*Teka of Political Science and International Relations – UMCS, 2023, 18/1*
DOI: 10.17951/teka.2023.18.1.25-35

# LITHUANIAN CYBERSECURITY STRATEGY DEVELOPMENT MODEL FOR 2022-2024

MARTINAS MALUŻINAS
Politechnika Koszalińska. Wydział Humanistyczny
http://orcid.org/0000-0002-2772-9534
email: martinasmaluzinas@gmail.com

**Abstract.** The annexation of Crimea in 2014 and Russia's aggression against Ukraine in 2022 have drastically changed Lithuania's perception of its security environment, especially since Lithuania actively supports Ukraine, making it a primary target of Russian cyberattacks. Cyberspace has become a new security domain for Lithuania, necessitating numerous changes both in operational practices and in the legal and organizational aspects of the state's security systems. The aim of this article is to present Lithuania's cybersecurity strategy model and to outline the role of Lithuanian state institutions in countering cyberattacks on critical infrastructure by external entities. The analysis results indicate that Lithuania will continue to develop new strategies and methods to combat cyber threats in order to protect both national critical infrastructure and private-sector assets.
**Keywords:** cyberattacks, institutions, strategy, Lithuania.

**Tytuł:** Model opracowania Litewskiej Strategii Cyberbezpieczeństwa na lata 2022–2024
**Streszczenie.** Aneksja Krymu w 2014 roku oraz agresja Rosji przeciwko Ukrainie w 2022 roku w istotny sposób zmieniły postrzeganie środowiska bezpieczeństwa przez Litwę, zwłaszcza że państwo to aktywnie wspiera Ukrainę, co czyni je jednym z głównych celów rosyjskich cyberataków. Cyberprzestrzeń stała się dla Litwy nową domeną bezpieczeństwa, co wymusiło liczne zmiany zarówno w praktykach operacyjnych, jak i w prawnych oraz organizacyjnych aspektach funkcjonowania państwowego systemu bezpieczeństwa. Celem niniejszego artykułu jest przedstawienie modelu strategii cyberbezpieczeństwa Litwy oraz określenie roli litewskich instytucji państwowych w przeciwdziałaniu cyberatakom na infrastrukturę krytyczną ze strony podmiotów zewnętrznych. Wyniki analizy wskazują, że Litwa będzie kontynuować rozwój nowych strategii i metod zwalczania zagrożeń cybernetycznych w celu ochrony zarówno narodowej infrastruktury krytycznej, jak i zasobów sektora prywatnego.
**Słowa kluczowe:** cyberataki, instytucje, strategia, Litwa.

## INTRODUCTION

Cybersecurity is now a crucial factor not only in economic and social life but also in political affairs. This is due to the fact that cybersecurity poses increasingly new threats affecting the continuity and quality of life for citizens and state institutions, placing government entities before new challenges in this sphere. Cybersecurity should be understood as the resilience of information systems against actions that compromise the confidentiality, integrity, availability, and authenticity of processed personal data or services provided by the system[1]. Efforts to build and develop a national cybersecurity system are embedded in the core functioning of state institutions. Despite the fact that new technologies offer vast opportunities for skill development, relationship-building, and access to an almost unlimited knowledge base, the primary role of state institutions in the field of cybersecurity remains ensuring an adequate level of security within cyberspace and for its users[2].

Raising awareness in this sphere goes hand in hand with a rapid increase in the number of cyber incidents and emerging threats. Lithuania is also a target of cyberattacks. Reports from Lithuanian security agencies indicate that in recent years, Russia has intensified hostile cyber operations against NATO countries and Lithuania[3]. For this reason, like other nations, Lithuania faces new challenges in developing legal, institutional, and organizational changes to ensure an adequate level of cybersecurity and the protection of its citizens operating within cyberspace.

The aim of this article is to present Lithuania's cybersecurity strategy model and to outline the role of Lithuanian state institutions in countering cyberattacks on critical infrastructure by external entities. The research methods applied in this study include content analysis and case studies. To achieve the research objectives, the following research questions were formulated:

How does Lithuania's cybersecurity strategy look like?

Which institutions are involved, and what is their role in countering cyberattacks?

Do cyberattacks on Lithuania's cybersecurity entail?

The rationale for conducting this analysis is the growing phenomenon of cyber threats from Russian intelligence services, which constitute one of the elements

---

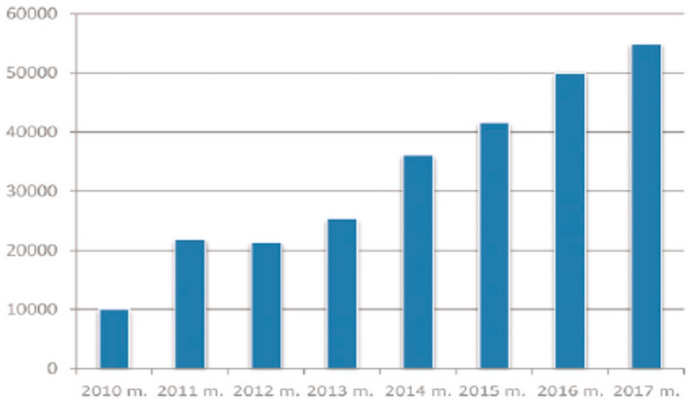
1 P.Pelc, C*yberbezpieczeństwo instytucji finansowych w wymiarze krajowym i międzynarodowym*, w: *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe.* red. M. Karpiuk, Akademia Sztuki Wojennej, Warszawa 2024, s. 38.

2 M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 22(2), 2012, s. 125.

3 A.M. Dyner, Rosyjskie cyberzagrożenia dla państw NATO, Państwowy Instytut Spraw Międzynarodowych, 172. https://www.pism.pl/publikacje/rosyjskie-cyberzagrozenia-dla-panstw-nato. [dostęp:21.11.2023].

of hybrid warfare against Lithuania and NATO countries. Russia's objective in waging hybrid warfare in Lithuania is to polarize society, escalate internal political tensions, create chaos, and strengthen the position of pro-Kremlin actors within Lithuania's political landscape. According to security reports, the activities of Russian intelligence services are evident in nearly every aspect of Russian engagement with Lithuania[4]. Moreover, significant cyber incidents have shown an upward trend since 2010 (see Figure 1).

Fig. 1. Dynamics of growth of cyber incidents in Lithuania in 2010-2017




Source: suvalkietis.lt (2018).

Moreover, Lithuanian military services have observed that most cyberattack incidents have targeted the energy sector, public security and law enforcement, foreign affairs, and security policy. The geographical spread of malicious software is closely linked to the strategic importance of state institutions, the military, and economic entities.

[4] B.Fraszka, *Państwa bałtyckie a rosyjskie zagrożenie,* Warsaw Institute, https://warsawinstitute.org/wp-content/uploads/2020/10/Pa%C5%84stwa-ba%C5%82tyckie-a-rosyjskie-zagro%C5%BCenia-hybrydowe-Bartosz-Fraszka.pdf, s. 14-15, [dostęp:30.10.2020].

## CYBERATTACKS ON STATE AND PRIVATE INSTITUTIONS IN LITHUANIA (2019–2024)

After February 24, 2022, when Russia invaded Ukraine, no significant changes were observed in Lithuania's cyber environment. According to the 2022 report from the National Cyber Security Center (NKSC), the number of registered cyber incidents (approximately 4,000) remained at a similar level to that of 2021. However, in 2023, the NKSC recorded a significant surge in cyberattacks targeting Lithuania's civilian infrastructure.

For instance, at the end of June 2022, the NKSC reported a massive wave of DDoS attacks directed at both the public and private sectors. Additionally, publicly available sources indicate that in 2023, attempts were made to interfere with at least 137 publicly accessible websites. Responsibility for these attacks was claimed by a hacker group supporting the policies of the Russian Federation[5].

In July 2022, the company Ignitis Grupė reported the largest cyberattack in the past decade. The website of ESO (Energijos Skirstymo Operatorius) was blocked, and responsibility for the cyberattack was claimed by a group linked to Russian intelligence services, known as Kill-net[6].

In 2023, the number of cyberattacks in Lithuania increased ahead of the NATO summit in Vilnius. According to data from the NKSC, the number of cyberattacks during the NATO summit tripled. After a breach in the information systems of one of the regional radio stations in Lithuania and the "Panorama" shopping center, messages were launched targeting NATO and the supply of weapons to Ukraine. Significant DDoS attacks also took place before and during the NATO summit. Among the companies affected by these attacks were City Service, Akropolio, Orlen Lietuva, Linas Agro, Govilnius. lt, as well as news agencies BNS, 15min, alfa.lt, and the service m.Ticket.

Although these events were not publicly announced, cybersecurity experts mentioned in interviews that during the NATO summit, there were "very serious attempts" to disrupt air navigation systems and attacks on critical infrastructure facilities. However, these cyberattacks were thwarted and did not affect the organization of the NATO summit meeting[7] .

---

[5] Nacionalinė kibernetinio saugumo būklės ataskaita už 2022 m. (2023). Nacionalinėje kibernetinio saugumo ataskaitoje, https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf. [dostep: 04.04.2023].

[6] T. Janeliūnas, Rusijos įtakos Lietuvai indeksas 2022-2023 m., Rytų Europos studijų centras, https://www.eesc.lt/wp-content/uploads/2024/01/Janeliunas_Rusijos-itakos-LT-indeksas_FINAL.pdf.

[7] Ibidem.

Table 1. Number of identified cyberattacks on state and private institutions in Lithuania in 2019-2023.

| Lata | Liczba zidentyfikowanych cyberataków | Niskiego wpływu | Średniego wpływu | Dużego wpływu |
|---|---|---|---|---|
| 2019 | 3241 | Nieustalono | Nieustalono | Nieustalono |
| 2020 | 4330 | 4262 | 67 | 1 |
| 2021 | 4088 | 3955 | 93 | 0 |
| 2022 | 4080 | 4047 | 33 | 0 |
| 2023 | 2 378 | 2200 | 33 | 0 |

Source: own study based on (Nacionalinė kibernetinio saugumo būklės ataskaita už 2022 m. and r 2023 m., 2023).

Analyzing the data above, it should be noted that in 2022, the NKSC registered a total of 4,080 cyber incidents, which is similar to the number from 2021. However, in 2023, the NKSC recorded 2,378 cyber incidents. Compared to 2022, the total number of registered incidents decreased by 30%, but the number of dangerous incidents with a moderate threat level increased by 12%[8].

This data indicates a growing trend in the number of cyberattacks on state and private institutions in Lithuania from 2019 to 2022. All of these incidents confirm that entities linked to state governments, such as Russia, China, and Belarus, regularly monitor and exploit vulnerabilities in Lithuania's cyberspace, attempting to disrupt IT and communication services. A significant portion of cyberattacks in Lithuania could be considered as tests or assessments of vulnerability levels. The sectors most affected by these incidents include hosting infrastructure, public administration, internet service providers, and end-user devices connected to these services.

In 2023, although the number of cyberattacks decreased, Lithuania's National Communication and Information System (referred to as "RIS") identified 1,963 communication and information systems (hereinafter "RIS") with potentially critical security vulnerabilities. The responsible RIS services discovered 74 cybersecurity vulnerabilities in various Lithuanian information systems and reported them to the NCSC in accordance with the responsible cybersecurity vulnerability disclosure process. The highest number of incidents was recorded in

[8] M. Gaučaitė-Znutienė, Ataki cybernetyczne przed szczytem NATO w Wilnie. Spoty propagandowe w centrum handlowym i radiu, https://www.lrt.lt/pl/wiadomosci/1261/2031038/ataki-cybernetyczne-przed-szczytem-nato-w-wilnie-spoty-propagandowe-w-centrum-handlowym- [dostęp: 10.07.2023].

the areas of state and municipal administration (564), security and defense (312), and business (159)[9].

## INSTITUTIONS, STRATEGY, AND METHODS FOR COMBATING CYBERATTACKS

Although Lithuania recorded a decrease in the number of registered cybercrime incidents in 2023 compared to 2022, the global situation demonstrates that cybercrime is rapidly becoming a lucrative "business", and geopolitical tensions are increasing in various parts of the world, including Lithuania. According to the 2023 Digital Quality of Life Index (DQL) survey, Lithuania ranks 10th in terms of cybersecurity[10]. Furthermore, with elections held in many countries worldwide in 2024, including Lithuania, these events are expected to be marked by even greater informational pressure than in 2023. However, experts note that Lithuania has achieved positive results in terms of resilience to cyberattacks. The Ministry of National Defense of the Republic of Lithuania plays a key role in this area.

To strengthen the country's capabilities in cybersecurity, the state's information resources, and the protection of critical infrastructure, the Ministry of National Defense of the Republic of Lithuania approved a development program in 2023. According to the program's assumptions, a sum of 40.15 million euros was allocated from the Recovery and Resilience Fund. Based on this Development Program, the Ministry of National Defense will carry out tasks outlined in the National Development Plan for 2021–2030, including strengthening cybersecurity and defense. Analyzing the development program, it is clear that the main strategic goal is to address and eliminate the problems emerging in Lithuania's cybersecurity landscape. Among the strategic objectives outlined in the program, Lithuanian authorities plan to:

- Review the system for formulating and implementing national cybersecurity policy, involving an increasing number of institutions in managing and ensuring cybersecurity.
- Update organizational and technical requirements for cybersecurity; modernize the infrastructure for detecting cybercrime and detecting cybercrimes.

[9] Nacionalinė kibernetinio saugumo būklės ataskaita už 2022 m. ir 2023 m., 2023, Nacionalinėje kibernetinio saugumo ataskaitoje, https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf.

[10] DIGITAL QUALITY OF LIFE INDEX. (2023). 2023 *Digital Quality of Life Index*. https://competitiveness.arta.gov.ph/reports/digital/digital-quality-of-life-index

- Strengthening the competences of cybersecurity workers and cybercrime investigators.
- Increasing public awareness of cybersecurity, especially among the most vulnerable groups in society: providing basic knowledge of cybersecurity, helping to acquire practical cyber hygiene skills such as installing security updates on used devices, creating and using passwords and making backup copies – all this will help prevent some cyber incidents and/or reduce their impact;
- Promoting cooperation between the public and private sectors. Assistance to small and medium-sized enterprises and active cooperation between the public and private sectors in the field of cybersecurity would not only help ensure greater cyber resilience, but would also encourage finding and offering innovative cybersecurity solutions on a national scale (KAM krasto apsaugos ministerija, 2023).

Another Lithuanian institution playing a crucial role in shaping resilience to cyberattacks is the National Cyber Security Centre (NKSC). In 2023, to enhance the tools designed to protect Lithuanian organizations and citizens, the NKSC expanded the DNS14 firewall, which was initially launched in 2018. This protection system covered nearly 4 million mobile phones and 775,000 fixed internet subscribers, safeguarding an average of over 2,000 citizens per day, who, unaware of the messages sent by cybercriminals, attempted to access websites aimed at stealing money or confidential data.

Moreover, by 2023, the NKSC had also begun developing a tool for managing blocked domains, which allows seven key Lithuanian institutions—such as the police, gambling oversight authority, Bank of Lithuania, Lithuanian Radio and Television Commission, the Journalism Ethics Inspectorate, the State Consumer Rights Protection Service, and the Department for the Control of Narcotics, Tobacco, and Alcohol—to issue orders to internet service providers (ISPs) to block malicious online resources. This collaborative effort aims to strengthen the country's defenses against cybercrime and protect citizens and organizations from falling victim to online fraud and data theft[11].

Among the key priorities of the analyzed institution, the National Cyber Security Centre (NKSC), is also the development of competencies in cyber security, which is one of the most important actions to increase the country's resilience to constantly evolving cyber threats. Since 2023, the NKSC has paid particular

[11] NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS, (2023).Blokuojamų domenų valdymo sistema „VASARIS", https://www.nksc.lt/vasaris.html.

attention to training and workshops, aiming to strengthen the capacity of entities responsible for cyber security to effectively manage risks, detect cyber incidents, and respond appropriately. In 2023, over 11,500 individuals from public administration institutions, non-governmental organizations, and small and medium-sized enterprises completed various theoretical training sessions organized by the NKSC. In 2024, more than 46,000 individuals from these institutions completed NKSC cyber security training[12].

Another institution playing a crucial role in shaping resilience to cyberattacks is the Lithuanian military forces, which regularly organize "Amber Mist 2024" cyber security exercises. The goal of these exercises is to enhance the cyber capabilities of the Lithuanian Armed Forces in the area of cyber defense, as well as to improve international and inter-institutional cooperation[13]. Other institutions responsible for building resilience against cyberattacks in Lithuania include:

- The Regional Cyber Defense Center (RKGC) plays a vital role in strengthening Lithuania's cybersecurity strategy. Its goals include enhancing cooperation with strategic partners, analyzing cybersecurity threats, organizing training for cybersecurity experts, and conducting research in the field of cybersecurity. This institution contributes significantly to the overall effort of bolstering Lithuania's cyber defenses[14].
- The National Coordination Centre (NCC), whose tasks in Lithuania are to strive for concentration and more effective coordination of investments in scientific research, technological and industrial development[15].

When analyzing all Lithuanian institutions whose role is to build comprehensive resistance to cyberattacks, it should be noted that the main methods of combating cyber threats include: training, preventive measures, and international cooperation.

[12] A. Paulauskaitė, Šiais metais NKSC mokymus apie kibernetinį saugumą užbaigė daugiau nei 46 tūkst. gyventojų. https://www.etaplius.lt/naujiena/siais-metais-nksc-mokymus-apie-kibernetini-sauguma-uzbaige-daugiau-nei-46-tukst-gyventoju-336487 [dostep:30.12.2024].

[13] Prasideda Lietuvos kariuomenės pratybos „Gintarinė migla 2024", kuriose bus treniruojamasi kovoti su kibernetinėmis atakomis, https://www.kariuomene.lt/prasideda-lietuvos-kariuomenes-pratybos-gintarine-migla-2024-kuriose-bus-treniruojamasi-kovoti-su-kibernetinemis-atakomis/26226. [dostęp:13.11.2024].

[14] Apie RKGC, https://www.nksc.lt/rkgc/

[15] Nacionalinis koordinavimo centras, https://www.nksc.lt/nkc/.

## SUMMARY

Despite some improvement in cybersecurity in Lithuania in 2023 compared to 2022, the situation remains challenging. The number of registered cyber incidents decreased by 26%, and the National Cybersecurity Center recorded nearly one-third fewer incidents than in the previous year. However, there are concerning signals, such as a 12% increase in incidents with a medium level of threat, and data breaches affecting 49% of both public and private entities. This indicates that cyberattacks are becoming subtler and effective, and the phenomenon of cyber threats, particularly in the context of the hybrid warfare conducted by Russian intelligence services, is more visible during this critical period.

The conducted research has shown that attacks on cybersecurity systems in Lithuania focus mainly on breaching critical infrastructure systems, spreading false messages, disrupting air navigation systems, as well as launching attacks on critical infrastructure and disrupting the delivery of IT and communication services. A recurring issue is also DDoS attacks, which target computer systems and network services of both public and private institutions.

In the face of these threats, Lithuania is taking numerous actions to strengthen its resilience against cyberattacks. These measures include modernizing protection infrastructure and intensifying cooperation between the public and private sectors. However, further actions, such as developing cybersecurity skills, modernizing preventive tools, and fostering international collaboration, are essential to effectively respond to the growing threats in cyberspace.

The effective Lithuanian strategy in countering cyberattacks stems from both the integration of cybersecurity issues with military structures and political engagement, as well as the involvement of public institutions. The main methods for combating cyber threats include raising public awareness of the issue, civic education through training, preventive actions, and international cooperation and experience exchange with other countries and international organizations to improve cybersecurity. The analysis has shown that since 2023, there has been a clear shift in the orientation of Lithuania's cybersecurity strategy, which is becoming increasingly effective in countering cyber threats to both public and private institutions.

## BIBLIOGRAPHY


1. DIGITAL QUALITY OF LIFE INDEX. (2023). 2023 *Digital Quality of Life Index.* https://competitiveness.arta.gov.ph/reports/digital/digital-quality-of-life-index.
2. Dyner, A. M. (2023). Rosyjskie cyberzagrożenia dla państw NATO, Państwowy Instytut Spraw Międzynarodowych, 172. https://www.pism.pl/publikacje/rosyjskie-cyberzagrozenia-dla-panstw-nato.
3. Fraszka, B. (2020). *Państwa bałtyckie a rosyjskie zagrożenie,* Warsaw Institute, https://warsawinstitute.org/wp-content/uploads/2020/10/Pa%C5%84stwa-ba%C5%82tyckie-a-rosyjskie-zagro%C5%BCenia-hybrydowe-Bartosz-Fraszka.pdf.
4. Gaučaitė-Znutienė M., Ataki cybernetyczne przed szczytem NATO w Wilnie. Spoty propagandowe w centrum handlowym i radiu, https://www.lrt.lt/pl/wiadomosci/1261/2031038/ataki-cybernetyczne-przed-szczytem-nato-w-wilnie-spoty-propagandowe-w-centrum-handlowym- [dostęp: 10.07.2023].
5. Grzelak, M. Liedel, K. (2012). *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, ,,BEZPIECZEŃSTWO NARODOWE" 22(2), 2012, 125-139.
6. Janeliūnas, T. (2024). Rusijos įtakos Lietuvai indeksas 2022-2023 m., Rytų Europos studijų centras, https://www.eesc.lt/wp-content/uploads/2024/01/Janeliunas_Rusijos-itakos-LT-indeksas_FINAL.pdf.
7. KAM krasto apsaugos ministerija, (2023). Dėl 2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos patvirtinimo, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/54521320591e11ee8e3cc6ee348ebf6d?jfwid=-1a256e44a1.
8. Lietuvos kariuomenės.lt (2024). Prasideda Lietuvos kariuomenės pratybos „Gintarinė migla 2024", kuriose bus treniruojamasi kovoti su kibernetinėmis atakomis, https://www.kariuomene.lt/prasideda-lietuvos-kariuomenes-pratybos-gintarine-migla-2024- kuriose--bus-treniruojamasi-kovoti-su-kibernetinemis-atakomis/26226.
9. Nacionalinė kibernetinio saugumo būklės ataskaita už 2022 m. (2023). Nacionalinėje kibernetinio saugumo ataskaitoje, https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf.
10. Nacionalinė kibernetinio saugumo būklės ataskaita už 2023 m. (2024). Nacionalinėje kibernetinio saugumo ataskaitoje, https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2023.pdf.
11. NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS, (2023).Blokuojamų domenų valdymo sistema „VASARIS", https://www.nksc.lt/vasaris.html.
12. nkcs.lt. (2024a). Apie RKGC, https://www.nksc.lt/rkgc/.
13. nkcs.lt. (2024b). Nacionalinis koordinavimo centras, https://www.nksc.lt/nkc/.

14. Paulauskaitė A. (2024). Šiais metais NKSC mokymus apie kibernetinį saugumą užbaigė daugiau nei 46 tūkst. gyventojų. https://www.etaplius.lt/naujiena/siais-metais-nksc-mokymus-apie-kibernetini-sauguma-uzbaige-daugiau-nei-46-tukst-gyventoju-336487.
15. Pelc, P. (2024). C*yberbezpieczeństwo instytucji finansowych w wymiarze krajowym i międzynarodowym*, w: *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe.* red. M. Karpiuk, Akademia Sztuki Wojennej, Warszawa.
16. suvalkietis.lt. (2018). *Kibernetinės atakos – mūsų kasdienybė,* https://www.suvalkietis.lt/2018/07/10/kibernetines-atakos-musu-kasdienybe/ ?fbclid=IwY2xjawIulNhleHRuA2FlbQIxMAABHadadJsxzb4PSXVax54neLYHe9xQwxJEeLgdYiMYYkNbQ8n4ljHWtyME8A_aem_ftTG2GnKmrXf30G96t0TJw.