Associació per a les Nacions Unides a Espanya
United Nations Association of Spain

JUNY 2023

Les noves tecnologies y les seves amenaces

Ens trobem en un moment de gran incertesa, adulació i por davant les noves tecnologies sense saber realment el que són, els seus usos, i les amenaces que causen.

Què és el Ciberterrorisme?

De moment no existeix una definició única que defineixi el concepte. No obstant això, segons la UNODC es considera que ciberterrorisme és un crim cibernètic perpetrat per a coaccionar a un govern o població concreta, i causar o amenaçar amb causar mal (Denning, 2001). És a dir, l'ús de mitjans tecnològics per part de grups terroristes per a cometre una intrusió, una fallada o un atac en els sistemes informàtics o les xarxes de telecomunicacions d'infraestructures o institucions polítiques, econòmiques o socials.

El ciberterrorisme es realitza en remot des de qualsevol part del món el que augmenta les vulnerabilitats de les víctimes i dificulta processos judicials o legislatius. Alguns exemples de ciberterrorisme són: llançar un atac informàtic, suplantar o robar una identitat digital, enviar un programa espia, introduir un virus troià per a controlar en remot l'equip d'un altre usuari i robar informació, i segrestar dades privades a usuaris per a després demanar un rescat, així aconseguir diners per a finançar altres operacions delictives.

A l'Hospital Clínic de Barcelona va prendre lloc un dels segrestos d'informació més grans d'Espanya. El Conseller de Salut, Manel Balcells, va definir el ciberatac com a terrorisme del segle XXI, el hackeo va afectar substancialment l'activitat de l'hospital, el qual va haver d'ajornar centenars de cirurgies i extraccions, a més de no poder atendre infarts o ictus en urgències en el moment del hackeo. El problema persisteix i l'hospital segueix sense recuperar les seves dades, el Departament de Salut i l'Agència de Ciberseguretat de Catalunya van declarar que no negociaran amb els hackers que demanen 4,5 milions de dòlars per a retornar les dades robades.

Font: Ester Delgado, El País (2023)

Com afecta als drets dels individus?

Segons el Consell d'Europa i les Nacions Unides tota persona té drets digitals, que són una extensió dels drets humans ja existents, aquests poden ser: dret a una vida privada, patrimoni, dignitat, seguretat, integritat psicològica, i la no intervenció de comunicacions privades.

El ciberterrorisme ocorre amb molta més freqüència de la que ens podem imaginar, de fet, segons Cybersecurity Statistics hi ha 2,200 atacs al dia, aproximadament un cada 39 segons. Hi ha diferents nivells de ciberterrorisme des de hackeos a governs, hackeos són l'obtenció d'informació privada de manera il·legal, fins a la suplantació d'identitat digital.

En el ciberespai les amenaces passen desapercebudes per als usuaris, per tant, és necessari fomentar l'educació digital, que les persones coneguin les amenaces a les quals s'exposen amb la finalitat del seu ús responsable i la presa d'accions preventives, per a salvaguardar els seus drets humans. Entre les accions que es poden prendre per a prevenir aquests atacs es troben usar contrasenyes fortes, no fer clics en enllaços o pàgines sospitoses, utilitzar softwares de seguretat com a antivirus, firewalls i detecció programes malignes, evitar l'ús de xarxes de Wi-Fi per a fer transaccions o enviar dades amb programes malignes, evitar l'ús de xarxes de Wi-Fi per a fer transaccions o enviar dades confidencials, mantenir còpies de seguretat i ser conscient dels riscos actuals.

Guerres Híbrides amb Ciberterrorisme

Les guerres modernes ja no són només amb armes de foc o estats que decideixen combatre els uns contra els altres. Ara els actors estatals i no estatals poden utilitzar tàctiques cibernètiques per a soscavar les infraestructures crítiques, interrompre les comunicacions, robar informació confidencial, difondre propaganda, desestabilitzar economies i dur a terme accions destructives en l'àmbit virtual. En realitzar això la població perd estabilitat i confiança en les estructures governamentals per la qual cosa és una tàctica molt difícil de combatre una vegada realitzada.

Com esmentem anteriorment el ciberterrorisme pot incloure atacs contra sistemes de control industrial, infraestructures energètiques, xarxes de comunicació, sistemes financers i governamentals, entre altres. Un exemple d'aquesta mena d'accions hostils va ser en 2007 quan Rússia va intentar bloquejar virtualment la infraestructura d'internet d'Estònia com a retribució després que el país llevés un centre commemoratiu de la Unió Soviètica que havia existit des de la II Guerra Mundial. Així mateix, Rússia ha emprat aquest tipus de tàctiques en altres països com Geòrgia, Crimea i en les eleccions de 2016 de Trump, afavorint els seus resultats i la publicació favorable d'informació relacionada amb l'expresident. Aquest tipus d'atacs s'usen amb la doctrina teòrica de Valery Gerasimov qui va parlar sobre l'emergència d'una guerra híbrida i com Rússia podia posar-la en pràctica, encara que per descomptat s'ha de recalcar que Rússia nega qualsevol ús de ciberatacs per a obtenir influència política.

La Intel·ligència Artificial

Què és la IA? Quin és el seu rol? Té un límit? Quin punt canviaran les nostres vides? En les següents seccions s'intenta proveir una mica de claredat al "misteri" d'aquestes innovacions i contestar algunes de les preguntes esmentades, ja que solen ser les més comunes entre les persones de qualsevol societat.

Entre acadèmics no existeix una definició única i comuna per a la descripció del que és la Intel·ligència Artificial ni fins a quin punt es poden desenvolupar les seves funcions. Moltes persones es pregunten si és un cercador intel·ligent com ChatGPT, un robot que substituirà als humans en els seus treballs o un conjunt de robots que arribaran a dominar el món; sí, per més distòpic que sembli moltes persones temen al poder de la IA, i amb una certa raó. La definició que li donarem en aquest article a la IA és que és una màquina que pot dur a terme tasques humanes incloent la creació d'altres màquines.

Primer, hem d'entendre que la IA no ens entén. Quan cercadors intel·ligents o assistents virtuals ens donen informació en un xat no són conscients del que fan ni entenen la informació que ens brinden. Aquestes eines funcionen amb una combinació de programació i probabilitats des d'una base de dades que els permet donar-nos el que estem buscant sense poder o haver d'interpretar-ho. Moltes persones es confonen en veure que les respostes dels models de llenguatge com ChatGPT o Baart són tan humanitzades i fins i tot arriben a pensar que es tornen éssers sentientes.

Els canvis en la vida quotidiana de les persones els treballs de les quals no estan relacionats amb la tecnologia encara no estan sent tan radicals, per tant, moltes persones no s'adonen de tot el que ha canviat amb l'existència de la IA. Des de "Robots Assassins" que són els nous soldats utilitzats en les guerres, vigilància extrema en països (no) democràtics, fins a autogeneració d'imatges en l'aplicació de tova Photoshop. Diàriament surten noves funcions o AI específics per a dur a terme una tasca, cada vegada millor i més avançada. Pot la IA conquistar el món? No, la IA està molt lluny de ser tan avançada com en les pel·lícules, ni tan sols és conscient de la seva pròpia existència i la captació de dades no és en viu, cosa que significa que necessita una base de dades introduïda per humans constantment per a poder proveir-nos dades actualitzades. Les persones han donat per descomptat que la IA funciona bé i que per això pot arribar a "dominar-nos" però realment la pregunta que hauríem de fer-nos és: La IA funciona? I si la resposta és sí: En una escala quantificada, quina tan funcional és? En aquesta segona pregunta moltes de les tecnologies no han aconseguit ni el 10% del seu poder ni realitzen tan "bé" el seu treball.

Militarització de la IA

La militarització de la Intel·ligència Artificial (IA) es refereix a l'ús de sistemes de IA amb finalitats militars i en operacions de defensa. Això implica l'aplicació de tecnologies de IA en l'àmbit militar. Les forces armades estan creant sistemes que empren la IA per a diverses tasques, com el comandament i el control, la força letal, el suport a la presa

de decisions i la logística. Aquestes capacitats semblen desenvolupar-se amb major rapidesa que els debats sobre els possibles perills, com si determinats usos causarien problemes de seguretat, alimentarien una carrera armamentística o eliminarien les barreres que impedeixen l'inici d'una guerra nuclear. Hi ha diferents àrees en les quals s'estan usant com a vigilància, ciberseguretat, anàlisi de dades, entre altres.

La IA té potencial per a contribuir a la salut i benestar d'individus, comunitats i estats i fins i tot de contribuir als gols de les ODS del 2030. No obstant això, les seves aplicacions poden afectar la pau i la seguretat internacional, especialment amb la militarització d'eines i sistemes nacionals militars. Majoritàriament aquestes aplicacions estan sent desenvolupades per entitats privades o institucions acadèmiques per a usos principalment civils.

La intel·ligència artificial no està exempta de riscos, especialment quan es tracta de l'exèrcit nacional. L'opinió pública s'interessa pels sistemes d'armes autònomes letals (LAWS) perquè són fàcilment imaginables i plantegen importants problemes de seguretat, jurídics, filosòfics i ètics.

És probable que els exèrcits utilitzin la IA per a ajudar en la presa de decisions. Això podria aconseguir-se proporcionant dades per a guiar la presa de decisions humana o fins i tot assumint tot el procés per complet. Això pot ocórrer, per exemple, en llocs on la comunicació és impossible o en llocs com el ciberespai, on les coses es mouen massa ràpid per a què les persones puguin entendre-les.

La capacitat d'un operador o comandant humà per a exercir un comandament i control directes sobre els sistemes militars pot veure's reforçada a conseqüència d'això, però també és possible que ocorri el contrari. La IA permet la creació de sistemes complexos que poden ser difícils de comprendre, la qual cosa planteja problemes de transparència i de capacitat per a determinar si el sistema funciona com s'espera o es pretén.

Els governs no sols s'utilitzen aquestes aplicacions contra altres estats, sinó que també amb les seves pròpies poblacions per a analitzar comportament de terroristes, amenaces a la seguretat nacional o fins i tot per a vigilància. Un clar exemple és la Xina. En els últims anys, els problemes de privacitat han augmentat també a la Xina. la Xina compta ara amb un dels sistemes de governança de dades més sòlides del món sobre el paper, gràcies a l'aprovació l'any passat de dues importants lleis: la Llei de Protecció de Dades Personals i la Llei de Seguretat de Dades. No obstant això, les forces de seguretat pública xineses estaven altament capacitades per a rastrejar i vigilar a sospitosos de delictes i dissidents del règim fins i tot abans del desenvolupament de sistemes tecnològics d'avantguarda que utilitzen IA.

Les capacitats de vigilància de l'aparell de seguretat pública han millorat ara amb el desplegament de la tecnologia de reconeixement facial. Per exemple, hi ha proves convincents que algunes tecnologies de reconeixement facial s'estan utilitzant a la regió de Xinjiang per a perseguir especialment persones d'ascendència uigur.

els Estats Units està intentant retardar l'avanç de la militarització de la IA a la Xina amb l'estricta implementació de sancions a companyies privades

i regulacions com la Llista d'Entitats o la prohibició d'exportació de Semiconductors, i el mateix intenta fer la Xina en baixar l'exportació de metalls imprescindibles per a la producció de tecnologies tant per a energies renovables com per a qualsevol tipus d'aplicacions tecnològiques.

***Font**: New York Times*

ChatGPT

ChatGPT és un model de llenguatge de la IA. Per a molts és una eina realment útil, però el que no es té en compte és que pot donar informació falsa, dolents o fins i tot perillosos consells sobre accions com realitzar explosius, manufacturar drogues il·legals i participar en altres activitats il·legals.

Encara que és crucial assenyalar que les directrius de Chat GPT prohibeixen la generació de continguts nocius, la falta de control total sobre els resultats suscita preocupació per la possibilitat que es produeixin desinformació i danys. A més, la incapacitat de Chat GPT per a verificar la informació o comprovar els fets de les seves respostes també pot donar lloc a consells inexactes. El conseller delegat de OpenAI, Sam Altman, s'enfronta a una audiència al Senat dels EUA sobre Intel·ligència Artificial (IA). La seva empresa va crear el ChatGPT. L'eina ha arribat a ser tan avançada que pot escriure redaccions, guions, poemes i resoldre la codificació de programari de la mateixa forma que ho faria un humà.

Membres del Senat busquen les possibles amenaces que la IA pot suposar per als humans en el futur i si ha de ser regulada pel govern. Experts com el Dr. Geoffrey Hinton han manifestat recentment la seva preocupació pel ràpid desenvolupament de la nova tecnologia.

La senadora Blumenthan va preguntar a Altman si creu que és bona idea explicar als usuaris la fiabilitat dels continguts que utilitzen. Va suggerir que els continguts rebessin "targetes de puntuació" per a reflectir la seva fiabilitat. Altman està d'acord i creu que les auditories independents són importants. Creu que, encara que hi ha un element d'error quan s'utilitza tecnologia de IA, es pot crear un altre tipus de programari per a detectar errors i precisió. A més, hi ha grans motivacions per a reduir la velocitat de l'avanç de la IA. La IA utilitza la capacitat de

resoldre problemes basant-se en la informació que se li proporciona ja sigui subjectiva o objectiva.

OpenAI és l'empresa que està darrere de ChatGPT. Va ser fundada en 2015 amb 1.000 milions de dòlars de suport amb inversors de Silicon Valley. Xat GPT-4 és la nova versió de ChatGPT. Pot reconèixer i explicar imatges. La seva capacitat pot ser més sofisticada i oferir suggeriments de receptes a partir de fotos d'ingredients, per exemple.

No obstant això, no tot és color de rosa. En un acte recent durant la seva visita a l'Índia, Altman va declarar: "Em fio menys de les respostes generades per ChatGPT que de qualsevol altra persona en la Terra". En resum, encara que ChatGPT i altres aplicacions de la IA han vingut per a canviar el nostre dia a dia, s'ha enfrontat a crítiques per la seva tendència a oferir respostes inexactes. Se sap que en múltiples ocasions al·lucina i crea escenaris ficticis.

Posició de les Nacions Unides

Les NU defensa el desenvolupament de la IA com una eina ètica i per al desenvolupament sostenible de l'ésser humà, ajudant-nos a complir els ODS i a canviar les regles del joc d'una forma positiva. No obstant això, l'Alt Comissionat de les Nacions Unides per als Drets Humans, Volker Türk, i en 2021 també Michelle Bachelet, denuncien estrictament els perills de la IA i la necessitat de la seva regulació abans de continuar el seu desenvolupament. El 8 de maig Türk va donar un discurs en el qual esmenta l'increment en la propagació dels discursos d'odi i de desinformació en l'espai digital, així com el possible ús de la IA per a reprimir la llibertat d'expressió. A més, així com es va esmentar anteriorment, va denunciar la desaparició del dret a la intimitat i la bretxa digital que amplia les desigualtats. Donada la importància de la utilització i creació de la IA s'està desenvolupant una proposta per a un **Pacte Digital Mundial** per a presentar-lo aquest 2024 en la Cimera del Futur basat en un procés inclusiu i transparent, que vol atendre les necessitats d'aquelles persones a les quals les innovacions digitals beneficien tant com a les que no. Així mateix, va ressaltar la responsabilitat del sector privat en el respecte dels drets humans, esmentant els Principis Rectors de les Nacions Unides sobre les Empreses i els Drets Humans com una guia. També es destaca el paper dels governs en la regulació de les activitats del sector privat i a garantir l'accés universal a Internet. S'emfatitza la importància de la transparència, la rendició de comptes i l'ètica en el desenvolupament de la intel·ligència artificial, així com la necessitat de prevenir possibles repercussions negatives.

El **Pacte Digital Mundial** es refereix a un marc proposat per a abordar els desafiaments i oportunitats associats amb la tecnologia digital i garantir que el seu desenvolupament i ús estiguin guiats pels principis dels drets humans. També, cerca establir normes i principis comuns que regeixin el comportament dels actors involucrats en l'àmbit digital, incloent-hi governs, empreses, organitzacions de la societat civil i altres actors rellevants. A més, promourà un enfocament inclusiu i transparent, assegurant la participació d'estats, individus i el sector privat en el seu

desenvolupament i aplicació. Intentarà equilibrar l'ús i els beneficis de la tecnologia digital amb la protecció dels drets humans, abordant temes com la privacitat, la llibertat d'expressió, la igualtat d'accés, la seguretat en línia i la rendició de comptes. L'objectiu no està 100% decidit però serà per a establir un marc universal i vinculant que ajudi a orientar les polítiques, regulacions i pràctiques relacionades amb l'àmbit digital, amb la finalitat de fomentar un entorn digital segur, inclusiu i respectuós dels drets humans a tot el món.

Segons Türk una vegada hagin "línies vermelles reguladores", transparència, col·laboració entre actors i es mantinguin els drets humans com la prioritat de la innovació digital es construirà una governança adequada per a un futur digital saludable i ajudarem en la consecució dels Objectius de Desenvolupament Sostenible.

Respecte a les diferents amenaces que presenta la militarització de la IA el Secretari General de l'ONU, António Guterres, en el seu programa per al desarmament "Assegurar el nostre futur comú", subratlla la necessitat que els Estats membres de l'ONU comprenguin millor la naturalesa i les implicacions de les tecnologies noves i emergents amb possibles aplicacions militars i la necessitat de mantenir el control humà sobre els sistemes d'armament. Subratlla que el diàleg entre els governs, la societat civil i el sector privat és un complement cada vegada més necessari dels processos intergovernamentals existents.

Nota conclusiva

Els atacs cibernètics realitzats per grups terroristes poden comprometre la seguretat de sistemes informàtics, xarxes de telecomunicacions termes de protecció dels drets dels individus. Els drets digitals, com el dret a la privacitat, la seguretat i la integritat, poden ser vulnerats per aquests atacs. i infraestructures polítiques, econòmiques o socials. És fonamental promoure l'educació digital i fomentar l'ús responsable de la tecnologia per a salvaguardar els drets humans i prendre mesures preventives contra el ciberterrorisme. A més, s'ha observat una creixent militarització de la intel·ligència artificial (IA) en l'àmbit de defensa i seguretat. L'aplicació de la IA en operacions militars planteja preocupacions sobre la transparència, el control i els possibles riscos per a la pau i la seguretat internacional. En general, tant el ciberterrorisme com la militarització de la IA plantegen desafiaments significatius en termes de seguretat, drets individuals i ètica. És necessari abordar aquests desafiaments a nivells nacionals i Internacionals amb regulacions adequades, educació digital i una major consciència sobre els riscos i beneficis d'aquestes tecnologies.

Yuliana Vázquez Hernández
Estudianta de Global Governance, Economics & Legal Order
ESADE

Fonts de referencia:

- Bachmann, M., & Gunneriusson, H. (2016). Hybrid wars: The 21st-century's new threat. Scientia Militaria - South African Journal of Military Studies, 44(2), 1-20. https://ung.edu/institute-leadership-strategic-studies/_uploads/files/bachmann-gunneriusson-hybrid-wars-16-sep-2016-scientia-militaria.pdf

- Big Data and Security (2019). The AI surveillance symbiosis in China: Joint development of military-civil fusion in national strategic emerging industries. Center for Strategic and International Studieshttps://bigdatachina.csis.org/the-ai-surveillance-symbiosis-in-china/

- Firstpost (2022, 19 de enero). Sam Altman, the inventor of ChatGPT, doesn't trust anything that his AI chatbot says. https://www.firstpost.com/world/sam-altman-the-inventor-of-chatgpt-doesnt-trust-anything-that-his-ai-chatbot-says-12714112.html

- Lavanguardia.com (2020, 10 de diciembre). La economía geopolítica a cuatro patas de la inteligencia artificial. Vanguardia Dossier. https://www.lavanguardia.com/vanguardia-dossier/20201210/49848571042/economia-geopolitica-patas-inteligencia-artificial.html

- OHCHR. (2023, mayo 15). Global digital compact must be guided by human rights, says Turk. Recuperado de https://www.ohchr.org/es/statements/2023/05/global-digital-compact-must-be-guided-human-rights-says-turk

- OHCHR. (2021, septiembre 1). Artificial intelligence risks privacy and demands urgent action, says Bachelet. Recuperado de https://www.ohchr.org/es/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet

- OHCHR. (2023, junio 1). New and emerging technologies need urgent oversight and robust transparency, says OHCHR. Recuperado de https://www.ohchr.org/es/press-releases/2023/06/new-and-emerging-technologies-need-urgent-oversight-and-robust-transparency

- Pool Marketing (2022, 27 de febrero). The dark side of ChatGPT has real-world consequences. https://poolmarketing.medium.com/the-dark-side-of-chatgpt-has-real-world-consequences-90bff03a00bf

- Stimson Center (2020). The Militarization of Artificial Intelligence. https://www.stimson.org/2020/the-militarization-of-artificial-intelligence/

- Tokio School (s.f.). Inteligencia Artificial y Política. https://www.tokioschool.com/noticias/inteligencia-artificial-politica/

- United Nations (2020). Towards ethics in artificial intelligence. The United Nations Chronicle. https://www.un.org/en/chronicle/article/towards-ethics-artificial-intelligence

- World Summit AI (2023, 14 de junio). OpenAI CEO faces US Senate hearing.

Publicat per:

Asociación para las Naciones Unidas en España
United Nations Association of Spain

Amb el suport de:

Generalitat de Catalunya

Associació per a les Nacions Unides a Espanya
United Nations Association of Spain

JUNIO 2023