

Research on Cyberspace Protection Strategy of Industrial Enterprises under the Background of Digital Transformation—China National Petroleum Corporation Case Study

Angze Li^{1*}

¹School of Cyber Science and Engineering, Sichuan University, Chengdu, Sichuan, 610207, China

Abstract. This research uses the China National Petroleum Corporation (CNPC) as a case study to explore the cybersecurity measures of industrial businesses amid digital transformation. As the rapid adoption of digital technologies reshapes the oil and gas sector, the study underscores the critical importance of robust cybersecurity frameworks. The case description delves into CNPC's current state of development, and the significant cybersecurity challenges it faces during its digital transition, such as internal threats, outdated infrastructure, and vulnerabilities in industrial control systems. The study identifies several critical issues, including a lack of cybersecurity awareness, limited capabilities for responding to cyber incidents, and inadequate integration between information technology (IT) and operational technology (OT) security. These challenges are largely driven by the swift pace of digital transformation, dependence on legacy systems, and the evolving nature of cyber threats. To address these concerns, the study offers several strategic recommendations: moderating the speed of digital transformation, fostering IT and OT security convergence, enhancing employee cybersecurity awareness, and fortifying the security of industrial control systems. The findings emphasize that aligning digital innovation with cybersecurity is essential to ensure that the implementation of new technologies does not compromise safety or operational integrity. For CNPC and other industrial enterprises, the study provides valuable guidance on safeguarding critical infrastructure and maintaining operational resilience in an increasingly digital world.

1 Introduction

1.1 Research background

In the broader sense of digital transformation, industrial companies face new and serious challenges, though there are also new opportunities. With information technology undergoing quick developments, these companies are moving away from methods that were

* Corresponding author: fenglian@ldy.edu.rs

more traditional to ones that are now more digital and smart. This kind of transition has the effect of making production and operations more efficient, and it can also increase the competitiveness of these companies in the global market. Nonetheless, cybersecurity remains a pressing issue and is growing more so. More recent statistics have shown a rise, around 45%, in the attacks on global industrial control systems (ICS) in the year 2023 compared to the prior year [1]. These cyber-threats present risks that extend beyond just production safety; they have implications that can be large for the financial interests of companies and their reputations, too.

In view of this, it is important to investigate cyberspace protection tactics for industrial companies undergoing digital transformation. First off, as the Industrial Internet of Things (IIoT) becomes more widely used, more systems and equipment are linked to networks, expanding the number of possible targets and attack surfaces for cybercriminals. This means that businesses need to deal with operational technology (OT) system security issues, which are more complicated than typical IT system security. Second, industrial companies' production control systems frequently involve vital infrastructure. Thus, any attack might have a big impact on the social and economic stability of the country. As a result, safeguarding industrial companies' cybersecurity during their digital transformation has significant societal and economic implications.

1.2 Literature review

Numerous academics have studied cybersecurity concerns in industrial businesses in recent years. For instance, Zhang et al. discovered that during digital transformation, internal employee malice, data breaches, and cyberattacks pose the most cybersecurity risks to industrial enterprises [2]. To counter these risks, they advise businesses to implement multi-layered security measures like intrusion detection systems, firewalls, and data encryption technologies.

Additionally, Tan et al. investigated how to use IIoT to save operating costs and increase production efficiency. Nevertheless, they also noted that IoT devices are more susceptible to intrusions because of their dispersed architecture and resource limitations [3]. When implementing IIoT, they advise businesses to give special consideration to the security of these devices and to take precautions such as end-to-end encryption and device authentication to avoid security flaws.

Zhou et al.'s investigation on the cybersecurity of vital infrastructure is another pertinent study. They suggested that there are still serious weaknesses in the security of OT systems, even though industrial companies have implemented several security measures to safeguard their IT systems [4]. They recommend that businesses strengthen the defenses against potential attacks on OT systems, with a special emphasis on the security of SCADA (Supervisory Control and Data Acquisition) systems.

Last but not least, research by Jiao examines the complexity of cybersecurity issues that industrial firms encounter when undergoing digital transformation. He stresses that new risks are introduced by the convergence of IT and OT systems as these businesses use digital technology in their operations more and more [5]. He contends that especially in light of advanced persistent threats (APTs) that target vital infrastructure, conventional cybersecurity solutions are inadequate to counter these new dangers. He advises a comprehensive approach to cybersecurity that incorporates incident response plans designed especially for the industrial sector, integration of threat intelligence, and ongoing monitoring. He also stresses the significance of developing an organizational security culture in order to reduce the risks associated with human factors, such as insider threats and inadvertent mistakes. This research underscores the necessity for industrial enterprises to adopt a multi-faceted approach to cybersecurity that not only protects against external

threats but also addresses internal vulnerabilities during their digital transformation journey.

Although many scholars have researched the cyber security of industrial enterprises, most of the research focuses on the protection measures against cyber attacks and the security of IoT devices [2,3,5]. Few scholars have deeply discussed how to achieve data compliance and privacy protection while ensuring network security in the context of digital transformation [4]. In addition, although there is some research on the security of OT systems, the research on coping with complex attack means and meeting the requirements of new regulations is still insufficient. These understudied areas constitute the research blank of this paper.

2 Case description

2.1 Basic information

The China National Petroleum Corporation, which is called CNPC, is among the biggest and most influential state-owned enterprises in China. Its main focus is on things like exploration, production, and the sale of oil and gas. In 1988, it was founded, and since that time, the role that CNPC plays in China's energy sector has been very significant. It is also a company that participates in the global petroleum industry, with activities happening not just in China but in more than 30 countries as well. The company has over 1.2 million people working for it. CNPC's operations, which are quite extensive, involve many aspects of the petroleum industry, and these range from the early stages of exploration and production to later processes like refining and also marketing. This whole value chain of the petroleum industry is something that CNPC is involved in.

2.2 Development status

In recent times, CNPC has attempted to follow the path of digital transformation with vigor, though how effectively this path has been followed remains a point of various interpretations. The pursuit of making their operations more effective, which is said to preserve their position in the world energy market, has been a focus, although what this effectiveness precisely means might not be easily pinpointed. The company, as has been indicated, has taken steps towards bringing into its processes certain technologies that are often labeled as advanced, including what is termed big data, as well as artificial intelligence (AI), and there is also mention of the Internet of Things (IoT). Through what is said to be the use of these technologies, CNPC claims to have made advancements such as digital refineries and smart oilfields, where there is an intention to maximize output, which is supposed to be achieved alongside reducing costs and improving safety, though the exact outcomes may vary. An initiative that has been highlighted and perhaps given some emphasis is the "CNPC Digital Oilfield" program.

2.3 Cyberspace protection challenges during digital transformation

As the digital transformation is advanced within China National Petroleum Corporation (CNPC), the protection of important infrastructure from various cyber threats becomes increasingly crucial and serious. The expanding use of digital technologies by CNPC in its operations has led to a wider attack surface, thus exposing and making it more vulnerable to various types of cyber-attacks. This is an issue of significant concern, considering CNPC's

strategic importance to China's overall energy security and its significant position in the global oil and gas industry.

Among the main challenges faced by CNPC are the security problems related to its industrial control systems (ICS) and its supervisory control and data acquisition (SCADA) systems. These systems, which are essential for the operation of oilfields and refineries, present substantial challenges. These systems, which were once more often disconnected and kept isolated from the Internet, are now becoming increasingly connected to wider corporate networks and cloud-based platforms. This process has been driven by the company's ongoing digital transformation efforts. With the increase in connectivity, ICS and SCADA systems are finding themselves more and more exposed and at risk, vulnerable to various potential cyber threats, including advanced persistent threats (APTs), which can disrupt operations or cause considerable damage to critical infrastructure [6].

The challenges being addressed by CNPC are through a cybersecurity strategy, a strategy that can be said to be comprehensive but also involves various aspects. Advanced security technologies have been deployed, but systems of defense that have multiple layers have also been established. CNPC has made significant investments, allocating resources toward next-generation firewalls and intrusion detection systems. There are also systems for managing security information and events, known as SIEM. The intention behind these deployments is the monitoring and protection of digital infrastructure, which could be described broadly as such. A Cybersecurity Operations Center, or CSOC, has been put in place by CNPC, which is dedicated to overseeing efforts that pertain to cybersecurity and coordinating necessary responses for potential incidents that might occur.

In addition, CNPC works toward building what is considered a culture of cybersecurity within the organization. Training programs, which are on an extensive scale, have been put in place with the purpose of raising awareness among employees about the risks associated with cybersecurity. These programs also ensure that best practices are followed across all levels of the organization. The human element, being crucial in cybersecurity, is recognized by CNPC, which emphasizes continuous education and vigilance to prevent threats that might arise from insiders and social engineering attacks.

3 Analysis on the problem

3.1 Cybersecurity challenges posed by digital transformation

Operational efficiencies and competitive advantages achieved by China National Petroleum Corporation (CNPC) in the global energy industry have been achieved, but the pathway through which this has occurred involves digital transformation. These advances, while offering potential benefits, they also bring cybersecurity challenges. Not managed well, such challenges could become a threat to energy security in China, but not just there—it might also have broader consequences for CNPC, and implications could extend to the global oil and gas industry, where the impact could be significant.

3.1.1 *Industrial control systems are vulnerable to increased attacks*

In the digital transformation process of CNPC, the matter of cybersecurity raises issues that cannot be ignored, one of which is that industrial control systems (ICS) are now exposed to heightened risk. These systems were once, as was usual, kept apart from the Internet, a separation that served as a barrier, providing some defense against the possibility of cyberattacks. But now, with the increased digitization of CNPC's operations, the connection of ICS with cloud platforms and enterprise networks is seen as something that cannot be

avoided. This shift increases the potential points of vulnerability, making ICS more susceptible to cyber threats [7].

As ICS connectivity increases, new avenues of attack, such as advanced persistent threats (APTs) and malware, have appeared. Serious consequences, like financial losses that are significant, operational disruption, and risks to security, can result from a cyber attack on these systems. For instance, if an attack happens on a supervisory Control and Data acquisition system (SCADA), disruption of processes, which might include oil extraction, refining, or distribution, could be caused by manipulating operational parameters. This disruption not only affects operations but may also bring about threats to both the environment and public safety.

3.1.2 Problems in protecting the old system

Challenges were also observed in the protection of legacy systems within the CNPC infrastructure. Reliance by much of CNPC's business on older systems, which were not designed with consideration for modern cybersecurity threats, was a concern. These older systems often do not align well with current security solutions, which increases the difficulty of protection. As CNPC continues pushing for digitalization, integration with new technologies and these older systems might produce vulnerabilities, thus turning into targets for cybercriminals. CNPC requires a significant investment in both technology and experience to protect these aging systems. Furthermore, the process is complicated by these systems, which often lack uniformity in security rules, making it harder to establish a coherent cybersecurity strategy.

3.1.3 Human factors and Internal threats

The element of the human factor, which continues to be a prominent and significant challenge that is very much present in the CNPC's overarching and all-encompassing strategy concerning cybersecurity, is something that, despite the relentless march and ongoing progression of technological advancements, persists in demanding attention. The awareness of security by employees, alongside their alertness and capacity for vigilance, remains vital, even to the cybersecurity endeavors that CNPC undertakes. The risks that originate from within, those of the insider variety, whether arising from negligence that is not intentional or actions that are indeed intentional and harmful, constitute a serious and substantial threat to the digital infrastructure of CNPC. Phishing attacks, which are among various social engineering attacks, exploit vulnerabilities that are not physical but psychological in nature—these vulnerabilities inherent in human psychology, which allow unauthorized and unwanted access to systems, are exploited, leading to breaches that could be prevented were it not for the human element.

3.2 Analysis of identified problems

3.2.1 Insufficiency of IT and OT security integration

During CNPC's digital transformation, it was found that a major issue existed, which was the integration of IT security with operational technology (OT), which was not sufficient. IT security and OT have been working separately for a while, and now, as the digital transformation progresses, these systems have begun to merge. The security requirements between IT and OT differ a lot. While OT security focuses mainly on the security and continuous operation of physical processes, IT security is more about the confidentiality

and availability of data. To ensure that each system addresses different threats, combining them is important, and an extensive security framework is needed for that.

3.2.2 Limited cybersecurity expertise

A problem faced by businesses is a shortage of cybersecurity knowledge. With the growth of CNPC's digital business, the need for cybersecurity experts is increasing. However, the fast pace of digital transformation makes it harder for businesses to hire and train employees with the right skills to manage and secure complex digital infrastructures.

The global problem, which is the lack of skill in cybersecurity, is something seen worldwide, but there are some sectors where it is found particularly severe, such as oil and gas, and in those sectors, physical security has always been the priority. CNPC, in this case, must take action regarding its cybersecurity strategy so that talent in the cybersecurity industry can be attracted, retained, and also cultivated. To achieve this, it may be necessary to consider investing in the ongoing professional development of existing personnel, and partnerships with academic institutions could also be considered, or maybe participating in programs aimed at cybersecurity talent development.

3.2.3 Insufficient cyber event response capabilities

As the complexity of cyber threats increases more and more, it might be said that CNPC's current capabilities in cyber incident response might not be as sufficient as needed. There is a growing risk of a cyber incident as organizations become more digital, and this risk also becomes more significant. There would be a need for advanced tools for detection and monitoring to respond to incidents in an effective way, along with a response strategy that has been rehearsed so the impact of any attack can be reduced. Although a Cyber Security Operations Center (CSOC) has been established by CNPC, which can be seen as a positive action, there is nevertheless much that remains to be done to enhance the capabilities of the organization in responding to incidents.

3.3 Analysis of the causes of the problems

3.3.1 Rapid pace of digital transformation

Within CNPC, the transformation that is happening in the digital sense is where issues have been found, with speed being a significant factor. The company's aspirations, which are quite high, do not align with its capacity to establish strong measures for cybersecurity. It is in the process of integrating digital technologies, and in doing so, the security aspect is not given adequate consideration. Therefore, new technologies are being put into place without sufficient attention to security, leading to an increase in attack surfaces, and consequently, a higher susceptibility to cyberattacks is observed among people.

3.3.2 Legacy infrastructure and technical debt

Furthermore, there is the matter of outdated infrastructure, which exists within CNPC's operations, and this is coupled with the buildup of technical debt. These are also major causes. Several issues related to cybersecurity have been connected to the challenge of protecting systems that are old and not designed to withstand cyberattacks of a contemporary nature. The continued reliance on these systems is what leads to vulnerabilities, and these vulnerabilities are both costly and complicated to fix.

3.3.3 Organizational silos and lack of cross-functional collaboration

The CNPC's organizational silos have also exacerbated the cybersecurity issues. The creation of a unified cybersecurity strategy has been hampered by divisions between the IT and OT departments as well as between various business units. Because of this lack of cross-functional cooperation, security measures have become fragmented and are unable to fully address the range of dangers related to digital transformation [8].

4 Suggestions

Cybersecurity problems have surfaced as China National Petroleum Corporation (CNPC) has used digital transformation to attain notable operational efficiency and competitive advantages in the global energy business [9]. In addition to posing a danger to China's energy security, these problems could have a big effect on the world's oil and gas market if they are not adequately resolved [10]. In light of the aforementioned analysis, this paper offers a number of suggestions to assist CNPC in addressing the cybersecurity issues associated with digital transformation while also preserving the enterprise's security and long-term growth.

4.1 Strengthen the safety of industrial control systems

Within CNPC, the transformation that is happening in the digital sense is where issues have been found, with speed being a significant factor. The aspirations of the company, which are quite high, do not align with its capacity to establish strong measures for cybersecurity [11]. It is in the process of integrating digital technologies, and in doing so, the security aspect is not given adequate consideration. Therefore, new technologies are being put into place without sufficient attention to security, leading to an increase in attack surfaces, and consequently, a higher susceptibility to cyberattacks is observed among people.

Furthermore, there is the matter of outdated infrastructure, which exists within CNPC's operations, and this is coupled with the buildup of technical debt. These are also major causes. Several issues related to cybersecurity have been connected to the challenge of protecting systems that are old and not designed to withstand cyberattacks of a contemporary nature. The continued reliance on these systems is what leads to vulnerabilities, and these vulnerabilities are both costly and complicated to fix.

4.2 Promote the effective integration of IT and OT security

For digital transformation to be driven, CNPC needs IT and OT security integration to be done successfully, with information technology and operational technology being integrated securely. To guarantee this, a thorough security architecture by CNPC is necessary to ensure that IT and OT security policies are synchronized. To remove impediments that are present organizationally, the first step should be the setup of a working group with responsibility, a group that is cross-departmental, for coordinating collaboration between departments, particularly those concerning IT and OT. Alongside this, uniform security guidelines and procedures are needed to guarantee that IT systems, when combined with OT systems, maintain security and interoperability. Also, CNPC should consider investing in multiple security layers, such as firewalls, VPNs, and network segmentation, so that attackers, after breaking into one system, cannot easily scale the entire network.

4.3 Regulate the pace of digital transformation appropriately

Due to the security risks that are caused, in part, by the rapid speed of such changes, it is necessary for CNPC to have a plan for digital transformation [12]. This plan must be broad and thorough, covering all aspects. Within this plan, there should be security evaluations at every phase and stage of the entire process. These security evaluations, once completed, should be utilized as a basis for adjusting both the pace and the direction of the ongoing transition to make sure that security, in all its forms, is fully accounted for. The implementation of any new technology should proceed in a staggered, gradual manner, rather than all at once, to ensure any security vulnerabilities that might possibly arise are detected and corrected well before a full launch takes place. Also, to minimize risks that are associated with external factors and elements outside the company's control, CNPC ought to improve how it collaborates with third-party suppliers and must verify that all technologies and services that are in use adhere to, and comply with the company's own rigorous security standards and requirements.

5 Conclusion

5.1 Conclusion of key findings

This study took upon itself the task of looking into the cybersecurity difficulties that CNPC encountered throughout its journey toward digital transformation. The analysis focused particular attention on security issues in both information technology (IT) and operational technology (OT). Some primary issues they noted included the lack of sufficient integration between the security of IT and OT, the shortage of expertise in cybersecurity, and the inability to respond to cyber incidents. What was observed to be the reasons behind these challenges was the fast pace of digital transformation, along with a reliance that remained on legacy infrastructure, and there were also organizational silos contributing.

Several suggestions were offered to address the problems mentioned. To begin with, it was suggested that a security structure, one that is cohesive and covers both IT and OT, be implemented to protect the organization from cyberattacks across its entire operational landscape. The security framework should include, among other things, the practice of conducting regular assessments of risks, having an integrated Security Operations Center (SOC), and facilitating cross-training programs for staff in both IT and OT. Moreover, it is important that CNPC improves its cybersecurity capabilities. This improvement might be achieved through various methods, such as cultivating internal talent, partnering with academic institutions, and better strategies for recruitment and retention. Additionally, CNPC's response capabilities for cyber incidents should be strengthened, and this can be done through activities like conducting exercises on a frequent basis, making investments in advanced systems for detection and monitoring, and performing analyses after events have occurred, to better its future response tactics.

The importance of balancing cybersecurity with the transformation of the digital is also emphasized by the author, who insists on the necessity of doing so. It is recommended that one consider the calculated risk of the inclusion of security matters in each phase of the digital adoption process. Lastly, managing aging infrastructure, along with technological debt, becomes necessary if one is to reduce risks, which, therefore, ensures the digital environment remains safe.

5.2 Research significance

The research, in its essence, is of notable importance to CNPC, as well as to the oil and gas sector at large, in ways that could be considered significant. As the use of digital technology is increasingly common, the necessity for robust measures in cybersecurity is recognized. This report provides, in a manner perhaps more suggestive than definitive, a kind of roadmap, so to speak, for CNPC to secure what can be broadly described as its digital assets while maintaining, in some respect, operational resilience. It does this by presenting what could be regarded as major cybersecurity issues alongside what might be thought of as actionable solutions. By implementing, or at least considering the recommended strategies, CNPC's stance on cybersecurity could, theoretically, be enhanced, thus creating a form of benchmark for others in the industry who may encounter similar challenges.

5.3 Limitations and future studies

While the report contains insightful information, it also contains flaws in CNPC's cybersecurity issues, which means that the report is not flawless. The research mostly relies on secondary data sources like industry reports, internal evaluations, and published works that have already existed. Because there is no direct data, like interviews with CNPC's cybersecurity staff in person or surveys of stakeholders, the results are not very comprehensive, nor are they very specific, which could be said to limit them. The focus on CNPC is narrow, which means that some of what is found might not apply completely to other organizations in different contexts or industries that are not the same.

Future research could possibly try to deal with these issues by using primary data-gathering methods, such as interviews and surveys so that understanding might be more comprehensive regarding CNPC's particular cybersecurity problems and solutions, but also not necessarily exclusive to it. These methods could lead to advice that is more personalized, as well as a deeper understanding that might be detailed of the difficulties in the real world that cybersecurity teams are facing.

The studies, if tracking the implementation of those recommended solutions, might, over a period of time, be found to provide assistance in the assessment of their effectiveness, which would also be useful in identifying any new issues. Research endeavors, furthering in nature, could potentially and possibly explore the application of technologies that are emerging, which may include, for instance, artificial intelligence as well as machine learning, with the intention to perhaps enhance cybersecurity in the broad and complex domain of the oil and gas industry.

References

1. Du, H. T., & Li, Y. Z. (2024). Research on cybersecurity protection mechanisms in foreign digital factories: A case study of Lockheed Martin. *Cybersecurity and Data Governance*, **5**, 11-17.
2. Zhang, G., Zhang, Y., & Liu, Z. Y. (2022). Thoughts and practical paths for building cybersecurity capabilities in the digital transformation of industrial enterprises in China. *Industrial Information Security*, **5**, 43-47.
3. Tan, J. F., Zeng, Y., Pang, M., Yang, Y., & Deng, Q. Z. (2023). Discussion on cybersecurity measures in the digital transformation of petroleum enterprises. *Cybersecurity Technology and Application*, **7**, 128-130.

4. Zhou, X., & Sun, Y. Data compliance and privacy protection in industrial enterprises. *Journal of Cybersecurity*, **9**, 125-138 (2023).
5. Jiao, M. (2023). Analysis and coping strategies of cybersecurity issues in the context of digital transformation. *Cybersecurity Technology and Application*, **8**, 158-160.
6. Zhang, M., & Wei, J. (2024). Analysis of path selection for digital transformation in petrochemical enterprises. *China Petroleum Enterprises*, **3**, 96-101.
7. Li, Y., Yan, F., Wang, Y., Wu, Q., & Wang, L. (2024). Cybersecurity in industrial control systems for oil and gas pipelines. In *Proceedings of the 2024 World Intelligence Congress Artificial Intelligence Security Governance Forum* (pp. 126-129). National Pipeline Corporation Oil and Gas Regulation Center; National Pipeline Corporation Production Department; National Pipeline Corporation Northeast Company.
8. Zhang, S., & Li, Q. Overcoming Organizational Silos in Cybersecurity: A Case Study (2023).
9. Chen, S. (2024). Cybersecurity: The ballast for the development of digital transformation. *Computer Simulation*, **5**, 400-404.
10. Shen, D., Qiao, D., Xin, H., Zhang, N., & Li, Q. (2022). Research on cybersecurity management in energy enterprises. *China Management Informationization*, **10**, 110-112.
11. Huang, T., Wang, Z., Liu, J., Long, Q., Kuang, B., Fu, A., & Zhang, Y. (2024). A review of research on the security of industrial control protocols. *Journal of Communications*, **6**, 60-74.
12. Li, H., & Li, Z. (2024). The impact of digital transformation on high-quality development and high-speed growth of enterprises: An examination from the perspective of "quality reform, efficiency reform, and power reform". *China Rural Economy*, **4**, 120-140.