ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
РУТ (МИИТ)

ЮРИДИЧЕСКИЙ ИНСТИТУТ

Минтранс России

Ространснадзор

Росжелдор

Программа
V Международного транспортно-правового форума

«ПУБЛИЧНО-ПРАВОВЫЕ ПРОБЛЕМЫ ТРАНСПОРТНОГО ПРАВА»

15—16 февраля 2023 г.
г. Москва

Информационные партнеры форума

юрист
издательская группа

КонсультантПлюс
надежная правовая поддержка

Cybersecurity Challenges in the Transportation Industry

Проблемы кибербезопасности в транспортной отрасли

Dr. Habib Badawi

https://www.ul.edu.lb/common/news.aspx?newsId=1683&lang=2

Lebanese University – Beirut - Lebanon

habib.badawi@ul.edu.lb – habib.badawi@gmail.com

https://orcid.org/0000-0002-6452-8379

Управляющее резюме

По данным Всемирного экономического форума, Кибератаки (Cyberattack), наряду с оружием массового уничтожения и изменением климата, являются пятой по серьезности глобальной угрозой. К 2025 году стоимость атак вырастет до $10,5 трлн по сравнению с $3 трлн в 2015 году. Например, в последние годы кибератакам подверглись крупнейшие нефтепроводы в США, а центрифуги в ядерных реакторах Ирана были саботированы.

Кибератаки (Cyberattack) стали инструментом для осуществления глобального влияния и международной конкуренции, чтобы вывести из строя жизненно важные сайты для стран из-за информационной революции. В ответ на растущую зависимость от компьютеров во всех аспектах жизни страны во всем мире были вынуждены усилить свои кибернаступательные возможности. В результате они усилили свою электронную защиту от них, тем самым укрепив свой защитный иммунитет против них.

1- Модели кибербезопасности для транспортного сектора.

2- Важность кибербезопасности:

i. Кибератаки (Cyberattack) дешевы по сравнению с другими инструментами власти.
ii. Разрушительное воздействие кибератак широкомасштабно.
iii. Сложность определения того, кто стоит за кибератаками.
iv. Скорость реализации поражающих целей.

3- Опасность кибератак на безопасность, международную экономику и транспортные маршруты.

4- Важность разработки законов о кибербезопасности в транспортном секторе.

Заключительные замечания

будущем руководители информационных технологий (ИТ) и руководители транспортного сектора должны уделять пристальное внимание следующим целям сокращения:

i. Внедрение интеллектуальной автоматизации.
ii. Применение аналитики для помощи в принятии решений.
iii. Повышение приоритета кибербезопасности.

Международное сообщество может снизить киберугрозы, поддерживать соответствие отраслевым и государственным стандартам и минимизировать финансовые последствия взлома путем внедрения самых современных передовых методов обеспечения безопасности и технологических решений. ИТ-руководители должны заранее иметь надежные программы управления рисками, оценки зрелости безопасности и планы действий.

Это повысит уровень безопасности их стран как для пассажирских, так и для грузовых перевозок.

Introduction

According to the World Economic Forum, cyberattacks, weapons of mass destruction, and climate change are the three most serious global threats. Attacks will cost $ 10.5 trillion by 2025, up from $ 3 trillion in 2015[1]. For example, in recent years, the largest oil pipelines in the United States have been subjected to cyberattacks[2], and centrifuges in Iran's nuclear reactors have been sabotaged[3].

Cyberattacks have become a tool for exercising global influence and international competition to disrupt vital sites for countries because of the information revolution. In response to the increasing dependence on computers in every aspect of life, nations worldwide have been forced to enhance their cyber-offensive capabilities. As a result, they have strengthened their electronic defenses against them, thus strengthening their defensive immunity against them.

1- Cybersecurity models for the transportation sector

In 2003, the Pentagon accused China for the first time of being responsible for a series of cyberattacks on government computer systems centered on key Défense Department contractors[4]. These attackers were able to obtain sensitive information that threatened national security[5].

In the Middle East, in 2012, about 30,000 Saudi Aramco computers were disrupted due to a cyberattack by the Shamoon virus[6]. Moreover, in 2016, services were disrupted at some Saudi government agencies. This was in addition to disabling the websites of the Ministries of Labor, Communications, and Information Technology, the Ministry of Defense, and the Ministry of the Interior. These Saudi governmental websites contain internal traffic systems[7].

---

[1] Steve Morgan. (2020, November 13). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[2] David E. Sanger, Clifford Krauss, Nicole Perlroth. (2021, May 8). *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*. The New York Times. https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

[3] Ronen Bergman, Rick Gladstone, Farnaz Fassihi. (2021, April 11). *Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage*. The New York Times. https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html

[4] Ball, Desmond. "China's Cyber Warfare Capabilities." *Security Challenges* 7, no. 2 (2011): 81–103. http://www.jstor.org/stable/26461991.

[5] Jeff Jones. (2020, May). *Confronting China's efforts to steal defense information*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information

[6] Editorial, R. (2012, December 9). *Saudi Arabia says cyber-attack aimed to disrupt oil, gas flow*. Reuters. https://www.reuters.com/article/saudi-attack-idUSL5E8N91UE20121209

[7] Christopher Bronk & Eneken Tikk-Ringas (2013) *The Cyber Attack on Saudi Aramco,* Survival, 55:2, 81-96, DOI: 10.1080/00396338.2013.784468

Colonial Pipeline, the largest U.S. pipeline operator, shut down its entire network after a ransomware-induced cyberattack[8].

In Germany, Oil Tanking Deutschland GmbH & Co. KG, which stores and transports oil, faced an unprecedented cyberattack that cut off gasoline supplies in the country's north[9]. The next day, vital facilities in Belgium and the Netherlands were similarly attacked after their oil facilities in ports were hit by a cyberattack[10]. Belgian companies C-Invest and Evos reported cyberattacks that crippled information systems and hampered the operation of ports.

In the Russian Federation, many studies indicate that cyberattacks have become the most effective tools of American aggression. This is what Russian Deputy Foreign Minister Oleg Syromolotov said in an interview with the Novosti News Agency. Most of the cyberattacks on Russia in 2020 were conducted from addresses registered in Western countries, and it was revealed that these attacks targeted facilities and sites related to vaccine design, government departments, financial sector institutions, military-industrial complex institutions, scientific and educational facilities and institutions, health care centers, and public transport institutions[11].

2- Global threats to cybersecurity

Cyberattacks have increased significantly recently, and there are estimates that a cyberattack occurs every 39 seconds[12]. This can be explained by considering the following factors and considerations:

a) Cyberattacks are low-cost when compared to other sources of power. Studies indicate that hacking tools have become less expensive and more accessible. This allows those who resort to them, whether countries, institutions, or individuals, to inflict severe damage for a small percentage of the previous cost. In total, these attacks cost only 4% of the price of a military vessel. Therefore, there is some indication that an entire cyberwar can be financed via the Internet at the expense of one tank.

---

[8] Ellen Nakashima, Yeganeh Torbati and Will Englund. (2021, May 8). *Ransomware attack leads to shutdown of major U.S. pipeline system*. The Washington Post. https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/

[9] Joe Tidy. (2022, February 1). *Cyber-attack strikes German fuel supplies*. BBC News. https://www.bbc.com/news/technology-60215252

[10] Prajeet Nair. (2022, February 5). *Cyberattack cripples European oil Port terminals*. Bank information security news, training, education - BankInfoSecurity. https://www.bankinfosecurity.com/cyberattack-cripples-european-oil-port-terminals-a-18465

[11] Xinhua. (2022, December 29). *Facts about Russia-Ukraine conflict: Russian deputy FM says west uses Ukraine to launch cyberwar*. People's Daily. https://en.people.cn/n3/2022/1229/c90000-10189727.html

[12] Matias Madou. (2022, November 7). *Cybersecurity: A global priority and career opportunity*. University of North Georgia. https://ung.edu/continuing-education/news-and-media/cybersecurity.php

b) The destructive impact of cyberattacks is wide-ranging. Cyberattacks are often devastating and may lead to complete paralysis of the infrastructure of countries in areas and sectors that are related to human life. This is especially evident in the fields of public health, electricity networks, water, communications, and transportation. A state that conducts a cyberattack on one of these sectors is enough to end life.
c) The difficulty of knowing who is behind cyberattacks This critical issue is difficult to detect. This makes it difficult to know who is behind it. This is evidenced by the fact that the investigation processes for these attacks take months and often end without identifying who carried them out. This is because these attacks are part of the covert wars that turn into electronic systems and precede military action.
d) The frequency at which harmful targets are implemented. Cyberattacks take only a brief time to implement their objectives, compared to conventional warfare, which takes years to resolve. More than seventy-four countries worldwide were exposed to the virus in May 2017. These countries were hit by severe, simultaneous cyberattacks that hit major countries such as China and Russia. According to some experts, these attacks are dangerous and terrifying because they can potentially disrupt life in many countries around the world. In addition, they can happen in record time.

3- The dangers of cyberattacks on security, the international economy, and transportation routes.

There is no doubt that the increasing resort to cyberattacks in all their manifestations poses a clear threat to international security, stability, and the economy, given the following:

a) Cyberattacks escalate trade and economic wars, especially since they penetrate the information systems of countries and obtain some secrets and sensitive financial information[13].
b) It threatens global economic stability, mainly if it targets international financial institutions, such as global central banks. As a result of the interdependence between banks and financial institutions, the exposure of any of them to a cyberattack can affect entire banking and commercial networks. This can lead to a state of economic chaos and the collapse of stock exchanges and stock markets. This results in countries' significant loss of income and distrust of the security system. It is especially critical when these attacks cause individuals to either cancel their accounts or recover their funds[14].

[13] Niekerk, B van, and T Ramluckan. "Economic Information Warfare: Feasibility and Legal Considerations for Cyber-Operations Targeting Commodity Value Chains." *Journal of Information Warfare* 18, no. 2 (2019): 31–48. https://www.jstor.org/stable/26894669.
[14] Smolanoff, J. (2023, January 16). *Cyber in 2023: Geopolitical and economic risks*. Kroll. https://www.kroll.com/en/insights/publications/cyber/2023-geopolitical-and-economic-risks-davos

c) Many countries adopt cyberattacks as practical tools in modern wars. Electronics are primarily used to launch attacks on enemy computers or even target civilian life and the information infrastructure in these wars. Security and strategic experts point out that countries with advanced technological infrastructure have a better chance of achieving broad electronic dominance if they enter a war. In a conflict of interest with any other country, instead of resorting to traditional military tools, pressing the keyboard can destroy the information infrastructure in the targeted country[15]. The result may have destructive effects beyond those obtained when military force is used.
d) Targeting the digital infrastructure of countries and their sensitive sectors and taking over their military, political, and industrial secrets are some of the most common ways to undermine national security in what is considered a type of explicit espionage, which can then be used to pressure the state and bargain with it to adopt specific positions on many issues and positions[16].

For example, a cyberattack can be launched to close vital sites, paralyze command and control and communication systems, or cut communication networks between central units and commands. This can be done by disabling air defense systems, derailing missiles, controlling air and sea navigation lines, or penetrating the banking system and harming the business and financial markets.

4- The substance of cybersecurity regulations in transportation (Lebanon are a model).

Being a part of developing countries, the major elements to be discussed are:

1. Creation of storage and distribution systems and logistics infrastructure.
2. Developing a system of transport and communication in accordance with international standards and taking into account the need for security.
3. Development of a comprehensive and integrated transportation system that takes into account the safety and protection of the environment, as well as the protection of public health.
4. Emphasizing the importance of promoting transportation through changes that promote universal mobility.
5. Encourage the participation of the private sector in the development of the transport sector.

[15] Buchan, Russell. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict and Security Law* 17, no. 2 (2012): 211–27. http://www.jstor.org/stable/26296227.
[16] Atrews, RA. "Cyberwarfare: Threats, Security, Attacks, and Impact." *Journal of Information Warfare* 19, no. 4 (2020): 17–28. https://www.jstor.org/stable/27033642.

6. Encouraging investment in the construction of roads and railways according to the BOT system and providing guarantees that encourage investors.
7. Establish a sustainable transport system that considers the protection of the environment from pollution and other adverse effects. Secure the national defense and disaster management requirements within a comprehensive national transportation plan.
8. Establishing highly qualified regulatory bodies to develop a comprehensive national transport plan and link it to the Arab and international transport systems.
9. Establishment and modernization of the traffic control system and developing the traffic control infrastructure with the latest technologies.
10. Establishment of a cybersecurity system to protect the transportation system from cyberattacks, as well as establishing a security management system for the transportation system.
11. Establishment of a digital and wireless system to provide services in the field of traffic and transportation, as well as any related services.
12. Establishment of a well-developed railway network for shared transport (people and goods) linking the various major cities and the capital
13. Establishment of an electronic system for the management of transportation and communication systems, as well as the application of security and safety measures.
14. Execution of some plans for bridge and tunnel construction in the capital and congested areas.
15. Freeing sidewalks and pedestrian crossings from obstacles and controlling the parking of violating vehicles.
16. Implement the plans held by the Ministry of Public Works and Transport by securing the funds required for this purpose.
17. Improving transportation efficiency, reducing monopolies, avoiding resource waste, promoting competition and reducing trust
18. Increasing public awareness about traffic safety and the importance of abiding by the laws.
19. Installation of speed control cameras and the implementation of a speed reduction system at the entrances and exits of cities and towns.
20. Organizing public transport, passenger safety and the provision of the necessary means of transport
21. Promotion of public transport, particularly in the capital and other major cities, by providing incentives for public transport users and raising the standards of public transport
22. Provide technical and scientific support to the Ministry of Transport and other bodies in the field of transport.
23. Provide the required financial and technical support to the Ministry of Transport in order to carry out the necessary studies and research in the field of transport.

24. Providing the required number of traffic detachments as well as training and equipping them with the necessary skills for law enforcement
25. Removing encroachments on public property, particularly those adjacent to highways and main roads, and completing the necessary plans
26. Strict enforcement of the provisions of the Traffic Act and activation of the work of the municipal police.

Concluding remarks

The transportation sector manages recovery efforts while contending with a lack of trained workers and elevated market demands and expectations. The Info-Tech Studies Group's Transportation Technology Trends 2022 Report examines research on innovative technology and cybersecurity trends in the transportation industry.

The aim is to discuss how technological advancements affect transportation businesses' operations and efficiencies.

In the future, information technology (IT) executives and leaders in the transportation sector should pay close attention to the following reduction objectives:

a) Applying analytics to aid decision-making: IT leaders can use analytics to create a data strategy that aligns with growth and business objectives. Without adequate data governance and architecture, trained data analytics personnel, or both, organizations run the risk of having low-quality data, which can prevent them from taking advantage of potential opportunities to increase revenue.
b) Heightening priority on cybersecurity: Cyberattacks on critical infrastructure pose a severe threat to the entire world, with the transportation sector one of the most lucrative targets for ransomware attacks.
c) Implementing intelligent automation: The challenge of a driver shortage in the transportation industry can be solved by automation. However, automation is a double-edged sword, and as the number of edge devices grows, so does the possibility of a more extensive cyberattack.

The transportation sector's rapid digitalization and deployment of new or more endpoint devices have created new points of entry for hackers. Organizations may reduce cyber threats, maintain compliance with industry and governmental standards, and lessen the financial effect of a breach by implementing the most effective security best practices and technological solutions.

IT leaders must have adequate risk management programs, security maturity evaluations, and a plan for organizing ransomware assaults as part of their preparations. The transportation

sector's rapid digitalization, with the introduction of additional or more terminal devices, has created new entry points for cyberattacks.

The international community may reduce cyber threats, maintain compliance with industry and governmental standards, and minimize the economic effect of a breach by implementing the most updated security best practices and technological solutions. IT leaders must have solid risk management programs, security maturity assessments, and roadmap planning beforehand.

These measures will enhance the security posture of their nations in transporting passengers and goods.

In conclusion, the transportation sector must prioritize implementing intelligent automation, applying analytics to aid decision-making, and increasing priority on cybersecurity to remain competitive and manage recovery efforts in the future. With the increased risk of cyberattacks, IT leaders should ensure that their organizations have adequate risk management programs. This translates into security maturity evaluations, and having a plan for responding to ransomware attacks in place. This will enable the transportation sector to manage recovery efforts, reduce cyber threats, maintain compliance with industry and governmental standards, and reduce the financial impact of a breach.

Bibliography

- Ball, Desmond. “China’s Cyber Warfare Capabilities.” *Security Challenges* 7, no. 2 (2011): 81–103. http://www.jstor.org/stable/26461991.
- Christopher Bronk & Eneken Tikk-Ringas (2013) *The Cyber Attack on Saudi Aramco,* Survival, 55:2, 81-96, DOI: 10.1080/00396338.2013.784468
- Niekerk, B van, and T Ramluckan. “Economic Information Warfare: Feasibility and Legal Considerations for Cyber-Operations Targeting Commodity Value Chains.” *Journal of Information Warfare* 18, no. 2 (2019): 31–48. https://www.jstor.org/stable/26894669.
- Atrews, RA. “Cyberwarfare: Threats, Security, Attacks, and Impact.” *Journal of Information Warfare* 19, no. 4 (2020): 17–28. https://www.jstor.org/stable/27033642.
- Buchan, Russell. “Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?” *Journal of Conflict and Security Law* 17, no. 2 (2012): 211–27. http://www.jstor.org/stable/26296227.
- Editorial, R. (2012, December 9). *Saudi Arabia says cyber-attack aimed to disrupt oil, gas flow*. Reuters. https://www.reuters.com/article/saudi-attack-idUSL5E8N91UE20121209
- Jeff Jones. (2020, May). *Confronting China’s efforts to steal defense information*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information
- Steve Morgan. (2020, November 13). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
- Ronen Bergman, Rick Gladstone, Farnaz Fassihi. (2021, April 11). *Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage*. The New York Times. https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html
- David E. Sanger, Clifford Krauss, Nicole Perlroth. (2021, May 8). *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*. The New York Times. https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
- Ellen Nakashima, Yeganeh Torbati and Will Englund. (2021, May 8). *Ransomware attack leads to shutdown of major U.S. pipeline system*. The Washington Post. https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/
- Joe Tidy. (2022, February 1). *Cyber-attack strikes German fuel supplies*. BBC News. https://www.bbc.com/news/technology-60215252
- Prajeet Nair. (2022, February 5). *Cyberattack cripples European oil Port terminals*. Bank information security news, training, education - BankInfoSecurity. https://www.bankinfosecurity.com/cyberattack-cripples-european-oil-port-terminals-a-18465

- Matias Madou. (2022, November 7). *Cybersecurity: A global priority and career opportunity*. University of North Georgia. https://ung.edu/continuing-education/news-and-media/cybersecurity.php
- Xinhua. (2022, December 29). *Facts about Russia-Ukraine conflict: Russian deputy FM says west uses Ukraine to launch cyberwar*. People's Daily. https://en.people.cn/n3/2022/1229/c90000-10189727.html
- Smolanoff, J. (2023, January 16). *Cyber in 2023: Geopolitical and economic risks*. Kroll. https://www.kroll.com/en/insights/publications/cyber/2023-geopolitical-and-economic-risks-davos