How smart is the use of smart devices in the office?

The case of **industrial cleaning robots** in the Netherlands

Firewalls, end-to-end encryption, private cloud, no smartphones during meetings. This is a small selection of the measures that organizations are taking to secure data traffic on their digital networks and to counter espionage. Many of these organizations also implement at first sight harmless technologies that make life easier, from smart TVs and smart lighting to cleaning robots. However, these internet-connected devices are full of sensors that collect data.

In this article, we use the case of industrial cleaning robots to show what the possible security risks are of using smart devices, and what organizations can do to safeguard their security. In doing so, we will dive deeper into the possible security risks of free-market forces in high-tech sectors with strong competition from non-European companies.

Ronald Heil MSc CISSP CISA GICSP
is a partner at KPMG Cyber & Privacy.

Marnix Bel MSc
is a former senior consultant at KPMG Cyber & Privacy.

Consumers still use equipment that uses and abuses personal data

INTRODUCTION

Smart devices are full of sensors that collect data. This data is often stored and/or processed in a cloud environment outside the EU and is then used to optimize the tasks of those devices. What data do these devices collect, where is this data stored and who owns this data?

In Europe, these questions are often only asked when Chinese products or companies enter the market. It is usually assumed that there are only innocent intentions behind the collection of data by Western companies, such as improving quality, as every set of terms and conditions tells us. That is a false assumption, as was demonstrated by the information that whistleblowers such as Edward Snowden and Julian Assange (WikiLeaks) made public. However, this has hardly affected the level of trust that European consumers have in Western brands. Consumers still use equipment that uses and abuses personal data. Offices are full of smart TVs, smart lighting and all kinds of other smart devices that record audio or video and possibly store it in the cloud. Data leaves the smart equipment, as well as the organizational location. It is therefore time to discuss the security risks associated with using these types of devices.

The dominant brands of smart devices are often non-European (in particular American and Asian), which limits European control over how data is collected and used. However, the EU has a fundamentally different attitude to data ownership than China and the US, for example. The EU prioritizes the protection of individual human rights over informing the central government or the economic profit of a small elite. How can the EU protect the personal data of its citizens when these citizens use Chinese and American technology?

The European economic security policy is currently focused primarily on China, where European high-tech companies with strategic technologies must be protected against takeovers or acquisitions of majority interests particularly by Chinese state-owned companies, using an investment screening mechanism. At the heart of this philosophy is the assumption that Europe has a technological lead over China and that this lead should be defended against attempts by the Chinese government to copy these technologies. The fact is, however, that European companies are no longer automatically in the top tier, so we will also have to learn how to deal with China as a supplier of high-quality technology, and in particular, how we can manage and limit the associated security risks.

The key recommendations from this article are:

1. It is in the interest of Dutch security to support European high-tech companies with the biggest potential so that they can continue to compete with non-European brands. In this way, customers will

Table 1. Supply of industrial cleaning robots on the Dutch market.
Source: Compiled from interviews with suppliers of industrial cleaning devices in the Netherlands ([Lugt21]).

Name of Company	HQ	Sofware	Number of models
Tennant	US	BrainOS	2
Hako	US	BrainOS	3
ICE Robotics/Softbank	China/Japan	BrainOS	1 (soon to be 4)
Nilfisk	Denmark	BrainOS	2
Fybots	France	Unknown	3
Cleanfix	Switzerland	Own software	1
Adlatus	Germany	Own software	1
Gaussian	China	Own software	3 (soon to be 6)

still have a European option and more control over their data.

2. Labelling and "benchmarking" the level of digital security of smart devices enables consumers and organizations to identify devices with higher cybersecurity prerequisites and make informed decisions.
3. Organizations are advised to develop policies for the use of smart devices within their organization, especially when it comes to locations where valuable and vulnerable data is used.

THE RISE OF THE INDUSTRIAL CLEANING ROBOT IN EUROPE

COVID-19 has accelerated our need for robots (and specifically their cleaning function) ([Lerm20]). On an increasing number of factory floors and offices, robots are taking over the physically intense tasks of cleaners so that these cleaners can focus on the more specialized cleaning tasks. Currently, all major cleaning machine suppliers are offering a robotic vehicle, or at least developing one. There are currently nine suppliers of industrial cleaning robots in the Netherlands. Table 1 shows that most cleaning robots on the Dutch market are non-European brands.

It is noticeable that half of the cleaning robots on the Dutch market use BrainOS software from the American company Brain Corp. Brain Corp develops software for robots and manages the data that the robots collect. The vice-president of Brain Corp recently announced that his company would like to do more with this data in the future:

Multifunction robots that can clean and scan at the same time will come eventually as an IoT source of information that's considered valuable. [...] Right now, the industry records everything but doesn't do anything with the data. We're very judicious about data." Phil Duffy, vice-president of innovation at Brain Corp ([Dema20]).

The fact that an American company is about to collect, store and analyze data from cleaning robots in the Netherlands on such a large scale should make us think about where we would like to use those cleaning robots. If a company has a "no-smartphones policy" during meetings, it would be contrary policy if that same company had a cleaning robot driving through the office and/or factory halls while data is collected and stored by a non-European company. What data does an autonomous cleaning robot collect and what possible security risks are associated with the use of such a cleaning robot?

Figure 1. Examples of exteroceptive sensors.
Source: Fybots and Gaussian Robotics sales brochures.

CLEANING ROBOTS AND SECURITY

Historically, technology has always had two faces. On the one hand, there is the perspective of progress and innovation. On the other hand, new technologies can shift vulnerabilities that can disrupt the "stable, comfortable equilibrium/normal".

In recent years, there has been an increasing focus on the cybersecurity aspects of industrial and consumer robots, but cleaning robots have remained below the radar. However, these machines also collect data while performing their work at airports, universities, companies and government buildings. To function optimally, they are equipped with cameras and/or other sensors that collect data.

The best hardware is only as good as its brains

We generally distinguish two basic types of robotic sensors:

- Proprioceptive sensors, which collect data about the robot itself.
- Battery status, maintenance status, etc.
- Exteroceptive sensors, which collect data about the workspace of robots.
- Lasers, distance sensors, cameras, etc.

In this article, we focus on the exteroceptive sensors.

With the help of these sensors, the robot can create a ground floor map, locate itself, avoid objects and stairwells, recognize glass walls and communicate with elevators.[1] Depending on the type of camera in the robot, it could make detailed recordings of its surroundings and the people walking around. This could be sensitive, personal and/or secret information. Some manufacturers therefore consciously choose not to place cameras on the robot and instead only use lasers (LiDAR sensors) and ultrasonic sensors. Brain Corp combines 2D LiDAR with cameras.[2] It claims that its cameras blur faces and texts during recording and that, as a result, those images are only stored and transmitted to Brain Corp in a blurred manner (interview with representative of Brain Corp). Brain Corp then converts this data into relevant data for its customers, which they can access through a portal. For example, the customer will receive a photo of what is in the way of the robot when it gets stuck. If this is a person, his or her face will be blurred. The customer trusts the manufacturer not to store potentially sensitive information.

As Gaussian formulates it on its website, "The best hardware is only as good as its brains" ([Gaus22]).The data that the cleaning robot collects only becomes meaningful when it is converted into information by drawing relational connections ([Rowl07]). To convert data into information, an object must be detected, identified and/or classified. Algorithms that run these processes are usually demanding in terms of computing power. For reasons of computing power, battery conservation or even cost reduction, these algorithms are often processed not in the robot but in the cloud. In the case of cleaning robots, the robots communicate generic "cleaning data" (such as images and floor plans) with the "parent company/cloud".

Data leaves the robot, as well as the cleaning location, to be converted into information. Moving and storing this information can entail security risks if the data contains privacy-sensitive or classified information. The manufacturers use different technologies to transmit the data collected by the robots, such as mobile connections (3G/4G/5G) and WiFi point-to-point.

Connectivity subjects the cleaning robots (and similar IoT devices) to Beckstrom's Law of Cybersecurity;

1. Anything connected to a network can be hacked.
2. Everything is connected to a network.
3. Because of this, everything can (potentially) be hacked.

A cleaning robot (with cameras and WiFi) that moves freely through the building is therefore potentially an ideal target for hackers. There are roughly three types of threat actors that we could distinguish ([Dams19]):

1 Other examples of devices with exteroceptive sensors are, for example, cameras in smart TVs and microphones in their remote controls. In this article, we focus on sensors in industrial cleaning robots to go deeper into the possible impact of the use of smart devices in the office and other places in the organisation.

2 In the literature this is referred to as a cost-effective alternative to 3D LiDAR. A 3D LiDAR can easily cost between $4,000 and $15,000, while a 2D LiDAR only costs $800 to $2,500.

IoT security and risks

The rise of the internet of things (IoT) leads to discussions about the security of devices connected to the internet. When an organization's devices, from production equipment to the air conditioning system and printing machine, send data over the internet, it creates new access points (and risks) for the corporate network ([Hods19]). However, many of these devices are designed and developed with limited security controls. In product development, higher security requirements often go hand in hand with higher costs and power consumption. This vulnerability is exploited by hackers who develop special malware for IoT equipment. For example, the Mirai botnet virus took down large and popular websites through massive Distributed Denial-of-Service (DdoS) attacks using hundreds of thousands of compromised IoT devices ([Burs17]). The compromised IoT devices ranged from printers and (security) cameras to baby phones.

Table 2. Specifications and functionalities of cleaning robots.
Source: Interviews with suppliers of the various cleaning robots in the Netherlands ([Lugt21]).

	Tennant		Hako	ICE Robotics	Nilfisk		Cleanfix	Adlatus	Fybots	Gaussian	
Robot	T7AMR	T30AMR	Robo-scrub	Whiz	Liberty SC60	Liberty SC50	RA 660 Navi XL	CR700	Sweep XL	Ecobot 50	Ecobot 75
Camera	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Teach & repeat	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fill-in function	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Dynamic path planner	✗	✗	✗	✗	✗	✗	?	✗	✓	✓	✓
Can start at any given point (without reprogramming)	✗	✗	✗	✗	✗	?	✗	✗	✓	✓	✓
Communicates with elevators	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
Re-routes itself in case of an obstacle	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓
Internet connection	4G/LTE	4G/LTE	4G/LTE	4G/LTE	4G/LTE	4G/LTE	LTE/WiFi	WiFi	WiFi/SIM	4G/LTE	4G/LTE
Software	BrainOS	BrainOS	BrainOS	BrainOS	BrainOS	Own software	Own software	Own software	?	Own software	Own software

- Script kiddies: Most hackers are referred to as "script kiddies" (i.e. inexperienced, usually young adolescent individuals or journalists looking for a juicy story and executing attacks (scripts) they found online without deep technical knowledge). The impact of their cyberattacks is, however, not to be underestimated. The success of the Mirai DDoS botnet attack shows the damage that this group can cause.
- Cybercriminal gangs: These gangs are mostly after money and have made a lucrative business model out of their activities.
- Nation-state actors: The revelations by whistleblower Edward Snowden showed that nation-state actors also hack digital devices to spy[3] (even on allies).

It is therefore important to think carefully about who (and which devices) can have access to internal facilities to limit and mitigate the security risks. This risk applies to European as well as non-European robots. However, when a robot runs on non-European software, the security of the data is much more complex.

In this digital age, data is the new gold, but it is not always treated that way. After all, there has been no commotion about the fact that most cleaning robots on the Dutch market run on American software. Who owns the data that these machines collect (and does it include sensitive personal data)? The raw data that industrial cleaning robots collect is often sent directly to the manufacturers. Does this automatically make them the owner of the data? In light of the General Data Protection Regulation (GDPR), how is this potentially personal data that the cleaning robots collect treated? The findings from our survey among manufacturers and suppliers of industrial cleaning robots in the Netherlands show that people hardly ever associate privacy (and GDPR requirements) with robots. Customers sometimes ask for it, but suppliers do not yet have adequate answers.

EUROPEAN BRANDS WILL SOON BE JOINED BY A STRONG COMPETITOR FROM CHINA: GAUSSIAN

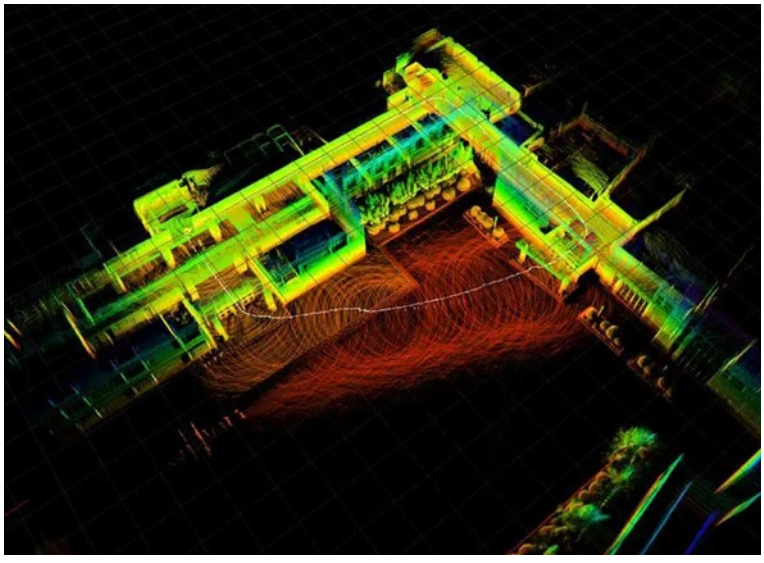
There are now at least two European initiatives that run on their own software: Adlatus and Cleanfix. How advanced are these European-produced robots compared to their American and Asian competitors? How advanced is the new Chinese robot that is about to compete for European market share? Will we still have a European competitive alternative in the future?

Table 2 shows how these European providers compare to the other providers of cleaning robots on the Dutch market.

3 Secret services sometimes intercept devices while they are on their way to their customer and then add eavesdropping equipment or disable the product. For example, the NSA has routinely intercepted shiploads of Cisco routers to install backdoors.

The teach-and-repeat technology means that you will need to guide the robot throughout the whole area that needs to be cleaned, after which the robot will follow this pre-programmed route. The fill-in function means that an operator needs to guide the robot along the outer lines of the area that needs to be cleaned, after which the robot will clean the area within these lines automatically. In this case, the robot will have to start at a pre-programmed starting point. Both technologies use SLAM, but to a lesser extent than with the dynamic path planner technology. SLAM is based on the multidimensional normal distribution (a derivative of the Gaussian distribution discovered by Carl Friedrich Gauss), hence the name Gaussian. The other brands also use SLAM, albeit to a lesser extent than Gaussian does, and that is the reason why these robots cannot determine their routes as independently.

Figure 2. Example of mobile robot position technology: visualization of SLAM.
Source: [AGVb20]



Gaussian has announced that it will market four more models of autonomous cleaning robots in 2021. With six different models, Gaussian will soon have the largest range of industrial cleaning robots (see Table 1). Moreover, Gaussian has a competitive advantage over almost all of its American and European competitors in the technological field[4]. For example, Gaussian and Fybots robots are the only industrial cleaning robots on the Dutch market that can start at any point in the room (without reprogramming a new starting point) and communicate with elevators. In addition, like only three other robots, Gaussian robots can re-route automatically if an obstacle blocks their passage.

As we mentioned above, half of the industrial cleaning robots on the Dutch market use the Brain Corp software BrainOS. BrainOS software is based on a "teach-and-repeat" technology. This technology is less advanced than the fill-in function or the dynamic path planner technology (see textbox). It is intended that the robots with BrainOS software will also start using the fill-in function during the first half of 2021. The European brands Adlatus and Cleanfix already use of this fill-in technology. The Gaussian robots, on the other hand, make their own map and determine their route automatically with the aid of Simultaneous Localisation And Mapping (SLAM) ([USP10]).

Adlatus and Cleanfix are more advanced than the robots using BrainOS software, but they are no match for the Gaussian robots[5]. Adlatus Robotics was founded in 2015 as a start-up in Ulm, Germany ([Ruts18]). Still a relatively small company with about 40 employees, Adlatus currently has one model of industrial cleaning robot on the market that won the PURUS Innovation Award in 2017 (Adlatus, 2017) and 2019 ([Adla19]). Cleanfix is a Swiss company with approximately 180 employees that has been developing and manufacturing cleaning machines since 1977.

European models can expect fierce competition from China's Gaussian Robotics. Founded in 2013, Gaussian produces high-quality industrial cleaning robots. The founders are Cheng Haotian (University of Cambridge electrical engineering alumnus) and Qin Baoxing (the founder of a Singaporean autonomous driving company). Gaussian Robotics employs approximately 450 people, of whom approximately 250 are engineers.

4 See Table 2: Specifications and functionalities of cleaning robots.

5 We received the information about the Fybots Sweep XL late in our research and were not able to include it in our analysis. For reasons of completeness, we have included the information in the table to show that there is another promising European brand.

Gaussian Robotics is the market leader in intelligent cleaning robots in China with a market share of more than 90% ([Zha020]). Gaussian exports about 40% of its products and is also the market leader in the rest of Asia. Gaussian (or Gao Xian in Chinese, which loosely translates as "height" or "high God") has recently also started focusing on the European market.

In September 2020, Gaussian Robotics raised $22 million in investment, with the largest investors being the Chinese Broad Vision Funds and China Capital Management ([CMAI20]). The interest of these two major Chinese funds shows confidence in the company and its growth potential. Last October the Dutchman Peter Kwestro (former Global Sales Leader of Adlatus) was appointed as Global Business Development Director of Gaussian ([Sch020]).

In short, there are currently many developments going on in this sector. The developments indicate that European manufacturers of industrial cleaning robots will face stiff competition, at least on paper, from China's Gaussian.

CONCLUSION

Will Chinese cleaning robots come to us to absorb our knowledge and secret information? We know one thing for sure: they are not coming for our knowledge about cleaning robots.

If customers and organizations choose advanced non-European cleaning robots, the market share of European organizations will decline and with it the appetite to seriously invest in R&D. That is particularly true if Gaussian also starts a price war. This could lead to a situation in which Gaussian's competitors throw in the towel one by one and buyers of industrial cleaning robots might be left with hardly any choice[6]. These are market forces and will not necessarily be a problem for the use of industrial cleaning robots in generic locations such as shopping centers and distribution centers. However, there must be a (high-quality) European alternative for locations where (secret) valuable and vulnerable data is used and stored, such as universities, high-tech organizations and government buildings (including defense buildings). In these locations in particular, careful consideration must be given to the use of smart devices such as cleaning robots that store floor plans and possibly also record, store and/or process detailed images of people and texts in a (non-European) cloud.

Therefore, action must be taken now that European alternatives still exist. It is in the interest of European security to support European cleaning robot manufacturers with the greatest potential so that they can continue to compete with non-European brands, making sure there is still an attractive and competitive European alternative. We need to ensure that European manufacturers of cleaning robots (that have far fewer robotics engineers than Gaussian) can keep up with non-European brands so that we will always have a European alternative.

Organizations also need to be smarter about the use of smart equipment, including cleaning robots. Smart devices offer many benefits and can make work significantly easier, but they must be used sensibly, especially when it comes to locations where valuable and vulnerable data is used. Awareness of the security risks associated with the use of smart devices is fundamental to increasing digital resilience.

A possible solution is labelling and "benchmarking" the level of digital security of smart devices. For example, the Cyber Security Agency of Singapore (CSA) has launched the Cybersecurity Labeling Scheme (CLS) for smart consumer devices as part of its efforts to improve the security of smart devices ([CSAS22])[7]. This enables consumers and organizations to identify devices with higher cybersecurity prerequisites and make informed decisions. Manufacturers can differentiate themselves from their competitors and be encouraged to develop safer products. Organizations are also advised to develop policies for the use of smart devices within their organization. Since it is a standard procedure for organizations to perform background research and screening of (support) staff, it is only logical to maintain the same policy for smart devices used within the organization.

6 In a similar way, Chinese telecom vendors Huawei and ZTE have pushed Western vendors out of the market with a price war and that is the reason why there are globally only four telecom vendors left: two Chinese (Huawei and ZTE) and two European (Ericsson and Nokia Alcatel-Lucent). Ericsson and Nokia have barely survived the price war with Huawei and are currently benefiting from the trade war between the US and China.

7 Various countries (e.g., USA, Finland, and Germany) are designing and adopting Smart Devices Cybersecurity Labelling Scheme (CLS) that improves safety for consumers. The labels are expected to feature ratings that reflect the quantity of data collected, how easily the device can be patched or upgraded to mitigate vulnerabilities, data encryption, and interoperability.

The report "How smart is the use of smart devices in the office?" ([Lugt21]) was published in the *Clingendael Spectator* magazine. The *Clingendael Spectator* (since 1947) is the magazine of Dutch think tank Clingendael, freely accessible for all with an interest in current developments concerning world politics. The report was written in collaboration with Dr. Sanne van der Lugt, who at the time of writing the report was a China researcher, intercultural trainer and senior policy advisor on foreign policy in the Dutch parliament. Her current research focus is on AI developments in China.

References

[Adla17] Adlatus (2017). *CMS Purus Innovation Award 2017 – Pressebericht CMS Messe Berlin.* Retrieved from: https://www.adlatus.eu/cms-purus-innovation-award-2017-pressebericht-cms-messe-berlin/

[Adla19] Adlatus (2019). *Adlatus Wins The Purus Innovation Award.* Retrieved from: https://www.adlatus.eu/en/adlatus-wins-the-purus-innovation-award/

[AGVb20] AGVblog (2020). *Mobile robot positioning technology – laser SLAM.* Retrieved from: http://www.agvblog.com/667.html

[Burs17] Bursztein, E. (2017). *Inside the infamous Mirai IoT Botnet: A Retrospective Analysis.* Retrieved from: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

[CMAI20] China Money AI (2020, September 2). *Chinese Clearning Robot Developer Gaussian Robotics Raises 22M in Series B Round.* Retrieved from: https://www.chinamoney-network.com/2020/09/02/chinese-cleaning-robot-developer-gaussian-robotics-raises-22m-in-series-b-round

[CSAS22] CSA Singapore (2022). *Cybersecurity Labelling Scheme (CLS).* Retrieved from: https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/product-list

[Dams19] Dams, T. & Verbij, R. (2019). *Gaming the new security nexus.* Netherlands: KPMG, Clingendael.

[Dema20] Demaitre, E. (2020, June 8). *Cleaning robots, ease of use, and data key to reopening retail, say Brain Corp execs.* Retrieved from The Robot Report: https://www.therobotreport.com/cleaning-robots-ease-use-data-key-reopening-retail-says-brain-corp/

[Gaus22] Gaussian Robotics (2022). *ECOBOT Scrubber 75.* Retrieved from https://www.gaussianrobotics.com/ecobotscrubber75

[Hods18] Hodson, C. (2018, August 7). *De security-risico's van IoT.* Retrieved from Computable: https://www.computable.nl/artikel/opinie/security/6425660/1509029/de-security-risicos-van-iot.html

[Lerm20] Lerman, R. (2020, September 8). *Robot cleaners are coming, this time to wipe up your coronavirus germs.* Retrieved from The Washington Post: https://www.washingtonpost.com/technology/2020/09/08/robot-cleaners-surge-pandemic/

[Lugt21] Van der Lugt, S. & Bel, M. (2021, April 12). *How smart is the use of smart devices in the office?* Retrieved from: https://www.clingendael.org/publication/how-smart-use-smart-devices-office

[Rowl07] Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science, 33*(2).

[Ruts18] Rutsch, S. (2018, April 11). *Adlatus Robotics wins Germany's first cleaning robot contest.* Retrieved from Vision.ifm: https://www.vision.ifm/en/adlatus-robotics-wins-germanys-first-cleaning-robot-contest/

[Scho20] Schoonmaak Journaal (2020, October 2). *Aziatische Gaussian Robotics zet met next level robots stevige voet aan Europese wal.* Retrieved from: https://schoonmaakjournaal.nl/digitalisering-robotisering/aziatische-gaussian-robotics-zet-met-next-level-robots-stevige-voet-aan-europese-wal

[USP10] United States Patent (2010, November 9). Retrieved from: https://patentimages.storage.googleapis.com/df/1a/f6/71b47649d11aa2/US7831094.pdf

[Zhao20] Zhao, L. (2020, September 3). *Chinese Cleaning Robot Maker Gaussian Robotics Raises $22M In Series B+ Round.* Retrieved from Pandaily: https://pandaily.com/chinese-cleaning-robot-maker-gaussian-robotics-raises-22m-in-series-b-round/

About the authors

Ronald Heil MSc CISSP CISA GICSP is a partner at KPMG Cyber & Privacy. For the past 18 years he specialized in the field of IT and OT Security, Cyber Defense/Resilience, Threat and Vulnerability Management, IT-auditing and the security of Industrial Control Systems (ICS) and Industrial Internet of Things (IIoT).

Marnix Bel MSc is a former senior consultant at KPMG Cyber & Privacy and now works at Thales. He specialized in the field of Automotive Cyber Security, Security and Defence issues, including the nexus between Cyber, Military and Geopolitics and the Public Key Infrastructure (PKI) domain, providing independent assessments of the effectiveness of the architecture and security of PKI environments.