Le vrai danger avec #ChatGPT

Les gens devraient regarder cette vidéo YouTube intitulée “Le vrai danger avec #ChatGPT” car elle explique les risques liés à l’utilisation des chatbots GPT-3. Ces chatbots sont des systèmes de conversation automatisés qui peuvent imiter le langage humain et sont de plus en plus populaires. Cependant, cette vidéo explique en quoi leur utilisation peut être dangereuse et comment ils peuvent être utilisés à des fins malveillantes.

This video transcription discusses the potential dangers of the recently released chatbot GPT. It explains how the chatbot’s popularity has caused massive investments in the development of similar algorithms, which can be used by cybercriminals to steal billions of dollars. It also explains how Google has developed similar chatbots, but has chosen not to make them publicly available due to potential risks. The video transcription concludes by urging the public to be aware of the potential dangers of chatbot GPT and other similar algorithms.

Source : UC0NCbj8CxzeCGIF6sODJ-7A | Date : 2023-01-23 18:00:22 | Durée : 00:21:30

➡ Accéder à CHAT GPT en cliquant dessus

Voici la transcription de cette vidéo :

Vous le savez certainement depuis quelques mois un chatbot appelé chat GPT a été rendu accessible au grand public et sa spectacularité a conduit tous les grands médias à en parler certains parlant même de révolution ou de technologie de rupture et bien souvent avec beaucoup d'enthousiasme et oui je Porte des gants parce que je filme ça chez moi et comme il y a pas le choix j'ai fait vachement froid chez moi ceci étant de nombreuses voix critiques se sont soulevées comme vous pouvez vous en rendre compte en lisant par exemple la page wikipédia de chaque GPT et si vous

Faites cet exercice vous verrez que parmi les critiques il y a un certain les Nguyen ou un angle pourtant le grand danger de chaque GPT à Meyzieu n'est pas listé dans cette page wikipédia et il n'est quasiment jamais cité dans les médias à part ceux qui m'ont invité à

Parler de ce danger et pour vraiment clarifier ce danger je vais m'appuyer sur un chiffre 6000 milliards de dollars 6000 milliards de dollars 6000 milliards de dollars c'est d'après le Sénat français une estimation raisonnable du revenu annuel du cybercrime milliards de dollars c'est le double du

PIB de la France et ses quatre fois plus que Google Amazon Facebook Apple et Microsoft combiné or on peut estimer que chaque GPT a coûté quelques dizaines de millions peut-être quelques centaines de millions pour être conçu notamment à cause de la facture d'électricité mais aussi à cause des salaires des

Ingénieurs et de la collecte éthiquement douteuses des données pour éduquer chaque GPT comme on en a parlé chez Monsieur fille mais surtout vu ce copenhay a partagé pété ne semble pas s'appuyer sur des techniques novatrices en fait il existe toute une jungle d'algorithmes de langage similaire dont

Certains comme lambda et palme de Google dont les progrès sont sûrement comparables et d'autres encore qui sont open source comme Dumble de hogging face mais surtout la sur médiatisation

des prouesses de chaque GPT a déjà amplifié les investissements déjà massifs dans le développement de ces technologies voire à convaincre certaines entreprises de

Réduire leur seuil de sécurité avant de déployer ces technologies ce qui va certainement conduire à des algorithmes bien plus spectaculaires encore que chaque GPT dans les années voire dans les mois qui viennent or les moyens actuels légaux financiers et humains pour auditer et réguler ces technologies sont extrêmement déficients et les

Lobbies industriels s'appuient souvent sur le succès de chaque GPT et la course à la performance pour dénigrer les appels à la régulation qui plus est ce que chaque GPT a montré à toute l'industrie du cybercrim c'est à quel point ces algorithmes de langage pouvaient booster leur business en automatisant l'écriture de logiciel

Malveillant les attaques par phishing les arnaques en ligne la désinformation le cyber-harcèlement et les appels à la haine entre autres enfin et surtout chaque GPT est un dangereux cool washing des intelligences artificielles et aide à distraire toute la société de ses applications les plus dangereuses que ce soit pour les claviers intelligents qui

Lisent tout ce que vous tapez sur vos téléphones la publicité qui exploite ses données et d'autres pour optimiser les appels à la surconsommation des entreprises privées ou la recommandation algorithmique de contenu qui bien plus que Google Search ou chaque GPT est devenu le portail principal à travers

Lequel les humains accèdent web en quand on me demande si chaque GPT il pourra remplacer Google Search j'ai surtout envie de répondre que l'algorithme de Tik Tok a déjà largement remplacé Google Search bref à bien y réfléchir le plus grand danger avec chaque GPT ce n'est

Pas chat GPT lui-même c'est tout ce qui l'impliquent pour

l’écosystème du développement des intelligences artificielles de Chuck Nora pour bien comprendre à quel point ce serait une erreur de penser chaque GPT de manière isolée il est important de prendre un peu de recul sur le développement de telles algorithmes en

Fait depuis 2017 il y a un article de recherche de Google publié à norrips c’est l’une des plus grandes conférences en machine learning les algorithmes de langage s’appuient sur une même architecture appelée le transformer depuis ses algorithmes n’ont cessé de progresser un rythme spectaculaire si bien que les performances de tchat GPT

Ne montrent personnellement pas vraiment surpris en effet chaque année on entraînant un algorithme dix fois plus gros que le précédent et en l’alimentant de 10 fois plus de données les équipes de recherche des groupes privées n’ont cessé de montrer que les modèles ainsi créés gagner drastiquement en spectacularité bref personnellement je

N’ai pas tout à fait l’impression que chaque GPT est une rupture et encore moins qu’il s’agit du dernier mot à ce sujet on est dans une phase de croissance exponentielle dans la complexification de ces algorithmes rendu notamment possible par l’optimisation des machines pour les calculs spécifiques de l’architecture

Dite du transformer mais aussi et surtout par l’in investissement en spectaculaire dont le développement de tels produits en particulier le facteur limitant aujourd’hui à la spectacularité de ses algorithmes n’est plus une innovation algorithmique révolutionnaire même s’il faut encore souvent combiner plein de petites astuces le facteur limitant c’est surtout l’ingénierie des

Machines à calculer la collecte de données massives et surtout la facture d’électricité pour faire les calculs nestiment ainsi que les meilleurs modèles de langage coûtent des

millions de dollars en électricité en tout cas le modèle Bloom conçu par roging face pour le projet ouvert big science rapporte à

Avoir dépensé de à 5 millions de dollars en électricité pour chaque j'ai répété ils ont peut-être mis les bouchées doubles voire les bouchers x 10 voir peut-être plus encore ou quelqu'un on pourrait parler de dizaines voire de centaines de millions de dollars mais probablement pas beaucoup plus vu que

Open high n'avait reçu qu'un milliard de dollars d'investissement de Microsoft bref ce que je veux surtout dire c'est que la conception d'algorithmes de langage et surtout une histoire d'argent aujourd'hui en tout cas si on néglige les problèmes de sécurité qui eux nécessitent beaucoup plus de développement à la fois au niveau de la

Recherche et de l'ingénierie par ailleurs si jamais il s'agissait davantage une affaire d'expertise notamment parce qu'il y a encore pas mal d'astuces techniques à trouver Google semble en fait mieux placé copenhae puisque ce sont beaucoup plus eux qui sont derrière les principales avancées dans le domaine à la fois avec

L'architecture des Transformers mais aussi avec des nouvelles machines à calculer dédiées comme les Tenser possessing unit ou TPU ou encore avec des innovations plus récentes comme les switch Transformers ou pas Waze en fait Google a développé des chatbots spectaculaires avant chat GPT à savoir lambda et palme mais ils ont préféré ne

Pas les rendre accessibles au grand public notamment pour éviter tout retour de bâton en fait ce qui se passe et sans doute que Google a surtout beaucoup plus à perdre en termes d'image que Microsoft et Open height et ça me semble surtout être la principale raison pour laquelle

Ils n'ont pas misé sur une euphorie en la rendant public comme ce café openerai mais Google et openia ne sont absolument pas

les seuls à développer de tels algorithmes suite à l'euphorie autour de ces modèles de langage il y a eu de nouveaux investissements massifs dans ces technologies et avec notamment

L'avènement de solutions open source comme il faut s'attendre à ce que dans les années à venir accéder à des modèles de langage très puissant se fassent à un coût beaucoup plus raisonnable qu'aujourd'hui voir que ça devienne facile pour des acteurs malveillants qui pourront affiner ces modèles comme bon

Leur semble dès lors qu'importe que chaque GPT aide et mesure de sécurité ou non en provoquant une euphorie ils ont essentiellement garanti l'apparition imminente de modèles de langage bon marché extrêmement puissant et facilement reprogrammable par le cybercrim pour que celui-ci continue à voler des milliers de milliards de

Dollars qui permettent des hôpitaux des voitures et des systèmes bancaires en danger en particulier dans ce cadre les algorithmes à la chaîne GPT pour être particulièrement dévastateur notamment parce que les cybercriminels s'appuient souvent avant tout sur le langage pour piéger leur victime le cybercrim justement parlons-en pour commencer quand on tombe par cybercrimes

En gros on parle d'utiliser des outils du numérique pour commettre des infractions des délits voire des crimes et il y a malheureusement une énorme diversité de telle pratique je vous en propose une petite classification ici qui est très loin d'être exhaustive et je vous renvoie notamment vers Wikipédia

Pour une liste plus complète pour commencer il y a les arnaques typiquement il y a le fameux coup du prince nigérian qui demande une aide financière qui sera récompensée ultérieurement mais ça c'est un peu l'arnaque de l'an 2000

aujourd’hui des arnaques similaires mais beaucoup plus sophistiqués ont été développés comme

Par exemple les love scams qui consiste à séduire des célibataires en ligne souvent pendant des mois avant de demander de l’aide financière natax similaire appelée l’attaque au faux supports téléphoniques consiste à faire croire à sa victime que son ordinateur est compromis et qu’il lui faut urgemment appeler un numéro d’aide sauf

Que c’est justement au moment de l’appel que l’arnaque est vraiment lieu par exemple parce que l’attaquant demande alors à l’utilisateur de se connecter à son compte en banque en ligne en écrivant le mot de passe que l’attaquant pourra ainsi noter et si vous voulez en savoir plus sur ce genre d’attaque je

Vous recommande vivement cet excellente en quête de MyCode globalement récupérer vos codes d’accès à des sites Web est une énorme activité du cybercrim et l’une des manières les plus efficaces pour y parvenir et l’attaque par hameçonnage aussi appelé attaque par phishing celles-ci est consiste typiquement à faire visiter une page qui

Ressemble comme deux gouttes d’eau à la page d’enregistrement d’un site très connu comme Gmail ou Facebook sauf que le mot de passe que vous rentrez sur cette page est envoyé non pas à Google ou à Facebook mais est envoyé directement aux machines de l’attaquant et alors quand il s’agit d’un compte

Personnel c’est déjà très dangereux notamment parce que l’attaquant peut ensuite se faire passer pour vous pour demander de l’aide financière à vos proches mais quand il s’agit de votre compte professionnel ceci peut mettre votre entreprise en danger surtout si vous travaillez dans une entreprise de petite taille en particulier l’une des

Attaques qui se normalisent de plus en plus sur les entreprises c’est d’exploiter de tels accès au système

d’information de l’entreprise pour le paralyser en chiffrant par exemple toutes les données utiles au fonctionnement de l’entreprise comme les informations des clients nécessaires pour leur envoyer des factures les attaquants sont ensuite typiquement

Demander une rançon pour rétablir le système d’information on parle alors d’attaque par ransomware et comme on parle ici John Oliver des milliers d’hôpitaux ont déjà été hackés ainsi et ont parfois dû refuser des clients en état critique parce que le système d’information était paralysé de façon terrifiante les attaques par ransomware

Se démocratise si bien qu’à marcher de ransomware Asus a émergé ou n’importe qui peut payer pour lancer sa propre attaque sans avoir à coder quoi que ce soit sauf que dans un contexte de guerre entre superpuissance un star de la Russie qui a cherché à paralyser le système électrique ukrainien à l’aide de

Bombe les intérêts à paralyser des industries critiques d’ennemis vont bien au-delà du simple profit financier dès lors il faut craindre une cybergure catastrophique voire notamment ainsi les outils nécessaires pour effectuer une attaque à grande échelle de Vienne abordable un très grand nombre de groupes il faudrait de plus en du

Screindre des attaques de cyber terrorisme ceci étant une grosse partie du super clean et beaucoup plus vicieux et discret en particulier les fraudes de publicité d’identité et d’attribution consiste à typiquement concevoir voler ou racheter un grand nombre de fauconstes pour ensuite produire une quantité massive de désinformation pour

Faire gonfler la popularité les prix ou les cours de certains produits pour amplifier le taux de cliquer donc de recommandations de certains contenus vous pour signaler massivement certains contenus critiques de gouvernement de

partis politiques ou d’entreprises privées ces faux comptes aujourd’hui souvent contrôlées par des fermes de

Troll ou si appeler usine à clic sont aussi utilisés pour produire des shits Storm et harceler massivement certaines cibles ce même harcèlement peut aussi abuser de Deep fake pour nuire à l’image de ses cibles voire alors bien-être mental notamment en produisant des deep fake pornographiques love scan faut supporter téléphonique hameçonnage

Hansomware siberger cyberies ferme un clic vague de harcèlement voir tes informations et appelle à la haine cette liste de cybercrim est loin d’être exhaustive mais elle est déjà extrêmement terrifiante et surtout très clairement des algorithmes de langage comme chaque GPT vont énormément faciliter la tâche de ceux qui veulent

Profiter de ces attaques illégales et ça va du coup rendre beaucoup plus difficile la tâche des professionnels de la cybersécurité normaliser le coûting de chaque GPT sans parler avec insistance des dangers civilisationnels de la démocratisation des algorithmes de langage et des besoins urgents de Moyaux monumentaux pour protéger les sociétés

Contre le cybercrime c’est rendre toute la population plus vulnérable encore à des disruptions majeures des systèmes d’information critiques dont nos sociétés dépendent tant qu’il s’agissent des hôpitaux du réseau électrique du système bancaire ou du tissu de petites et moyennes entreprises mais à quel point son marché est-il grand faut-il vraiment croire que les

Avancées en IA seront beaucoup plus souvent exploités par des acteurs malveillants que pour des fins nobles comme des applications médicales et pour sauver des vies non seulement l’ampleur de ce marché du cyberclim est une énorme mute news mais ce qu’on mesure sans doute tout aussi mal c’est sa croissance

Spectaculaire estimez un coup de 3000 milliards de dollars en 2015 par Cyber Security 24 il semble avoir atteint 6000 milliards de dollars en 2021 il pourra atteindre 10 000 milliards en 2025 à titre de comparaison d'après mes recherches que j'avoue être un peu sommaire et donc auquel je ne suis pas

Sûr de faire entièrement confiance le marché illégal des armes ne représenterait que 60 milliards de dollars par an le marché était drogues illégal lui et estimé à 500 milliards de dollars par an selon certaines sources alors que le marché de la contrefaçon dépasserait 1000 milliards de dollars

Tout ça pour dire que les individus louchent enfin la loi pour s'enrichir ont en fait tout intérêt à investir davantage dans le cybercrim que dans ces autres marchés légaux devenus beaucoup trop classique et visiblement ils sont énormément à s'y être mis oui car pour être clair vu l'échelle des enjeux et

Des profits potentiels le cybercules est très loin d'être une affaire de gamins isolé sur leur machine dans le garage de leurs parents il s'agit d'un véritable business d'un crime organisé avec des fournisseurs et des clients par exemple en 2012 et selon Wikipédia la menace prédominante du web était non pas un

Virus mais un kit que les clients pouvaient acheter pour eux-mêmes attaquer leur victime de la même manière vous avez peut-être entendu parler de Pegasus qui revendu à des états à défendre de surveillance en fait dès 2015 Ginny rometti alors PDG d'IBM affirmait que je cite le cybercrim et la

Plus grande menace pour toutes ces professions toutes les industries et toutes les entreprises du monde en 2017 un expert en cybersécurité sondait son audience Twitter pour voir à quel point elle était d'accord avec ce constat la majorité approuvait le message de remetty imaginez si les voitures le

réseau électrique les hôpitaux ou le

Système bancaire mais aussi tout simplement les systèmes de réservation de la SNCF ou encore les bases de données gouvernementales étaient tout à coup paralysé par des acteurs malveillants qui exigeraient des rançons énormes pour rétablir le fonctionnement de ces systèmes ou si des milliards de Deep fake personnalisés demandaient à

Chacun de vos concitoyens d'effectuer des actions obscures sur le web en se faisant passer pour leurs proches leurs collègues voir pour leur boss please any of the messenger everything Unito verify face à ce discours réaliste du paysage des algorithmes vraiment déployés aujourd'hui les enthousiastes de l'IA se précipitent souvent pour minimiser la

Responsabilité des IA beaucoup vont ainsi comparer ces algorithmes à des couteaux oui les algorithmes peuvent être utilisés pour tuer mais faut-il les interdire pour autant lors d'un meurtre au couteau la faute ne revient-elle pas à l'humain qui manipule le couteau ce dont j'ai essayé de vous convaincre ici

C'est que la comparaison entre chaque GPT et un couteau est en fait très mal à droite surtout d'un point de vue conséquentieliste en particulier les conséquences probables du développement d'un nouveau couteau surtout dans une société où il y a déjà pas mal de couteaux assez comparables c'est conséquences du nouveau couteau me

Semble absolument pas comparable par rapport aux éditions aux conséquences du développement et du déploiement précipité de chaque GPT qui normalisent et démocratise le développement et l'utilisation de ces outils qui dans les mois qui viennent et j'espère vous en avoir convaincu seront plus probablement utilisés à des fins de cybercrim qui a

Des fins utiles au bien-être et à la sécurité du plus grand nombre autrement dit le problème du développement et du

déploiement précipité me semble contextuelle dont le monde dans lequel on vit avec des contraintes écologiques et économiques et surtout avec la prolifération à contrôlée du cybercrime et avec l'instabilité géopolitique à

L'échelle mondiale accélérer le développement d'algorithmes surpuissant à tout faire et sans préoccupation pour leur sécurité ça me paraît très nettement beaucoup plus dangereux que freiner se développements et investir massivement en particulier dans leur régulation d'autant que à part dans le domaine de l'art les applications bénéfiques à l'humanité de ce genre de

Technologie me semble très limité et très peu convaincante autrement dit la balance risque bénéfice du développement des algorithmes de langage comme chaque GPT ça me semble très largement penché en faveur des risques et pas des bénéfices malheureusement cette balance risque bénéfice est souvent en très loin de l'esprit de beaucoup le Cool washing

De l'IA notamment à la reliant trop souvent à la science-fiction ou à l'art mais aussi l'insistance à parler de problèmes très secondaires à mes yeux comme le rôle de l'humain l'empreinte carbone de ces technologies qui est non négligeable mais qui n'est pas non plus délirant ou le fait que ces technologies

Ne pas encore conçu sur le territoire européen fait de soulever ses préoccupations très secondaires ça me semble avoir conduit à un grave manque de méfiance du grand public mais aussi des chercheurs des journalistes et des politiciens envers le développement de ces technologies dans le contexte actuel ou le cybercrim domine ces algorithmes

Sont extrêmement dangereux il faudrait urgemment investir beaucoup plus dans leur régulation leur audit voire leur interdiction or ça malheureusement ça nécessite non seulement des lois mais ça requiert plus encore des investissements

beaucoup plus importants dans des agences de cybersécurité comme l'Agence nationale de la sécurité des systèmes d'information l'annecy mais aussi dans

La recherche publique sur la cybersécurité ne recherche publique qui je pense devrait largement prioriser le recrutement de chercheurs orientés sécurité par opposition à des chercheurs qui sont très bons dans l'art d'optimiser des systèmes d'apprentissage sans attention alors sécurité après tout le cybercules n'est pas un problème individuel si demain des employés de

Google de Tesla d'EDF ou de la Société Générale se font hacker et si cela permet aux attaquants d'A et de paralyser des systèmes d'information critiques de ces multinationales dont les produits sont utilisés par tout le tissu économique et la population alors les conséquences seraient catastrophiques pour tous pour tous y

Compris moi-même même si j'ai fait très attention à ma propre cybersécurité le manque d'attention à cybersécurité des seins peut menacer toute la sécurité de toute la société dès lors une réponse collective et nécessaire et les développeurs chercheurs journalistes politiciens et juristes ont un rôle critique dans cette réponse aujourd'hui encore très largement déficiente

D'ailleurs un autre très gros danger avec l'attention démesurée donnée à open heigh ça me semble être l'inattention que cela provoque pour les algorithmes les plus dangereux qui restent à mes yeux les algorithmes de ciblage publicitaires et de recommandations de contenu ces algorithmes sont très largement déployés et ont déjà provoqué

Des cas sociaux aux États-Unis au Brésil et au Royaume-Uni et des génocides au milieu de mare en Éthiopie et peut-être bientôt en Inde ces autres intelligences artificielles qui sont beaucoup moins spectaculaire mais tout aussi sophistiqué

que chaque GPT sont aussi beaucoup plus dangereux pour la société

Mais il me semble aussi avoir déjà très clairement violé beaucoup de lois malheureusement la justice manque aujourd'hui de moyens et d'attention pour prioriser l'application de la Loi à ses entités par exemple pour appliquer les régulations sur la publicité ou publicité ciblées en ligne pour punir la diffusion massive de contenu illégaux

Dont Google et d'autres profitent tant et vu à quel point ce manque de moyens de la justice me semble difficile à combler dans un avenir proche je trouverai cela judicieux d'imposer des lois simples à faire appliquer comme hashtag taxons la pub de la même manière de manière très concrète alors que des

Milliards de fonds philanthropiques ont été versés à des entreprises comme Open et high pour concevoir des algorithmes de langage des alternatives dédiées à l'éthique à la sécurité et à la gouvernance collaborative des algorithmes les plus dangereux du web comme tournesol manque aujourd'hui gravement de dons et de visibilité au

Niveau de la recherche et des médias dans le cas de tournesol après notamment presque trois ans on a juste de quoi payer un salaire de développeur or même avec les meilleures idées qui soient c'est très compliqué avec un seul employé de concurrencer open air Google ou Tik Tok d'autant que le développement

D'algorithmes vraiment sécurisé est en fait souvent plus sophistiquée encore en tout cas sur le plan mathématique que le développement de spectaculaire comme ceci étant dit au niveau de la recherche en tout cas depuis quelques années les problématiques d'éthiques de sécurité et de gouvernance gagne en importance mais

Vous pouvez nous aider à accélérer cette tendance en utilisant notre extension tournesol pour Chrome Firefox contribuant à la

plateforme pour identifier plus de vidéos de top qualité et surtout en promouvant tournesol autour de vous et des journalistes c’est en encourageant ce genre d’initiative que vous pourrez pousser les

Technologies à être conçu avec davantage de considération pour la sécurité et le bien-être du plus grand nombre