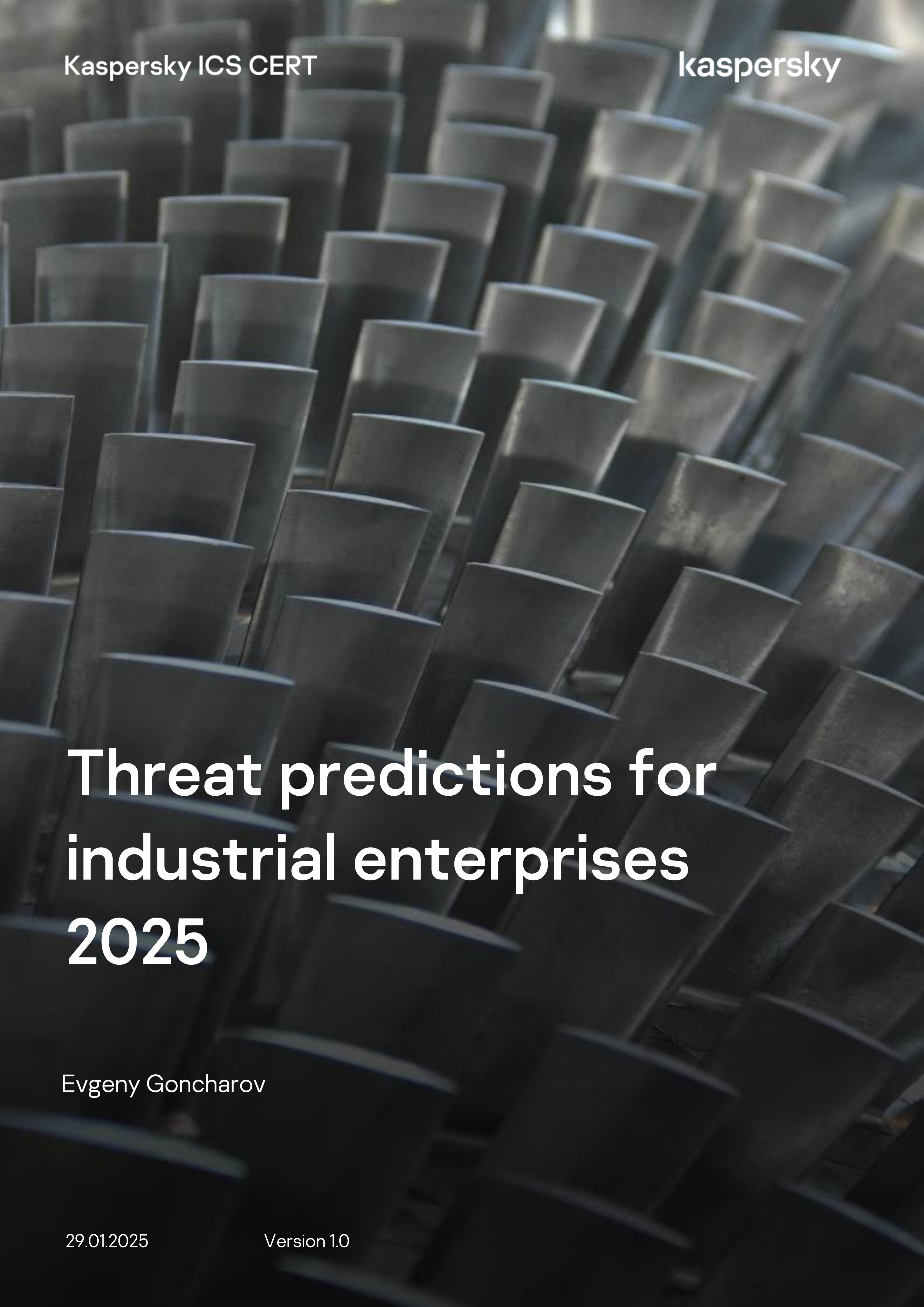
Kaspersky ICS CERT



Threat predictions for industrial enterprises 2025

Evgeny Goncharov

29.01.2025 Version 1.0

Key global cyberthreat landscape development drivers

Hunt for innovations

Innovations are changing our lives. Today, the world is on the threshold of another technical revolution. Access to new technologies is a ticket to the future, a guarantee of economic prosperity and political sovereignty. Therefore, many countries are looking for their way into the new technological order, investing in promising research and development in a variety of areas: AI and machine learning, quantum computing, optical electronics, new materials, energy sources and types of engines, satellites and telecommunications, genetics, biotechnology and medicine.

In terms of cybersecurity, growing interest in innovation means APTs are focusing on institutions and enterprises involved in new tech research and development. As the demand for the technical know-how grows, elite cybercriminal groups – such as top ransomware gangs and hacktivists – are also joining the game, hunting for the leading innovative enterprises' trade secrets.

Industrial enterprises should keep in mind that this information might be even easier to access and exfiltrate from the shop floor than from within research lab and office network perimeters. The supply chain and network of trusted partners are also very logical potential targets.

Intentionally created barriers and sanction wars

Increasing geopolitical turbulence, sanction wars, and the artificial restriction of access to efficient technology is boosting the drive to violate the intellectual property rights of leading enterprises. This may lead to the following security risks.

- OT technology developers and suppliers are facing the problem that existing mechanisms built into their products may no longer be effectively safeguarding their intellectual property.
- Cracks, third-party patches, and various other ways to bypass license restrictions, come at the price of increased cybersecurity risks right inside OT perimeter.
- In addition to stealing documentation related to cutting-edge technological developments, attackers will continue to hunt for technical know-how – for

example, collecting 3D/physical models and CAD/CAM designs as we saw in the attacks by Librarian Ghouls.
- PLC programs, SCADA projects, and other sources of technological process information stored in OT assets may also become another target for malicious actors.

New technologies mean new cyber risks

When trying something completely new, one should always expect some unexpected consequences in addition to the promised benefits. Today, many industrial enterprises are keeping up with organizations in other sectors (for example, financial or retail) in the implementation of IT innovations, such as augmented reality and quantum computing. As in many other fields, the biggest boost in efficiency is expected from the widespread use of machine learning and AI systems, including their direct application in production – when tweaking and adjusting technological process control. Already today, the use of such systems at certain facilities, such as non-ferrous metallurgy, can increase final product output by an estimated billion dollars per year. Once an enterprise experiences such an increase in efficiency, there's no going back – such a system will become an essential production asset. This may affect the industrial threat landscape in several ways:

- The improper use of AI technologies in the IT and operational processes of industrial enterprises may lead to the unintended disclosure of confidential information (for example, by being entered into a model training dataset) and to new security threats. The seriousness and likelihood of some of these threats is currently hard to assess.
- Both the AI systems and the unique enterprise data they use (either in its raw form – historical telemetry data – used as a training dataset, or as neural network weights incorporated into the AI model), if they become crucial assets, may now be new cyberattack targets. For example, if the systems or data get locked by the bad guys, they may be impossible to restore. Additionally, attacking these systems may not pose risks to the safety of the victim facility, unlike for traditional OT systems, meaning malicious actors may be more inclined to go for the attack.
- Attackers also do not ignore technical progress; their use of AI at various stages of the killchain (for malicious tools development and social engineering, such as text generation for phishing emails) reduces costs, thereby accelerating the development of cyberthreats. This tendency will certainly evolve in 2025.

Time-tested technologies mean new cyber risks

Just because a system has not been attacked, it doesn't necessarily mean that it is well protected. It could be that attackers have simply not reached it yet – perhaps because they already had simpler, more reliable and automated ways to perform attacks, or maybe you've just been lucky.

The expression "if it ain't broke, don't fix it" takes on a special meaning in OT infrastructures. Sometimes systems have been running for years or even decades without any modifications, even without installing critical security patches or changing insecure configurations, such as unnecessary network services, debug interfaces and weak passwords. Sometimes systems are still running in the exact same state as when they were put into operation.

Things get even more complicated when you take into account the poor quality of information about OT product vulnerabilities available from the developers or public sources. Fortunately, malicious actors still very rarely attack industrial assets and industrial automation systems.

Moreover, in addition to unprotected industrial automation systems such as PLCs and SCADA servers, which are in fact very difficult to keep cybersecure, there are many other types of devices and even entire infrastructures that are somehow connected to the technological network. The security of these systems is often unjustifiably overlooked:

- Telecom equipment. Its security is usually considered either the responsibility of the telecom operator or thought to be unnecessary for some reason. For example, mobile base stations and technological networks of mobile operators are believed to be already sufficiently protected from cyberattacks, which is why "no one attacks them". For some reason, this problem is largely ignored by security researchers as well: while the security of endpoints and their key components, such as modems, is thoroughly studied, there are extremely few in-depth publications on the security of base stations or core network equipment. However, the equipment can obviously be compromised, at least from the operator's side, for example, during maintenance. After all, telecom operators themselves are far from being immune to cyberattacks, as the story of the Blackwood attacks using the NSPX30 implant shows us. Thus, the following must be kept in mind:
    - At the very least, the threat model of industrial enterprises must include "man-in-the-middle" attacks on telecom equipment and the infrastructure of telecom operators.

    - Given how rapidly all kinds of smart remote monitoring and control systems are being implemented – primarily in mining and logistics, but also in other sectors and types of facilities – the priority of securing telecom-related infrastructures will only increase correspondingly. For example, to guarantee the safety of robotized infrastructures and the use of automated transport at facilities, we're seeing the introduction of wireless communication. Industrial enterprises should clearly invest in telecom security in order to avoid cyberincidents, perhaps as early as this year.

- The security of smart sensors, meters, measuring and control devices, and other devices in the Industrial Internet of Things is typically neglected by both the enterprises using them and, correspondingly, the developers themselves. However, as the history of FrostyGoop shows, these devices may also become attack targets.

- The connection points of small remote industrial infrastructure facilities typically use inexpensive network equipment, sometimes not even designed for industrial use (for example, SOHO devices). Their cybersecurity can be extremely difficult to keep in good condition, both due to architectural limitations and the complexity of centralized maintenance. At the same time, such devices can be manipulated not only to distribute general-purpose malware or host botnet agents (as in the case of Flax Typhoon/Raptor Train), but also as an entry point into the IT or OT network.

- The Windows OS family has been the most popular platform for workstations and automation system servers for decades. However, in recent years, many industrial enterprises have been increasingly installing Linux-based systems in their OT circuits, for various reasons. One of the decisive arguments in favor of choosing Linux is often the belief that such systems are more resistant to cyberattacks. On the one hand, there is indeed less malware that can run on this OS, and the probability of accidental infection is lower than for Windows OS. On the other hand, protecting Linux systems against a targeted attack is just as difficult, and in some cases even more so. The fact is that:

    - Developers of security solutions for Linux have to catch up with solutions protecting Windows infrastructure. For a long time, many functions were not in demand by customers and, therefore, were not implemented. At the same time, implementing new functionality is more expensive because it is necessary to support multiple OS strains developing in parallel, and the integration of security solutions is not a priority for kernel developers. There are two downstream consequences of this: first, a lack of effective standard integration mechanisms, and second, updating the kernel can easily "break" compatibility – and a simple module rebuild may not be enough.

- On the industrial enterprise side, there are clearly not enough information security specialists who are also Linux experts, so both secure device configuration and monitoring and incident detection may not be that effective.
- Both Linux OT solutions themselves and their developers often demonstrate insufficient information security maturity and can be an easy target for attackers, as was revealed, for example, during the investigation of a series of Sandworm attacks on Ukrainian critical infrastructure facilities.

Wrong vendor choice means big trouble

Insufficient investment of product developers or technology providers in their own information security guarantees that their customers will experience incidents. This problem is especially relevant for providers of niche products and services. An illustrative case is the attack on CDK Global, which led to direct losses of its customers exceeding a total of one billion dollars.

The situation for industrial enterprises is complicated by a number of factors. Key among these are:

- Extremely long technology supply chains. Equipment, including automation systems for key production assets, is very complex. An enterprise's industrial equipment fleet may include both all the main components typical of IT systems and many components created as a result of cooperation between multiple manufacturers of industry-specific technologies. Many of these may be relatively small developers of niche solutions without the necessary resources to satisfactorily ensure their own security and that of their products. Moreover, the installation, initial setup, and regular maintenance of equipment requires the involvement of various third-party specialists, further expanding the attack surface of the supply chain and trusted partners.
- Almost every large industrial organization is its own vendor. The specifics of the particular industry and enterprise require significant modification of ready-made solutions, as well as the development of new automation solutions tailored for the organization. Often, these developments are

carried out either within the organization itself or by subsidiaries or related companies. All of this multiplies almost all of the risk factors described above: such developments are rarely carried out with a high level of security maturity, resulting in solutions full of basic vulnerabilities that even mediocre attackers can exploit. Obviously, these security issues are already being used in cyberattacks and will continue to be.

Security by obscurity doesn’t work anymore for OT infrastructures

The availability of so many tools for working with industrial equipment (just count the number of libraries and utilities implementing industrial network protocols posted on GitHub) makes developing and implementing an attack on an industrial enterprise’s main production assets significantly easier than just a few years ago. In addition, industrial enterprises themselves continue to evolve – over the past few years, we’ve seen big efforts to not only automate production, but also to inventory and document systems and processes. Now, to impact an industrial facility on the cyber-physical level, attackers no longer need to carefully study textbooks on the particular type of protective systems (such as SIS or circuit/relay protection) basics and to involve external experts in the particular industry. All the necessary information is now available in convenient digital form in the organization’s administrative and technological network. We have seen cases of attackers telling journalists that after they entered the victims’ network perimeter they studied internal facility’s safety-related documentation for a long time before choosing which OT systems to attack, in order to avoid putting employee’s lives at risk or polluting the environment as a result of the attack.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global project of Kaspersky aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com