihasználó modellinverziós támadások és alapvető ellenintézkedések". *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 2015.
[44] Zhang, Yuheng, et al. "The secret revealer: generatív modell-inverziós támadások mély neurális hálózatok ellen". *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (IEEE/CVF konferencia a számítógépes látásról és mintafelismerésről)*. 2020.

3. ábra: Ábra Vizualizáció Ellentétes ML jogi kockázatok

Támadás	Leírás	1030(a)(2) megsértése? (Szűk értelmezés a második, negyedik és kilencedik bíróságok részéről)	1030(a)(2) megsértése? (Az első, ötödik, hetedik és tizenegyedik kerületi bíróságok tág értelmezése)	1030(a)(5)(A)(A) jogsértés
Kitérő támadás	A támadó módosítja a lekérdezést a megfelelő válasz érdekében	Nem	Nem	Nem
Modell inverzió	A támadó gondos lekérdezésekkel visszanyeri a modellben használt titkos jellemzőket.	Nem	Lehetséges	Nem
Tagsági következtetés	A támadó le tudja szűrni, hogy az adott adatrekord része volt-e a modell képzési adathalmazának vagy sem.	Nem	Lehetséges	Nem
Modell lopás	A támadó gondos lekérdezéssel képes visszaszerezni a modellt.	Nem	Lehetséges	Nem
Az ML rendszer átprogramozása	Az ML-rendszer újrafelhasználása olyan tevékenység elvégzésére, amelyre nem volt beprogramozva.	Nem	Igen	Igen
Mérgezéses támadás	A támadó beszennyezi az ML rendszerek képzési fázisát a kívánt eredmény elérése érdekében	Nem	Lehetséges	Igen
Az ML ellátási lánc megtámadása	A támadó veszélyezteti az ML-modelleket, miközben letöltik használatra	Igen	Igen	Lehetséges
Szoftverfüggőségek kihasználása	A támadó hagyományos szoftveres kihasználásokat használ, például puffer túlcsordulást, hogy összezavarja az ML	Igen	Igen	Igen

	rendszereket.			

Itt sem valószínűsíthető az 1030(a)(5)(A) szakasz megsértése, mivel a rendszer "integritásának" vagy "rendelkezésre állásának" nem áll fenn "károsodása". A 1030(a)(2)(C) szakasz megsértése szintén nem valószínű a szűk értelmezés alapján, mivel nem kerül meg semmilyen technológiai hozzáférési korlát vagy kódalapú korlátozás, csak a lekérdezési válaszokon alapuló következtetések. A tágabb értelmezés azonban bonyolultabb. A modelllopási támadásokhoz hasonlóan a CFAA tágabb értelmezése is azon múlik, hogy a bíróság mennyire tágan értelmezi a TOS-t. A bíróság arra a következtetésre juthat, hogy ez a hozzáférés nem megfelelő célú, és így meghaladja az engedélyezett hozzáférést, mivel a modell "forráskódjának" "visszafejtését" jelenti, ami ellentétes a TOS-szal. A bíróság azt is megállapíthatja, hogy a képzési készletekre vagy a tagságra vonatkozó információk *levonása az* adatbázis "építésében" részt vevő lépésnek minősül, amelyet a TOS záradékában foglalt tilalmak is előirányoznak. Ha 3.igen, akkor ez valószínűleg a CFAA megsértését jelentené.

Az ML rendszer átprogramozása

Ebben a támadásban a támadó speciális lekérdezések küldésével olyan feladat elvégzésére kényszerítheti a modellt, amelyet a készítője nem így tervezett. A kutatók például [45]bemutatták, hogy az ImageNet-et, a képek különböző kategóriákba sorolására használt rendszert hogyan használták át négyzetek számolására. A tanulmány szerzői kifejtik, hogy ez a támadás hogyan vezethet az ML-rendszerekkel való visszaéléshez: egy támadó például spam-fiókokat akarhat létrehozni, de ezt a megoldandó CAPTCHA-képek akadályozzák. Az átprogramozási támadás segítségével a támadó a felhőalapú képtárolókban használt képfelismerő rendszert át tudná alakítani a CAPTCHA-k megoldására, és így megszüntethetné az akadályt.

Ebben az esetben a szűken értelmezett 1030(a)(2) szakasz nem sérülne, mivel ismétlem, nem került sor a technológiai hozzáférés akadályának megkerülésére. Egy tágabb értelmezés más következtetéshez vezethetne, mivel ez minden bizonnyal az ML-rendszerbe való beavatkozásnak vagy az ML-rendszer megzavarásának minősülne, ami ellentétes az ÁSZF 2. szakaszával, mivel az ML-rendszer integritása sérül. Ez a támadás az 1030. szakasz a) pontja (5) bekezdésének A) alpontja alapján felelősségi aggályokat is felvet, mivel a speciális lekérdezések "kódnak" vagy "parancsoknak" minősülnek, amelyeket tudatosan és szándékosan "továbbítanak" az ML-rendszerbe. A támadás az ML-rendszer "integritásának" vagy "rendelkezésre állásának" "károsodását" is okozza. Ez *prima facie* jogsértést jelentene.

A képzési adatokat beszennyező támadások:

Mérgezéses támadás

A mögöttes adateloszlásban bekövetkező esetleges változásokhoz való alkalmazkodás érdekében az ML-modelleket gyakran újra képzik a modell által generált kimeneteken és a felhasználó által adott visszajelzéseken. Például egy spamosztályozási környezetben minden alkalommal, amikor a felhasználó visszajelzést ad a modellnek arról, hogy a levelet helytelenül osztályozta, a válasz elküldésre kerül a mögöttes modelleknek, és újratanítják őket. Ezt a visszajelzési csatornát, amelyben a válasz visszakerül a képzési adatokba, a támadók kihasználhatják a képzési adatok megmérgezésére. A kanonikus példa a Microsoft Tay chatbotja, amely a Tay felhasználókkal folytatott interakciói által generált válaszokat használta képzési adatként. Néhány órán belül a24

[45] Elsayed, Gamaleldin F., Ian Goodfellow és Jascha Sohl-Dickstein. "Adversarial reprogramming of neural networks." *arXiv preprint arXiv:1806.11146* (2018).

kiadásakor a Microsoftnak le kellett állítania, mivel az internetes trollok kihasználták ezt a visszajelzési csatornát, aminek következtében Tay rasszista megjegyzéseket és képeket osztott meg.[46]

Szűkebb értelemben valószínűleg nem áll fenn az 1030(a)(2) szakasz megsértése, mivel a támadás során nem kerülhető meg semmilyen technológiai hozzáférési akadály vagy hitelesítési kapu. A támadás azonban vitathatóan zavarja vagy megzavarja az ML rendszer működését, ellentétben 2az ÁSZF záradékával, így tágabb értelmezés esetén fennállhat a felelősség.

Ez a támadás valószínűleg az 1030(a)(5)(A) szakasz megsértésének minősül, mivel a lekérdezések valószínűleg "kódot" vagy "parancsokat" tudatosan "továbbítottak" az ML rendszerbe. A parancsok pedig az ML rendszer megrongálásával és "megmérgezésével" nagy valószínűséggel a szakasz értelmében vett "károkozás" formáját jelentik, mivel az ML rendszer "integritását" vagy "rendelkezésre állását" károsítják. Ez *prima facie* jogsértés.

Támadások az alapul szolgáló környezet ellen:

Támadás az ML ellátási lánc ellen
Ezekben a támadási osztályokban a támadó a forráskód, az építési folyamatok vagy a frissítési mechanizmusok manipulálásával felforgatja a gépi tanulási rendszert. Jelenleg az NLP és a számítógépes látás területén az előzetesen betanított modellek használatának trendje figyelhető meg, amelynek során a gigantikus általános adathalmazokon és nagy teljesítményű számítógépeken betanított ML-modelleket a nyilvánosság számára elérhetővé teszik a feladatspecifikus testreszabáshoz.[47] A kutatók kimutatták[48], hogy a támadók man-in-the-middle támadást indíthatnak, miközben ezeket a modelleket letöltik használatra, vagy egyszerűen rosszindulatú kódot illeszthetnek be a nyilvános tárolóba, ahol a modelleket tárolják.

Ez a támadás mindkét szakasz alapján felelősségre vonási aggályokat vet fel. Ha a támadás a technológiai biztonság vagy a hozzáférési korlátok megsértését jelentette az ML-ellátási lánc veszélyeztetése érdekében, ez a külső támadók esetében "jogosulatlan hozzáférésnek" minősülne, a bennfentesek esetében pedig akár tágan, akár szűken értelmezve "meghaladná a jogosultságot". A kódalapú korlátozások megkerülése és a védett számítógépen lévő forráskód engedély vagy felhatalmazás nélküli kompromittálása a 1030. szakasz a) pontjának (2) bekezdése alapján tiltott számítógépes hackelés klasszikus esetei, akár szűk, akár tág értelmezés szerint.

Az 1030(a)(5)(A) szakasz megsértése is valószínűsíthető, attól függően, hogy a támadást hogyan hajtják végre. Ha egy technológiai akadályt megkerültek, akkor valószínű, hogy egy "kódot" vagy "parancsot" tudatosan "továbbítottak" az ML-rendszerbe, és e cselekmény eredményeként az ML-rendszer "integritása" vagy "rendelkezésre állása" - az ellátási láncán keresztül - "sérült". Ez szintén *prima facie* jogsértésnek minősül.

[46] https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/ (megjegyezve, hogy "Sajnos az online megjelenés első 24 órájában egy összehangolt támadás során az emberek egy része kihasználta a

Tay. Bár a rendszerrel való visszaélések számos típusára felkészültünk, a konkrét támadással kapcsolatban kritikus figyelmetlenséget követtünk el. Ennek eredményeként a Tay vadul helytelen és elítélendő szavakat és képeket tweetelt").

[47] https://huggingface.co/calculator/

[48] Gu, Tianyu, Brendan Dolan-Gavitt és Siddharth Garg. "Badnets: Identifying vulnerabilities in the machine learning model supply chain." *arXiv preprint arXiv:1708.06733* (2017).

Szoftverfüggőségek kihasználása
Itt a támadó ahelyett, hogy a képzési adatokat, a modellt vagy a lekérdezésekkel történő szondázást támadná, a mögöttes infrastruktúrát támadja, amelyre az ML rendszer épül. A kutatók például [49]bemutatták, hogyan használhatják ki a támadók a népszerű ML-csomagok, például a numpy és a tensorflow nem javított sebezhetőségeit, és hogyan sérthetik meg a titkossági, integritási és rendelkezésre állási garanciákat.

Ez a támadás valószínűleg mindkét esetben felelősségre vonást eredményez. Az ML-rendszer szoftveres sebezhetőségének kihasználása sérti a 1030. szakasz a) pontjának (2) bekezdését, mivel azt jelenti, hogy a technológiai hozzáférési korlátokat jogosulatlanul vagy a jogosultságot túllépve kijátsszák, és ezzel kárt vagy veszteséget okoznak. Az ML ellátási lánc elleni támadásokkal kapcsolatos érvelésünkhöz hasonlóan itt is ugyanarra a következtetésre vezet akár a szűk, akár a tág értelmezés.

A támadás jellegétől függően a 1030(a)(5)(A) szakasz alapján is fennállhat a felelősség. Ha egy technológiai akadályt exploit kód segítségével megkerültek, akkor valószínű, hogy egy "kódot" tudatosan "továbbítottak" az ML-rendszerbe, ami végső soron az ML-rendszer "integritását" vagy "rendelkezésre állását" károsította. Ez is *prima facie* jogsértés lenne.

Van Buren és a jövő irányai

Elemzésünk megpróbált eligazodni a CFAA alkalmazásának jelentős következetlenségei között. Ezen értelmezési kérdések némelyikét az Egyesült Államok Legfelsőbb Bírósága a folyamatban lévő
Van Buren kontra Egyesült Államok ügyben hozott határozat, amelyről valószínűleg az In2021.[50] *Van Buren*, the
a vádlott egy rendőrtiszt volt, aki "nem rendeltetésszerű céllal" férhetett hozzá egy rendőrségi adatbázishoz, azaz nem a rendőri munkához kapcsolódóan, hanem azért, hogy az adatbázisból származó információkat eladja egy harmadik félnek. A harmadik félről kiderült, hogy egy FBI-akció része volt, és a vádlottat a 1030(a)(2) szakasz alapján bűncselekmény miatt elítélték. Az Eleventh Circuit helybenhagyta az ítéletet, és a vádlott most a Legfelsőbb Bírósághoz fellebbezett. A Bíróságnak kell eldöntenie, hogy a vádlott azáltal, hogy az adatbázishoz való jogosulatlan hozzáféréssel "túllépte-e az engedélyezett hozzáférést".

Röviden, a Legfelsőbb Bíróságnak lehetősége van arra, hogy feloldja az 1030(a)(2) szakasz e nyelvezetének alkalmazásával kapcsolatos megosztottságot, és akár szűkebb, akár tágabb értelmezést fogadjon el, és nagyobb biztonságot teremtsen a CFAA alkalmazása terén. A döntés valószínűleg hatással lesz a CFAA egyéb értelmezési kérdéseire is, mint például arra, hogy az egyszerű TOS megsértése "jogosulatlan hozzáférésnek" minősülhet-e a hackerellenes jogszabály más alszakaszainak alkalmazásában.

Hogyan fog dönteni *Van Buren*? Véleményünk szerint a CFAA-nak a *Nosal I-ben* megfogalmazott, a Kilencedik Körzet által alkalmazott szűkebb értelmezése hűségesebb a CFAA eredeti és központi céljához, mint a hacker elleni törvényhez. Amint azt a *Nosal I.* ügyben eljáró bíróság megjegyezte, a Kongresszus a CFAA-t "elsősorban a számítógépes

hackerek növekvő problémájának kezelésére" alkotta meg, és egy olyan szűk értelmezés, amely a CFAA
a hackelés és a technológiai akadályok megkerülése jobban megfelelne ennek a fókusznak, "mint a

[49] Xiao, Qixue, et al. "Biztonsági kockázatok a mélytanulási implementációkban". *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018.
[50] Van Buren v. United States, F940.3d (119211th Cir. 2019), petíciót nyújtottak be (U.S. Dec. 201918,) (No. 19-783) (a fellebbezésről szóló határozat függőben).

a CFAA-t egy átfogó internet-rendőrségi mandátummá változtatva".[51] A CFAA tágabb értelmezése gyakorlatilag kriminalizálja a szerződésszegést, azáltal, hogy a TOS vagy más általános magánjellegű számítógép-használati irányelvek megsértését bűncselekménnyé változtatja. Ez azt jelentené - jegyzi meg a bíróság -, hogy "gyanútlan egyének milliói tapasztalnák, hogy bűncselekményt követnek el".[52] Más szóval, a szűk értelmezés jobban megfelel a CFAA eredeti céljainak, és elkerülhető az a nyugtalanító eredmény, hogy az internetfelhasználók büntetőjogi felelősségre vonhatók legyenek olyan egyszerű TOS-ok megsértéséért, amelyeket a legtöbb ember nap mint nap elkövet, tudatosan vagy sem.

Ha igazunk van, és a Legfelsőbb Bíróság követi a Kilencedik Körzet szűk értelmezését, ennek fontos következményei lesznek a kontradiktórius ML-kutatásra. Sőt, úgy véljük, hogy ez hosszú távon jobb biztonsági eredményekhez fog vezetni. Először is, ha az ML biztonsági kutatók és az iparági szereplők nem támaszkodhatnak a kiterjedt TOS-ra a támadások bizonyos formáival szembeni elrettentés érdekében, akkor ez erőteljes ösztönzést kell, hogy jelentsen az ilyen támadások elleni védekezéshez szükséges robusztusabb technológiai és kódalapú intézkedések kifejlesztésére. A CFAA szűkebb értelmezésével pedig az ML-biztonsági kutatókat kevésbé fogják visszatartani attól, hogy teszteket és egyéb feltáró munkát végezzenek az ML-rendszereken, ami hosszú távon szintén jobb biztonságot eredményez.

Másodszor, még ha az ÁSZF-re lehet is támaszkodni, nem valószínű, hogy elrettentik a valóban rossz szereplőket. Az átlagos felhasználók nem olvassák el a TOS-t, és a kifinomultabb ellenfeleket valószínűleg nem riasztja el a támadásoktól pusztán a számítógép-használati szabályzat egy záradéka. Mint ilyenek, ezek a politikák és szerződéses intézkedések kevés proaktív védelmet nyújtanak a támadásokkal szemben, miközben gyakran elriasztják a törvényes kutatókat a rendszerek tesztelésétől vagy az eredmények bejelentésétől. A legvalószínűbb azonban, hogy az ML biztonsági kutatóit tartják vissza, *akik* odafigyelnének az ÁSZF-re, és a CFAA felelősségtől való félelem miatt visszariadhatnak a kutatástól.[53] Ebből a szempontból nézve a kiterjesztő szolgáltatási feltételek a biztonsági színház egyfajta jogi színházi formája lehetnek: performatív, kevés tényleges biztonsági védelmet nyújtanak, miközben valójában visszaszorítják azokat a gyakorlatokat, amelyek a biztonság javításához vezethetnek.

Harmadszor, a CFAA e tekintetben történő tág értelmezése legfeljebb utólagos lehetőségeket biztosíthat a veszteség vagy kár megtérítésére, de már léteznek jogi lehetőségek. Bár a jogorvoslatok minden bizonnyal eltérőek, a TOS megsértése miatt kárt vagy veszteséget elszenvedő áldozatok az állami törvények alapján is kereshetnek jogorvoslatot, például szerződésszegés vagy deliktuális beavatkozás miatti polgári jogi igényt. Röviden, jó és kényszerítő okok szólnak amellett, hogy a CFAA-nak továbbra is a hacker elleni szövetségi törvénynek kell maradnia, nem pedig egy átfogó versenyellenes törvénynek. Ez pedig hosszú távon az ML biztonsági kutatásának és eredményeinek javulásához vezethet.

Visszaigazolás

Szeretnénk köszönetet mondani Beth Friedmannak a tanulmányhoz adott átgondolt visszajelzéseiért és szerkesztéséért.

[51] Nosal I, 859-862. o.
[52] Nosal I at 861.
[53] Lásd például: Sandvig v. Barr, No. CV 16-1368, 2020 WL 1494065 (D.D.C. 2020) (megállapítva, hogy a fogyasztói honlapok gyakorlataira vonatkozó javasolt tudományos kutatási tervek - amelyek megsértik az említett fogyasztói honlapok ÁSZF-jét - nem vezetnének büntetőjogi felelősségre vonáshoz a CFAA alapján).