Securing the Future: Exploring Privacy Risks and Security Questions in Robotic Systems

Diba Afroze, Yazhou Tu, and Xiali Hei(✉)

University of Louisiana at Lafayette, Lafayette, LA 70504, USA
xiali.hei@louisiana.edu

Abstract. The integration of artificial intelligence, especially large language models in robotics, has led to rapid advancements in the field. We are now observing an unprecedented surge in the use of robots in our daily lives. The development and continual improvements of robots are moving at an astonishing pace. Although these remarkable improvements facilitate and enhance our lives, several security and privacy concerns have not been resolved yet. Therefore, it has become crucial to address the privacy and security threats of robotic systems while improving our experiences. In this paper, we aim to present existing applications and threats of robotics, anticipated future evolution, and the security and privacy issues they may imply. We present a series of open questions for researchers and practitioners to explore further.

Keywords: Robotics · Security · Privacy · Artificial Intelligence · Autonomous Device · Risk Analysis

1 Introduction

The twenty-first century is witnessing an unprecedented increase in the evolution and utilization of robots. With the upcoming Industry 4.0 revolution, we are approaching the era of robotics [39]. Currently, robotic systems play an important role, from performing medical procedures to serving as salespeople in shopping centers. Robots are now even replacing human companions. This remarkable growth, from a simple machine to an autonomous humanoid robot, has become possible because of the advancement of Artificial Intelligence, Natural Language Processing, Sensor Technology, and Processing Power.

To employ automation in work, different types of robots are used, designed to suit the specific nature of the work. We can categorize three general types of robots, i.e., *Industrial Robots*, *Service Robots*, and *Specialized Robots* [23]. Nowadays, these robots perform multipurpose applications seamlessly alongside humans in industries as well as at home. They handle heavy, mundane tasks for humans effortlessly. Additionally, they are becoming reliable in specialized tasks like healthcare assistance, surveillance, space exploration, rescue missions, etc.

Y. Chen et al. (Eds.): SmartSP 2023, LNICST 552, pp. 148–157, 2024.
https://doi.org/10.1007/978-3-031-51630-6_10

Robots are also helping as nurses or companions for older people. The vehicle industry is being revolutionized by the uprising of autonomous vehicles. All these advancements illustrate the prospect of reducing the gap between science fiction and reality.

As we embrace the help of robots in our daily lives, it may not be very long before these intelligent machines start to co-exist with us in society in every sector. Robotic help can undoubtedly simplify our lives, but it comes with potential privacy and security risks to our personal and social lives. Therefore, it is imperative to develop methods to prevent different kinds of privacy and security threats of robots to humans. Existing versions of robots are not free from threats, thereby indicating that future versions are unlikely to be different. There are several questions concerning privacy and security that a robot must answer before we may consider it to be safe to release in society. If we do not ensure that robots' mechanisms can answer these questions, we might have to reassess the deployment of robot among humans due to the inherent risk it poses to human life. In this paper, we explore a few of these questions.

In the following sections of this paper, we will address the growth of robotic advancement and several privacy and security-related questions that need our attention.

2 Literature Review

The proliferation of Robots is accelerating rapidly in our daily lives, and with it comes a rise in potential dangers. From the beginning of the use of robots, back in 1979, the first death induced by an industrial robot has been recorded [53]. After that, several deaths and injuries were caused by robots [25]. Even though robot R&D companies are trying to implement policies for secure interaction between humans and robots, new threats arise with the development of new robot technologies.

Today, Robots are serving in many roles, such as security guards, salespeople, helping hands at home, nurses, etc. In emergency situations, humans might not follow the instructions of robots acting as security guards [2]. An open question is: What would happen if people refused to take commands from robots? Will the robot force humans or let them pass? Trust has not yet been fully established for robot services. People are concerned about their security; They are skeptical about letting unknown robots into their living spaces [8]. Trust also depends on the appearance of robots; in some cases, people may feel threatened by humanoid robots that perform better than them at work [57].

Robots are vulnerable to various forms of cyberattacks. Clark et al. present different cyber attack scenarios [11], for example, buffer overflow attacks to take control over companion robots, attacks on automated vehicles during firmware updates by pushing corrupted updates, hardware backdoor attacks on military drones, etc. Additionally, researchers show a comprehensive view of several cybersecurity issues such as malware, Trojan, replay attacks, fault injection, tampering attacks, etc. [28,54,58].

Automated vehicles can be one of the targets of attackers. The attackers may use jamming, high-brightness Infrared LEDs, Digital Radio Frequency Memory (DRFM), etc. [40], to provide false navigation data. Additionally, autonomous vehicles are generally connected to users' smartphones. Sugawara et al. [46] presented an audio injection attack on the voice-controlled smartphone system connected to automated Tesla and Ford cars. In addition, the classification system of autonomous vehicles is at risk of potential attack. The work in [15,31] demonstrated that a simple perturbation of the traffic signal could make the CNN classification model misidentify the signal. This attack poses significant security risks and can potentially cause chaos on roadways. Unmanned Automated Vehicles (UAVs), such as drones and rovers, are also in danger of being attacked. Dash et al. [13] demonstrated three attacks on UAVs protected by control invariants (CI) [10] and the extended Kalman filter (EKF) [9]. The authors designed the attacks on UAVs by injecting minor false data into the control system, which caused the automated vehicle to change its position and angular orientations, injecting time delays to make the UAV receive commands late, and lastly, injecting malicious code to switch the mode of the UAVs. In [50], Tu et al. presented two attacks (i.e., Side Swing [22], and DoS [21]) to cyber-physical systems, and they manipulated two automatic self-balancing robots by spoofing embedded Micro Electro Mechanical Systems (MEMS) inertial sensors.

Telerobots [38] come in handy in medical surgery, military operations, and rescue missions. In [5,7], the authors elaborated that telerobots are vulnerable to common cyber attacks such as viruses, worms, and malware. They also mention security threats such as command manipulation, denial of service, and communication loss. Recently, several medical centers have filed lawsuits against Intuitive Surgical, a surgical robot manufacturer, alleging that they were coerced into signing restrictive repair contracts, forcing them to buy new parts from the aforementioned company [42]. An operation had to be postponed due to the usage of third-party repair. This incident adds another dimension to the challenges of surgical robots. Shah et al. [44] demonstrated a successful side-channel attack-*Fingeprint* on surgical robots. Besides, other potential side-channel attacks on robots are Radio-frequency attacks [45] and cache-based attacks on automated vehicles [32].

Lutz et al. [33] observed robot usage from a different perspective, implying that social robots might affect the psychological and social privacy of human beings. Van et al. [17] express their concern about whether we are compromising privacy in exchange for robotic services. *The Guardian* reported [18] about wifi-enabled Barbie dolls, which can be hacked and turned into a surveillance device to spy and collect information without anyone's knowledge. Robots are also becoming companions of humans, sometimes as caregivers. However, some authors are concerned about ethical issues. For example, the authors fear that companion robots might create a hallucinatory reality for some people [6].

3 Future Evolution and Security Questions

Robots are evolving and becoming more intelligent, precise, and *human-like.* Understandably, people are apprehensive about whether robots are going to be a threat to our lives, as depicted in science fiction movies. We are going to elaborate on some sectors for possible futuristic advancements in robots and the privacy and security questions that come with them.

- ***Cyber Security:*** Robots are now connected to wired and wireless networks for smooth data exchange and communication like any other device. However, robots have a lot of security issues, such as lack of authorization, authentication, secure network, tamper-resistant hardware, privacy, integrity, etc. [54]. Robotic networks and computer networks are different in nature; the same countermeasures in general computers may not work on robotics networks [52]. Robotic Operating System (ROS) is also becoming popular among developers. Nevertheless, ROS is vulnerable to attacks such as DoS, DDoS attacks, malware, buffer overflow, malicious code injection attacks, etc. [11].

  Ransomware is another concern for robot users. In [34], Mayoral-Vilches et al. show a ransomware attack-*Akerbeltz* on industrial robots, which locks and encrypts the robot from its vendor network. The attack was carried out by simply connecting a USB device to the robot or remotely accessing the adjacent network. Furthermore, another ransomware attack was demonstrated on a SoftBank Robotics NAO humanoid robot [29].

  > ***Open Question 1:*** Is there a way to identify security vulnerabilities early in robots? Is the robotic system software updated, or are security patches issued promptly?

- ***IoT Connections:*** Robots are now becoming part of IoT and interconnecting with other devices. In homes, industries, and offices, it is common to connect robots with home assistants, smartphones, and TVs. Consider a scenario where an industrial robot integrates with other devices within a multi-purpose company. If an unauthorized user takes control of the robot, the whole system will be compromised. The attacker can take control of other devices and perform dangerous tasks. For example, this security breach may lead to injury, financial damage, and data theft. Thus, it is necessary to secure the additional mobile attack interface - robots. Another scenario is depicted by Amoozadeh et al. [4], where each vehicle receives beacon messages from the immediately preceding vehicle using the IEEE 802.11p protocol. The authors demonstrated security (e.g., message falsification attack, spoofing attack, distributed DoS, Radio jamming, etc.), system-level attacks (e.g., hardware or software tempering), and privacy attacks (e.g., eavesdropping attack) on different layers of automated vehicle networks. A compromised network of vehicles can endanger passengers in all connected vehicles. Moreover, the attacker can evade privacy by leaking personal information such as vehicle identity, current vehicle position, speed, and acceleration.

> ***Open Question 2:*** How can the robot immediately detect and respond to a security breach? Can the robot alert the administrator about the intruder?

- ***Mutual Authentication:*** Authentication has become one of the main concerns in robotics. Mutual authentication is necessary to establish secure communication between robots and humans. Several works have been done to authenticate users, such as face recognition, voice recognition [52], behavior-based recognition [3] etc. However, as we are employing an increasing number of robots in our work, the robots' identities need to be verified as well. Some delivery robots [26,43,48] use OTP (One-Time Password) or mobile applications on users' smartphones to authenticate to the user. But these methods are insufficient because they are susceptible to attacks [36]. Adi et al. proposed an *unclonable identity* for robots based on the work [1]. This identity will be unique to human DNA. However, this process is complex, expensive, and not feasible for mass production. Later, Gavrilova et al. [16] presented an idea to use biometric principles (e.g., physical and behavioral characteristics) to recognize and authenticate *virtual* avatars.

  > ***Open Question 3:*** Is it possible to assign unique biometrics for robot authentication?

- ***Autonomous Robot:*** The current generation of robots is not fully autonomous; they depend on pre-programmed commands. However, several initiatives are underway to extend the perimeter and allow robots to have autonomy to some extent, e.g., unmanned vehicles, Tesla bot [49].

  Military services are also trying to utilize autonomous robots in war, spying, bomb defusal, and other dangerous jobs. However, the use of robots at war is a controversial topic, as it can violate international *Humanitarian law* [47]. The question arises with the *Robot at war*, what happens when an order contradicts the *war robot*'s system. For example, if a robot receives an order to attack a house, the robot detects with sensors that the house is full of children. The order contradicts the robot's system in minimizing civilian casualties. Should the robot be allowed to have an awareness of these types of situations, or should the order override the robot's system [30]?

  > ***Open Question 4:*** What if autonomous robots start to make decisions or refuse orders that might cause harm to humans, like kicking back a human who kicks it?

- ***Robot Learning:*** Robot Learning [12] is popular for teaching robots without programming every movement explicitly. Robots can learn from demonstrations, teleoperations, or observation [27]. Learning methods can be supervised, unsupervised, transfer learning, and reinforcement learning [41]. The robots adapt their decisions as they perceive the environment or dataset. The attackers can intentionally manipulate the data during the learning process, such as injecting poisonous data into the training set, spoofing sensor data (e.g., camera, audio), or changing learning conditions. Due to these attacks, robots may learn unsolicited behaviors that can exhibit danger to their surroundings. For example, Yang et al. [55] demonstrated an adversarial attack on a reinforcement learning-based robot learning system where the attacker uses a pulse to generate random observations, degrading the learning performance.

  > ***Open Question 5:*** How can anomalies in robot training data be discovered and addressed so that the robot does not learn and perpetuate dangerous behavior?

- ***Integration with ChatGPT:*** Robots are expected to undergo revolutionary changes using ChatGPT, especially ChatGPT-4. We have seen some proposed frameworks [19,51] in recent times. Vemprala et al. [51] suggested using a ChatGPT prompt to write code automatically for non-technical users to make the robot perform a certain task. In one scenario, the user asks the robot to cook an omelet and serves it to the user's grandfather. Recently, Google DeepMind introduced Robotic Transformer 2 (RT-2), a novel vision-language-action (VLA) model that learns from web-scale datasets [56]. This model is built on the same tech as ChatGPT; It can interpret these data as plain language instruction and execute it [14].

  > ***Open Question 6:*** If ChatGPT can be successfully implemented on robots, what if robots can write code and modify themselves in an unwanted way?

- ***Access Control:*** Certain robots (e.g., service robots in our homes) continuously surveil us as part of their functions. These robots have access to our personal data; they can take pictures and videos, and monitor our locations. Nonetheless, if the vendor of these robots unethically grants access to the robots' system during manufacturing and takes advantage of our confidential data, it can pose significant privacy and security risks. For example, unauthorized users can collect passwords and credit card information by simply taking photos or videos when the user is entering the data.

  > ***Open Question 7:*** How can we effectively incorporate access control in robots to protect the security and privacy of the end users?

- ***Trolley Problem in Robotics:*** Imagine a scenario where a person is watching a runaway trolley heading towards a track where five people are standing, and if nothing is done, these people will *certainly* die. There is another track where he can divert the trolley, but there is another person standing on it that will be killed. Here arises the ethical dilemma of whether killing one person is okay instead of killing five people. As robots become more involved in society, they will inevitably encounter many ethical dilemmas in decision-making. So, it is essential to solve the trolley problem to mitigate any risks that an action of the robot may pose.

> ***Open Question 8:*** What would be the robot's reaction during a 'Trolley Problem' [24] scenario?

4 Conclusion

The widespread adoption of robots signals the imminent revolution of robotics technology. It may not be very long before we generalize the idea of coexisting with robots. We must be prepared for the privacy and security risks to embrace this transition fully. Robotic systems are made of different subsystems and subcomponents. Securing the subcomponents is necessary but not sufficient for protecting the whole system. This is because components are integrated with one another and therefore, exhibit complex and subtle dependencies and interactions [35]. We need to enforce a robotics framework and a universal policy for developing or changing any robots. Such a comprehensive measure will ensure that robots and their manufacturer follow the standard user safety practice. European Commission has created a *voluntary* code of ethics and standards for manufacturers and users of robotics technology [37]. IEEE undertakes a global initiative-*The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems*, which aims to ensure that the involved persons prioritize ethical consideration and benefits of humankind [20]. However, as these policies are not enforced as obligatory, the concerns still prevail.

References

1. Adi, W.: Clone-resistant DNA-like secured dynamic identity. In: 2008 Bio-inspired, Learning and Intelligent Systems for Security, pp. 148–153 (2008). https://doi.org/10.1109/BLISS.2008.33
2. Agrawal, S., Williams, M.A.: Robot authority and human obedience: a study of human behaviour using a robot security guard. In: Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction, pp. 57–58 (2017)
3. Almohamade, S.S., Clark, J.A., Law, J.: Behaviour-based biometrics for continuous user authentication to industrial collaborative robots. In: Maimut, D., Oprina, A.-G., Sauveron, D. (eds.) SecITC 2020. LNCS, vol. 12596, pp. 185–197. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-69255-1_12

4. Amoozadeh, M., et al.: Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Commun. Mag. **53**(6), 126–132 (2015)
5. Bernadotte, A.: Cyber security for surgical remote intelligent robotic systems. In: 2023 9th International Conference on Automation, Robotics and Applications (ICARA), pp. 65–69 (2023). https://doi.org/10.1109/ICARA56516.2023.10126050
6. Bisconti Lucidi, P., Nardi, D.: Companion robots: the hallucinatory danger of human-robot interactions. In: Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society, pp. 17–22 (2018)
7. Bonaci, T., Herron, J., Yusuf, T., Yan, J., Kohno, T., Chizeck, H.J.: To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots (2015). arXiv preprint arXiv:1504.04339
8. Booth, S., Tompkin, J., Pfister, H., Waldo, J., Gajos, K., Nagpal, R.: Piggybacking robots: Human-robot overtrust in university dormitory security. In: Proceedings of the 2017 ACM/IEEE International Conference on Human-Robot Interaction, pp. 426–434 (2017)
9. Bristeau, P.J., Dorveaux, E., Vissière, D., Petit, N.: Hardware and software architecture for state estimation on an experimental low-cost small-scaled helicopter. Control. Eng. Pract. **18**(7), 733–746 (2010)
10. Choi, H., et al.: Detecting attacks against robotic vehicles: a control invariant approach. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 801–816 (2018)
11. Clark, G.W., Doran, M.V., Andel, T.R.: Cybersecurity issues in robotics. In: 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), pp. 1–5. IEEE (2017)
12. Connell, J.H., Mahadevan, S.: Robot learning. In: Sammut, C., Webb, G.I. (eds.) Encyclopedia of Machine Learning. Springer, Boston, MA (2011). https://doi.org/10.1007/978-0-387-30164-8_732
13. Dash, P., Karimibiuki, M., Pattabiraman, K.: Out of control: stealthy attacks against robotic vehicles protected by control-based techniques. In: Proceedings of the 35th Annual Computer Security Applications Conference, pp. 660–672 (2019)
14. Edwards, B.: Google's RT-2 AI model brings us one step closer to WALL-E (2023). https://arstechnica.com/information-technology/2023/07/googles-rt-2-ai-model-brings-us-one-step-closer-to-wall-e/
15. Eykholt, K., et al.: Robust physical-world attacks on deep learning visual classification. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1625–1634 (2018)
16. Gavrilova, M.L., Yampolskiy, R.V.: Applying biometric principles to avatar recognition. In: 2010 International Conference on Cyberworlds, pp. 179–186 (2010). https://doi.org/10.1109/CW.2010.36
17. van Genderen, R.H.: Privacy and data protection in the age of pervasive technologies in AI and robotics. Eur. Data Prot. Law Rev. **3**, 338–352 (2017). https://doi.org/10.21552/edpl/2017/3/8
18. Gibbs, S.: Hackers can hijack Wi-Fi Hello Barbie to spy on your children) (2015). https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children
19. He, H.M.: RobotGPT: From chatGPT to robot intelligence (2023). https://openreview.net/forum?id=wWe_OqpCcU8
20. IEEE: The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (2017). https://standards.ieee.org/wp-content/uploads/import/documents/other/ec_about_us.pdf

21. Injected, Demos, D.: DoS attacks on a self-balancing robot (accelerometer) (2018). https://youtu.be/yDz8y_ht3Xg
22. Injected, Demos, D.: Side-Swing attacks on a self-balancing robot (2018). https://youtu.be/oy3B1X41u5s
23. International Federation of Robotics (IFR): Service Robots as Defined by ISO 8373. https://ifr.org/service-robots
24. Kamm, F.M.: The Trolley Problem Mysteries. Oxford University Press (2015)
25. Kirschgens, L.A., Ugarte, I.Z., Uriarte, E.G., Rosas, A.M., Vilches, V.M.: Robot hazards: from safety to security (2018). arXiv preprint arXiv:1806.06681
26. Kiwibot: Kiwibot. https://www.kiwibot.com/
27. Kroemer, O., Niekum, S., Konidaris, G.: A review of robot learning for manipulation: challenges, representations, and algorithms. J. Mach. Learn. Res. **22**(1), 1395–1476 (2021)
28. Lacava, G., et al.: Cybser security issues in robotics. J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl. **12**(3), 1–28 (2021)
29. Larson, S.: Ransomware experiment shows the dangers of hacking robots (2018). https://money.cnn.com/2018/03/09/technology/robots-ransomware/index.html
30. Lin, P., Bekey, G.A., Abney, K.: Robots in war: issues of risk and ethics (2009)
31. Liu, Y., Ma, X., Bailey, J., Lu, F.: Reflection backdoor: a natural backdoor attack on deep neural networks. In: Vedaldi, A., Bischof, H., Brox, T., Frahm, J.-M. (eds.) ECCV 2020. LNCS, vol. 12355, pp. 182–199. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-58607-2_11
32. Luo, M., Myers, A.C., Suh, G.E.: Stealthy tracking of autonomous vehicles with cache side channels. In: 29th USENIX Security Symposium (USENIX Security 20), pp. 859–876 (2020)
33. Lutz, C., Schöttler, M., Hoffmann, C.P.: The privacy implications of social robots: scoping review and expert interviews. Mob. Media Commun. **7**(3), 412–434 (2019)
34. Mayoral-Vilches, V., Carbajo, U.A., Gil-Uriarte, E.: Industrial robot ransomware: Akerbeltz. In: 2020 Fourth IEEE International Conference on Robotic Computing (IRC), pp. 432–435 (2020). https://doi.org/10.1109/IRC.2020.00080
35. McDaniel, P., Koushanfar, F.: Secure and trustworthy computing 2.0 vision statement (2023). arXiv preprint arXiv:2308.00623
36. Mulliner, C., Borgaonkar, R., Stewin, P., Seifert, J.-P.: SMS-based one-time passwords: attacks and defense. In: Rieck, K., Stewin, P., Seifert, J.-P. (eds.) DIMVA 2013. LNCS, vol. 7967, pp. 150–159. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39235-1_9
37. Nevejans, N.: EUROPEAN CIVIL LAW RULES IN ROBOTICS (2016). http://www.europarl.europa.eu/committees/fr/supporting-analyses-search.html
38. Niemeyer, G., Preusche, C., Stramigioli, S., Lee, D.: Telerobotics. In: Siciliano, B., Khatib, O. (eds.) Springer Handbook of Robotics, pp. 1085–1108. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-32552-1_43
39. Othman, F., Bahrin, M., Azli, N., et al.: Industry 4.0: a review on industrial automation and robotic. J. Teknol. **78**(6–13), 137–143 (2016)
40. Petit, J., Shladover, S.E.: Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. **16**(2), 546–556 (2015). https://doi.org/10.1109/TITS.2014.2342271
41. Ranaweera, M., Mahmoud, Q.H.: Virtual to real-world transfer learning: a systematic review. Electronics **10**(12), 1491 (2021)
42. REUTER, E.: Hospitals sue surgical robot maker, saying it forced them into restrictive contracts. https://medcitynews.com/2021/07/hospitals-sue-surgical-robot-maker-saying-it-forced-them-into-restrictive-contracts/ (2021)

43. Serve: Serve Robotics Becomes First Autonomous Vehicle Company to Commercially Launch Level 4 Self-Driving Robots. https://www.serverobotics.com/level-4-autonomy
44. Shah, R., Ahmed, M., Nagaraja, S.: Fingerprinting robot movements via acoustic side channel (2022). arXiv preprint arXiv:2209.10240
45. Shah, R., Ahmed, M., Nagaraja, S.: Reconstructing robot operations via radio-frequency side-channel (2022). arXiv preprint arXiv:2209.10179
46. Sugawara, T., Cyr, B., Rampazzi, S., Genkin, D., Fu, K.: Light commands: Laser-Based audio injection attacks on Voice-Controllable systems. In: 29th USENIX Security Symposium (USENIX Security 20), pp. 2631–2648. USENIX Association (2020). https://www.usenix.org/conference/usenixsecurity20/presentation/sugawara
47. Szpak, A.: Legality of use and challenges of new technologies in warfare - the use of autonomous weapons in contemporary or future wars. Eur. Rev. **28**(1), 118–131 (2020). https://doi.org/10.1017/S1062798719000310
48. Team, Y.S.D.: The story behind the creation of Yandex's delivery robot (2021). https://medium.com/yandex-self-driving-car/the-story-behind-the-creation-of-yandexs-delivery-robot-e07017940589
49. Tesla: Tesla Bot Update (2023). https://www.youtube.com/watch?v=XiQkeWOFwmk
50. Tu, Y., Lin, Z., Lee, I., Hei, X.: Injected and delivered: fabricating implicit control over actuation systems by spoofing inertial sensors. In: 27th USENIX Security Symposium (USENIX Security 18), pp. 1545–1562 (2018)
51. Vemprala, S., Bonatti, R., Bucker, A., Kapoor, A.: ChatGPT for robotics: design principles and model abilities. Microsoft Auton. Syst. Robot. Res **2**, 20 (2023)
52. Wang, T.M., Tao, Y., Liu, H.: Current researches and future development trend of intelligent robot: a review. Int. J. Autom. Comput. **15**(5), 525–546 (2018)
53. Winfield, A.F.T., Winkle, K., Webb, H., Lyngs, U., Jirotka, M., Macrae, C.: Robot accident investigation: a case study in responsible robotics. In: Software Engineering for Robotics, pp. 165–187. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-66494-7_6
54. Yaacoub, J.P.A., Noura, H.N., Salman, O., Chehab, A.: Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. Int. J. Inf. Secur. 1–44 (2022)
55. Yang, C.H.H., et al.: Enhanced adversarial strategically-timed attacks against deep reinforcement learning. In: ICASSP 2020–2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 3407–3411. IEEE (2020)
56. Yevgen Chebotar, T.Y.: RT-2: New model translates vision and language into action. https://www.deepmind.com/blog/rt-2-new-model-translates-vision-and-language-into-action (2023)
57. Yogeeswaran, K., Złotowski, J., Livingstone, M., Bartneck, C., Sumioka, H., Ishiguro, H.: The interactive effects of robot anthropomorphism and robot ability on perceived threat and support for robotics research. J. Hum.-Robot Interact. **5**(2), 29–47 (2016)
58. Zhu, Q., Rass, S., Dieber, B., Vilches, V.M., et al.: Cybersecurity in robotics: challenges, quantitative modeling, and practice. Found. Trends® Robot. **9**(1), 1–129 (2021)