由网络安全提供支持的人工智能

(Yóu wǎngluò ānquán tígōng zhīchí de réngōng zhìnéng)

描述：技术**正在迅速**发**展，世界正在被新的**趋势**和机遇所塑造。人工智能 、物**联网 、**云**计**算、增**强现实**等一系列技**术**正在**发**生令人**兴奋**的**发**展。这些新**兴**技**术**有其自身的**优势**和挑**战。让**我**们**看看人工智能是如何由网**络**安全**驱动**的。**

Miáoshù: Jìshù zhèngzài xùnsù fāzhǎn, shìjiè zhèngzài bèi xīn de qūshì hé jīyù suǒ sùzào. Réngōng zhìnéng, wù liánwǎng, yún jìsuàn, zēngqiáng xiànshí děng yī xìliè jìshù zhèngzài fāshēng lìng rén xīngfèn de fǎ zhǎn. Zhèxiē xīnxīng jìshù yǒu qí zìshēn de yōushì hé tiǎozhàn. Ràng wǒmen kàn kàn réngōng zhìnéng shì rúhé yóu wǎngluò ānquán qūdòng de.

网络安全

网络安全是保护、预防和检测不需要的攻击或未经授权的访问的过程。网络安全是组织用来保护其网络资产的人员、政策、流程和技术的组合。 网络安全针对业务定义的级别进行了优化，在资源需求与可用性/可管理性以及风险抵消程度之间取得平衡（高德纳 词汇表）。随着对技术的依赖和使用的增加，网络威胁和攻击的影响也在增加。网络安全实践可防范网络钓鱼、拒绝服务 、恶意软件攻击 等威胁。起源于任何商业空间甚至个人的内部或外部。

Wǎngluò ānquán

Wǎngluò ānquán shì bǎohù, yùfáng hé jiǎncè bù xūyào de gōngjí huò wèi jīng shòuquán de fǎngwèn de guòchéng. Wǎngluò ānquán shì zǔzhī yòng lái bǎohù qí wǎngluò zīchǎn de rényuán, zhèngcè, liúchéng hé jìshù de zǔhé. Wǎngluò ānquán zhēnduì yèwù dìngyì de jíbié jìnxíngle yōuhuà, zài zīyuán xūqiú yǔ kěyòngxìng/kě guǎnlǐ xìng yǐjí fēngxiǎn dǐxiāo chéngdù zhī jiān qǔdé pínghéng (gāo dé nà cíhuì biǎo). Suízhe duì jìshù de yīlài hé shǐyòng de zēngjiā, wǎngluò wēixié hé gōngjí de yǐngxiǎng yě zài zēngjiā. Wǎngluò ānquán shíjiàn kě fángfàn wǎngluò diàoyú, jùjué fúwù, èyì ruǎnjiàn gōngjí děng wēixié. Qǐyuán yú rènhé shāngyè kōngjiān shènzhì gèrén de nèibù huò wàibù.

此外，根据数字杂志- **源**讯公司 报告（2023 **年**），**有各种**类别的网络威胁，例如：

勒索软件威胁：它是一种恶意软件，旨在加密受害者的文件并要求支付解密密钥的费用。

供应链威胁：它针对有权访问组织计算机系统和数据的供应商和供应商的网络和系统。这些威胁可能会导致数据丢失、金钱损失和声誉受损。

云威胁：它针对云计算环境，包括在具有互联网访问权限的第三方服务器上存储、处理、访问数据和应用程序。

移动威胁：它针对存储敏感数据并用于个人和专业目的的移动设备。

Cǐwài, gēnjù shùzì zázhì- yuán xùn gōngsī bàogào (2023 nián), yǒu gè zhǒng lèibié de wǎngluò wēixié, lìrú:

Lèsuǒ ruǎnjiàn wēixié: Tā shì yī zhǒng èyì ruǎnjiàn, zhǐ zài jiāmì shòuhài zhě de wénjiàn bìng yāoqiú zhīfù jiěmì mi yào de fèiyòng.
Gōngyìng liàn wēixié: Tā zhēnduì yǒu quán fǎngwèn zǔzhī jìsuànjī xìtǒng hé shùjù de gōngyìng shāng hé gōngyìng shāng de wǎngluò hé xìtǒng. Zhèxiē wēixié kěnéng huì dǎozhì shùjù diūshī, jīnqián sǔnshī hé shēngyù shòu sǔn.
Yún wēixié: Tā zhēnduì yún jìsuàn huánjìng, bāokuò zài jùyǒu hùliánwǎng fǎngwèn quánxiàn de dì sānfāng fúwùqì shàng cúnchú, chǔlǐ, fǎngwèn shùjù hé yìngyòng chéngxù.
Yídòng wēixié: Tā zhēnduì cúnchú mǐngǎn shùjù bìngyòng yú gèrén hé zhuānyè mùdì de yídòng shèbèi.

随着技术的发展并在我们的日常生活中变得越来越普遍，网络攻击的可能性也在增加。然后，技术专家设计了防御网络攻击的方法。这些网络安全解决方案可以根据其功能进行分类，例如网络安全、数据安全、应用程序安全、云安全、访问管理等。这些解决方案可保护敏感信息，同时保护数据机密性。

Suízhe jìshù de fǎ zhǎn bìng zài wǒmen de rìcháng shēnghuó zhōng biàn dé yuè lái yuè pǔbiàn, wǎngluò gōngjí de kěnéng xìng yě zài zēngjiā. Ránhòu, jìshù zhuānjiā shèjìle fángyù wǎngluò gōngjí de fāngfǎ. Zhèxiē wǎngluò ānquán jiějué fāng'àn kěyǐ gēnjù qí gōngnéng jìn háng fēnlèi, lìrú wǎngluò ānquán, shùjù ānquán, yìngyòng chéngxù ānquán, yún ānquán, fǎngwèn guǎnlǐ děng. Zhèxiē jiějué fāng'àn kě bǎohù mǐngǎn xìnxī, tóngshí bǎohù shùjù jīmì xìng.

人工智能

人工智能是一个流行语，无论是在商业、研究还是教育领域，都会产生很多噪音。根据 国家标准技术研究院 的定义，人工智能 是计算机科学的一个分支，专注于创建数据处理系统，这些系统可以从事通常与人类智能相关的推理、学习和自我改进等活动。 它可以概括为一个系统，可以执行通常需要人类智力的基于感知的决策和自然语言处理等任务。让我举一个例子，当你在Facebook上上传图像，你可以观察，系统检测面孔和自动标记个人的图像。让我举一个例子，当你在 面书 上上传图像，你可以观察，系统检测面孔和自动标记个人的图像。该系统使用机器学习算法扫描可用的数据，以识别面孔和斑点模式，使其能够精确匹配人脸。面书 采用AI驱动的人脸识别技术，与深度学习算法配合使用，能够识别民众的人脸模式。

Réngōng zhìnéng

Réngōng zhìnéng shì yīgè liúxíng yǔ, wúlùn shì zài shāngyè, yánjiū háishì jiàoyù lǐngyù, dūhuì chǎnshēng hěnduō zàoyīn. Gēnjù guójiā biāozhǔn jìshù yán jiù yuàn de dìngyì, réngōng zhìnéng shì jìsuànjī kēxué de yīgè fēnzhī, zhuānzhù yú chuàngjiàn shùjù chǔlǐ xìtǒng, zhèxiē xìtǒng kěyǐ cóngshì tōngcháng yǔ rénlèi zhìnéng xiāngguān de tuīlǐ, xuéxí hé zìwǒ gǎijìn děng huódòng. Tā kěyǐ gàikuò wéi yīgè xìtǒng, kěyǐ zhíxíng tōngcháng xūyào rénlèi zhìlì de jīyú gǎnzhī de juécè hé zìrán yǔyán chǔlǐ děng rènwù. Ràng wǒ jǔ yīgè lìzi, dāng nǐ zài miàn shū shàng shàngchuán túxiàng, nǐ kěyǐ guānchá, xìtǒng jiǎncè miànkǒng hé zìdòng biāojì gèrén de túxiàng. Gāi xìtǒng shǐyòng jīqì xuéxí suànfǎ sǎomiáo kěyòng de shùjù, yǐ shìbié miànkǒng hé bāndiǎn móshì, shǐ qí nénggòu jīngquè pǐpèi rén liǎn. Miàn shū cǎiyòng AI qūdòng de rén liǎn shìbié jìshù, yǔ shēndù xuéxí suànfǎ pèihé shǐyòng, nénggòu shìbié mínzhòng de rén liǎn móshì.

人工智能如何为网络安全领域做出贡献？

简而言之，我们可以说人工智能是网络安全的推动者。人工智能具有检测、预防和响应网络攻击的潜力，从而提高了网络安全解决方案的有效性。例如：

- 人工智能算法有助于分析数据集并发现指向潜在网络攻击的趋势;

- 它还分析恶意软件病毒的行为模式并评估风险;

- 人工智能可以自动响应可能的攻击，减少响应时间和损害，同时还可以预测未来的攻击。

另一方面，黑客或网络犯罪分子也使用人工智能来增加其攻击的影响。网络犯罪分子使用人工智能驱动的方法来创建复杂的技术来逃避检测并渗透到计算机系统和网络中。

Réngōng zhìnéng rúhé wèi wǎngluò ānquán lǐngyù zuò chū gòngxiàn?

Jiǎn ér yán zhī, wǒmen kěyǐ shuō réngōng zhìnéng shì wǎngluò ānquán de tuīdòng zhě. Réngōng zhìnéng jùyǒu jiǎncè, yùfáng hé xiǎngyìng wǎngluò gōngjí de qiánlì, cóng'ér tígāole wǎngluò ānquán jiějué fāng'àn de yǒuxiào xìng. Lìrú:
- Réngōng zhìnéng suànfǎ yǒu zhù yú fēnxī shùjù jí bìng fāxiàn zhǐxiàng qiánzài wǎngluò gōngjí de qūshì;
- Tā hái fēnxī èyì ruǎnjiàn bìngdú dí xíngwéi móshì bìng pínggū fēngxiǎn;

- Réngōng zhìnéng kěyǐ zìdòng xiǎngyìng kěnéng de gōngjí, jiǎnshǎo xiǎngyìng shíjiān hé sǔnhài, tóngshí hái kěyǐ yùcè wèilái de gōngjí.

Lìng yī fāngmiàn, hēikè huò wǎngluò fànzuì fēnzǐ yě shǐyòng réngōng zhìnéng lái zēngjiā qí gōngjí de yǐngxiǎng. Wǎngluò fànzuì fēnzǐ shǐyòng réngōng zhìnéng qūdòng de fāngfǎ lái chuàngjiàn fùzá de jìshù lái táobì jiǎncè bìng shèntòu dào jìsuànjī xìtǒng hé wǎngluò zhōng.

同时，随着我们使用越来越多的技术，网络犯罪也在不断增加。安全运营分析师 专注于 AI 来检测潜在的攻击。此外，他们正在努力进行定制，以纳入独特的特征，从而大大缩短对此类攻击的响应时间。截至目前，我们了解到人工智能正在支持网络安全解决方案。让我们来看看网络安全是否比人工智能更好。

Tóngshí, suízhe wǒmen shǐyòng yuè lái yuè duō de jìshù, wǎngluò fànzuì yě zài bùduàn zēngjiā. Ānquán yùnyíng fēnxī shī zhuānzhù yú AI lái jiǎncè qiánzài de gōngjí. Cǐwài, tāmen zhèngzài nǔlì jìnxíng dìngzhì, yǐ nàrù dútè de tèzhēng, cóng'ér dàdà suōduǎn duì cǐ lèi gōngjí de xiǎngyìng shíjiān. Jiézhì mùqián, wǒmen liǎojiě dào réngōng zhìnéng zhèngzài zhīchí wǎngluò ānquán jiějué fāng'àn. Ràng wǒmen lái kàn kàn wǎngluò ānquán shìfǒu bǐ réngōng zhìnéng gèng hǎo.

然而，一方面，网络安全提供了保护系统的解决方案或策略，而人工智能则创建了智能模式来有效地应用这些解决方案以获得更好的结果。安全与新兴技术中心正在开展一个名为“网络人工智能”的项目。该项目的目的是利用人工智能实现网络运营和预防的自动化。根据 德勤 洞察 的一篇文章（技术趋势，2022 年），使用网络人工智能，组织可能能够比攻击者更快地做出响应。它还可以帮助他们预测攻击者的下一步行动并准备立即响应。 网络人工智能工具和技术仍处于采用的早期阶段。此外，该帖子还指出，人工智能可以充当力量倍增器，帮助技术专业人员自动执行耗时的任务，并加快遏制和响应。

Rán'ér, yī fāngmiàn, wǎngluò ānquán tígōngle bǎohù xìtǒng de jiějué fāng'àn huò cèlüè, ér réngōng zhìnéng zé chuàngjiànle zhìnéng móshì lái yǒuxiào dì yìngyòng zhèxiē jiějué fāng'àn yǐ huòdé gèng hǎo de jiéguǒ. Ānquán yǔ xīnxīng jìshù zhōngxīn zhèngzài kāizhǎn yīgè míng wèi “wǎngluò réngōng zhìnéng” de xiàngmù. Gāi xiàngmùdì mù dì shì lìyòng réngōng zhìnéng shíxiàn wǎngluò yùnyíng hé yùfáng de zìdònghuà. Gēnjù déqín dòngchá de yī piān wénzhāng (jìshù qūshì,2022 nián), shǐyòng wǎngluò réngōng zhìnéng, zǔzhī kěnéng nénggòu bǐ gōngjí zhě gèng kuài dì zuò chū xiǎngyìng. Tā hái kěyǐ bāngzhù tāmen yùcè gōngjí zhě de xià yībù xíngdòng bìng zhǔnbèi lìjí xiǎngyìng. Wǎngluò réngōng zhìnéng gōngjù hé jìshù réng chǔyú cǎiyòng de zǎoqí jiēduàn. Cǐwài, gāi tiě zǐ huán zhǐchū, réngōng zhìnéng kěyǐ chōngdāng lìliàng

bèizēng qì, bāngzhù jìshù zhuānyè rényuán zìdòng zhíxíng hào shí de rènwù, bìng jiākuài èzhì hé xiǎngyìng.

网络安全的主要目标是保护系统、网络、数据等，人工智能可用于加强网络安全防御。因此，网络安全和人工智能对于管理不断变化的网络威胁都很重要。

Wǎngluò ānquán de zhǔyào mùbiāo shì bǎohù xìtǒng, wǎngluò, shùjù děng, réngōng zhìnéng kěyòng yú jiāqiáng wǎngluò ānquán fángyù. Yīncǐ, wǎngluò ānquán hé réngōng zhìnéng duìyú guǎnlǐ bùduàn biànhuà de wǎngluò wēixié dōu hěn zhòngyào.

参考

CNBC商业。（2022 年 9 月 13 日）。人工智能在网络安全中发挥着越来越大的作用，但坏人可能受益最大. AI has bigger role in cybersecurity, but hackers may benefit the most (cnbc.com)

德勤（Deloitte）洞察. (2022). 网络人工智能 : 雷亚尔 防御. The future of cybersecurity and AI | Deloitte Insights

高德纳 词汇表, Definition of Cybersecurity - Gartner Information Technology Glossary

美国国家标准与技术研究院定义词汇表、信息技术实验室、计算机安全资源中心, CSRC Topics - artificial intelligence | CSRC (nist.gov)

普华永道出版物。（2021）. 平衡权力与保护：网络安全中的人工智能和人工智能中的网络安全. pwc-balancing-power-protection-ai-cybersecurity.pdf

2023 年的威胁预测. (2023). The top 10 cybersecurity threats for 2023 - Atos