Cybersecurity in Ukraine

Market Overview

January 2025

This research was conducted by DataDriven, initiated by EBA Cybersecurity Subcommittee and CyberTech Committee of IT Ukraine Association. The study was supported by Aspen Institute Kyiv, which implements the programme “Cybersecurity dialogue” powered by USAID project “Cybersecurity for critical infrastructure in Ukraine”

Key project partners

USAID ВІД АМЕРИКАНСЬКОГО НАРОДУ

THE ASPEN INSTITUTE KYIV

Initiated by

EBA European Business Association

IT Ukraine Association

Thanks for your assistance*

IO GUARDS

ASTERS

CHECKOEYE

CyberLab Комп'ютерна криміналістика

DataArt

EVE.calls

EY

FSG feel secured · globally

ICWR INSTITUTE OF CYBER WARFARE RESEARCH

InDev LAB

INTELLIGENT IT DISTRIBUTION

ISSP

inovo VC

molfar

osavul

seeton

uklon

UNIT.City

UVCA UKRAINIAN VENTURE CAPITAL & PRIVATE EQUITY ASSOCIATION

ZAS VENTURES

*Interviews were conducted with these organisations during the preparation of the study. The list is provided in alphabetical order.
The study represents the position of the authors and does not necessarily reflect the positions of the organisations interviewed or the partners of the study.

Definitions 1/2

Cybersecurity is the process of protecting information systems, networks, applications, and data by ensuring their confidentiality, integrity, and availability. It involves managing identification, detection, protection, response, and recovery measures.

The cybersecurity market in Ukraine includes solutions such as professional services, managed services, and products. These cover functions like identification, detection, protection, and response, as well as related services like solution support, deployment, and training. However, the study does not include business continuity, disaster recovery, physical security, or internal cybersecurity measures.

Professional (consulting) services: are specialised expert services aimed at evaluating and managing processes such as identification, detection, protection, response, and recovery.

Managed services and products: offer support for cybersecurity tasks through specialised platforms that handle monitoring, threat intelligence, incident response, and more. These solutions help organisations scale and automate these functions effectively.

Definitions 2/2

Cyber solutions are products or services tailored to meet the unique requirements of organisations, considering their risk landscape and security strategies. Cyber solutions include:

Application security	Cloud security	Data security	Network security	Endpoint security	Other solutions
Protection methods to ensure the security of computer programs from external threats, exploitation of vulnerabilities and unauthorised access to software.	Protection practices in public, private and hybrid cloud environments aimed to ensure the security of IT systems, data and applications from cyber threats and data leakage risks.	Security measures to ensure the availability, integrity and confidentiality of sensitive data, including access control and encryption to prevent unauthorised access and theft.	Technologies and procedures that protect networks from unauthorised access, hacking, and data sabotage.	Protection of endpoints, such as workstations, servers, and mobile devices, from various attacks, using antivirus protection and modern solutions against zero-day threats.	Additional solutions for identity and access management, risk management that maintain compliance with regulatory requirements and protect against security risks, etc.

Content

1. Market Overview

The importance of cybersecurity grows amid technological progress

Historical context. The most well-known cybercrimes:

1962. First cyberattack

Passwords leakage from MIT computer network

1988. "Morris Worm"

Attack that affected NASA and Stanford University databases

1995. First bank system hacking

Attack on Citibank, with losses of more then $10.7 million

2000. Series of DDoS attacks

Attacks on the services of Amazon, Yahoo, Ebay, CNN & etc.

2010. Stuxnet

Attack on Iranian industrial facilities included in its nuclear program

2017. WannaCry Ransomware

Cyberattack on government agencies in 150 countries, possibly involving DPRK hackers

2020. Breakdown of SolarWinds

Russian hackers gained access to 18000 data sets

2024. Attacks on Royal Mail

Ransomware, possibly involving hackers from the Russia, caused chaos in service operation worldwide

Main facts about cybersecurity in the world

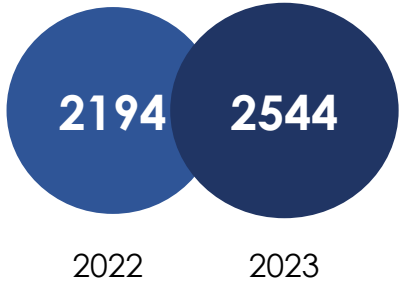
- The most affected sectors: **manufacturing, finance, healthcare and digital services.**
- The most widespread types of cyberattacks: **DDoS, Ransomware, Phishing**
- **The states** that experience the most cyberattacks: the USA, Ukraine, South Korea, China.

- The cybersecurity service market maintains **steady growth.**
- **The USA, China, Germany and the UK** hold the largest share in the cybersecurity market.
- The global cybersecurity market is projected to grow to **$186 billion** in 2024 with an **annual growth rate of 7.92%** by 2029.

Sources: Teal, Knowledge academy, Statista, Fortra, Fortune Business Insights, Oxford University, Microsoft Digital Defence Report.

Russian cyber aggression against Ukraine underline the need to develop a national industry of cybersecurity services and products

Number of registered cyber incidents in Ukraine:

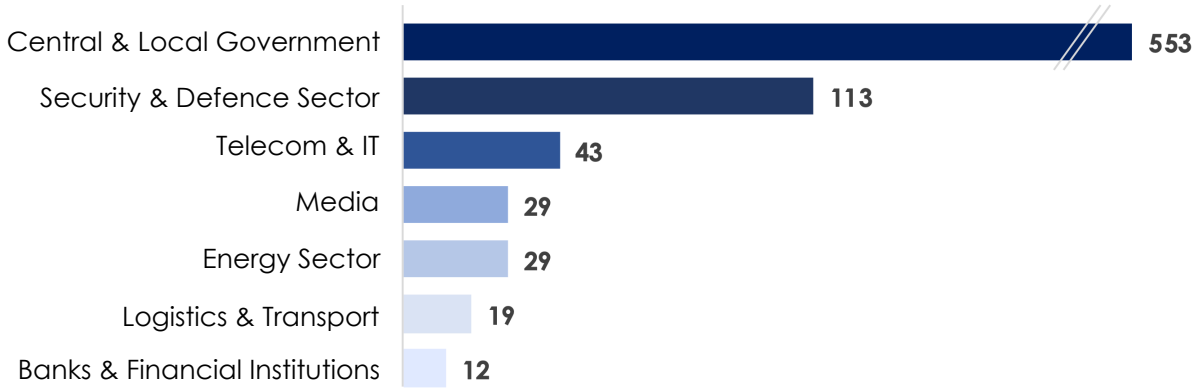


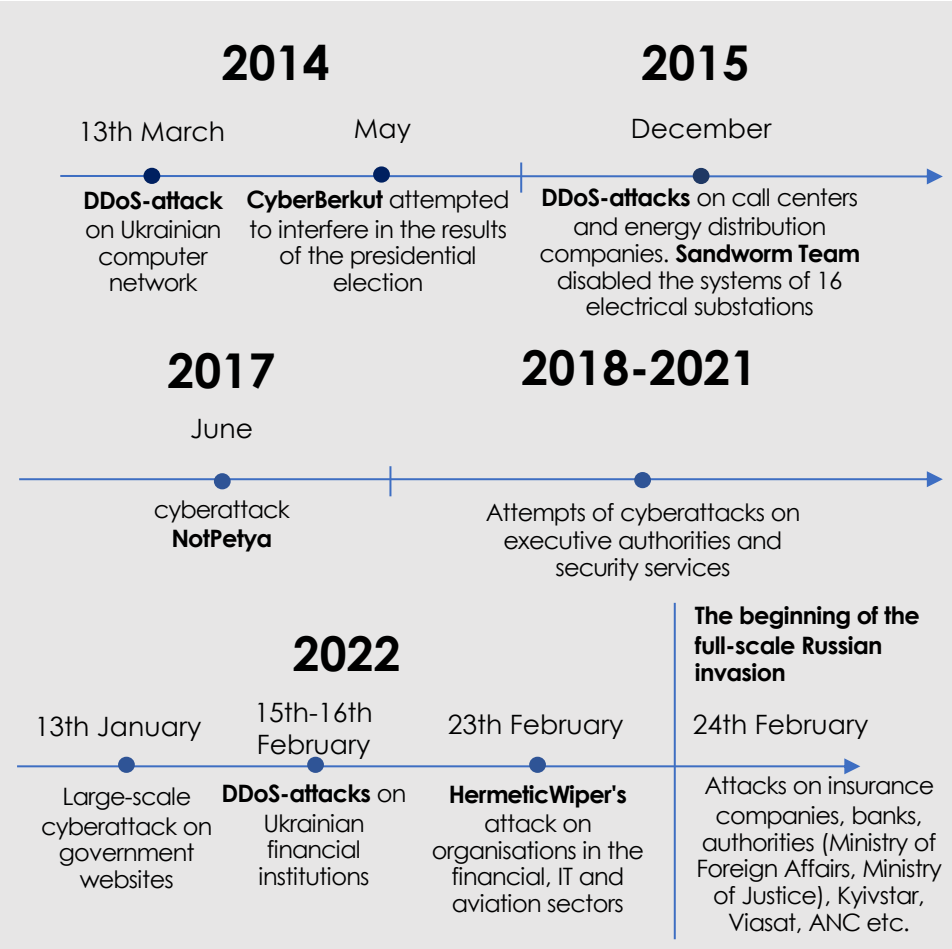
UAC-0010 (Gamaredon/FSS) remains the most active Russian hacker group:

- In the first half of 2022 the group carried out **76** cyberattacks.
- In the first half of 2023 they carried out **94** cyberattacks.

Key sectors attacked

Number of cyber incidents in 2022



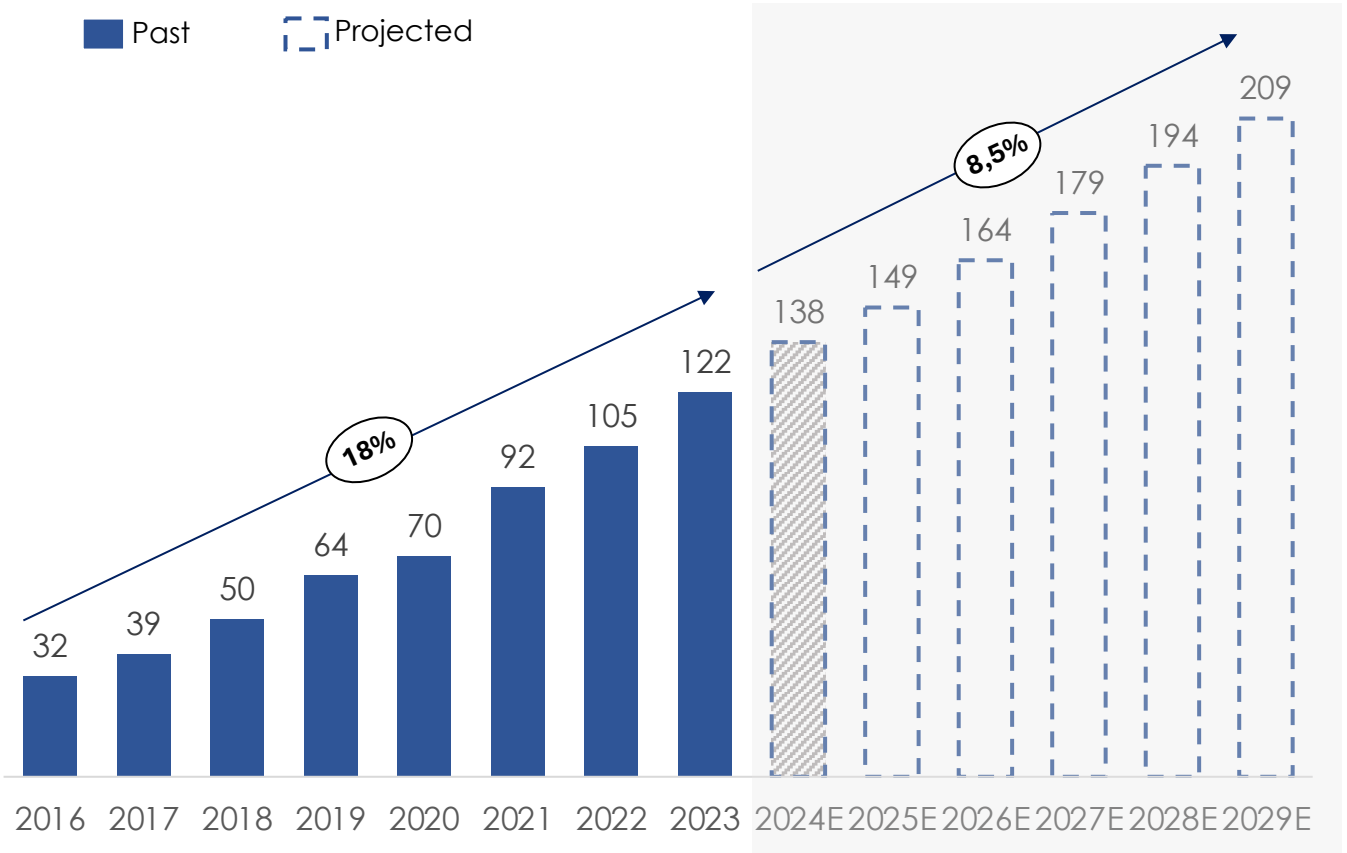


Sources: State Service of Special Communications and Information Protection of Ukraine, DataDriven Analysis.

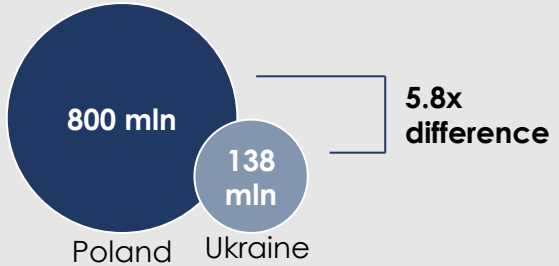
The Ukrainian cybersecurity market has grown 4 times over the past 8 years and is projected to grow by another 50% by 2029

Size of the Ukrainian cybersecurity market* 2016-2029E

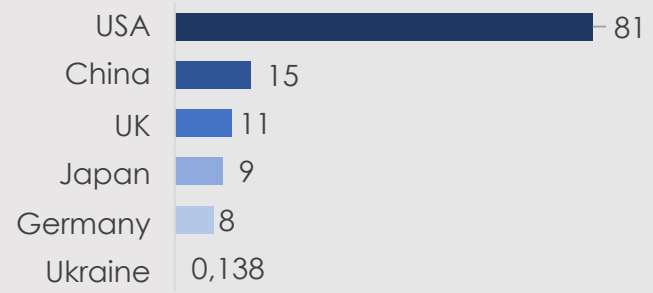
Market size, in million USD at current exchange rates, CAGR in %.



Comparison of the markets of Ukraine vs Poland



Leaders of world cybersecurity market, in billion $



Ukraine's share in the world market

~0,07% which is expected to reach **USD 186 billion in 2024.**

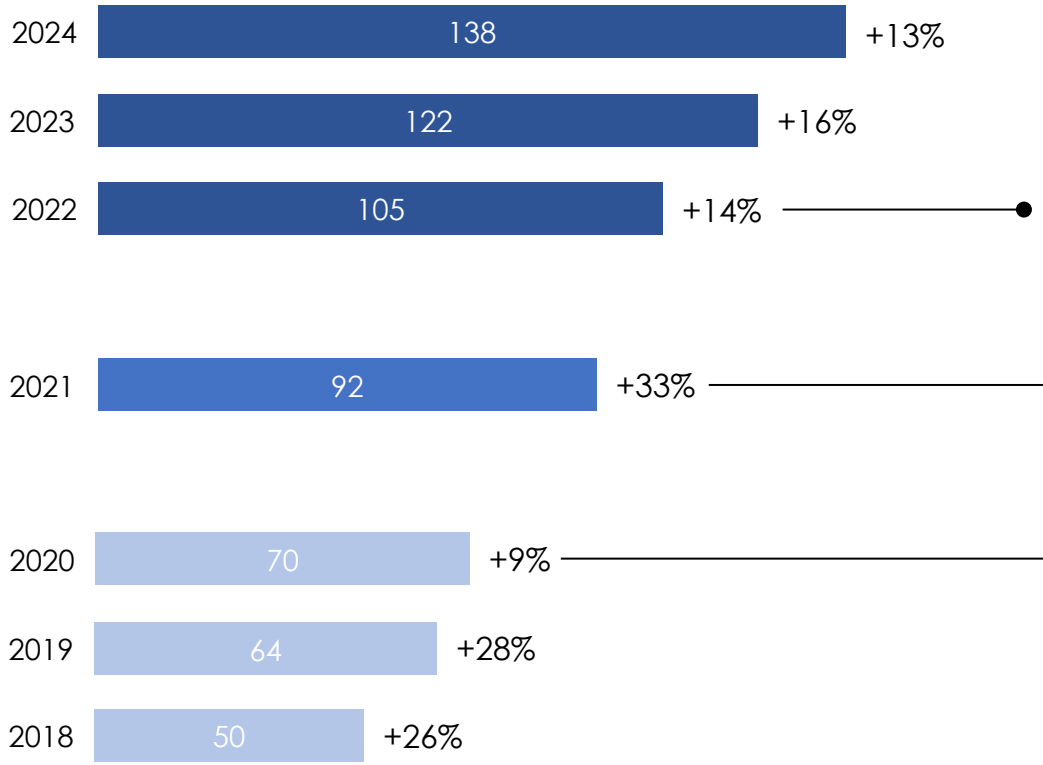
DataDriven | Research & Consulting

*The data sample takes into account companies from B2B, B2C, and B2G segments. Market dynamics are represented through the eyes of consumers of cybersecurity services and products. Data is based on companies' cybersecurity spending // Sources: Statista, DataDriven Analysis.

The growth of cybersecurity market was fluctuating with periods of acceleration and deceleration in 2020, 2021 and 2022.

Annual growth of cybersecurity market in Ukraine*

In million USD at the current exchange rate



- Moderate market growth in 2022 was driven by company relocations and office closures, which led to a decrease in domestic demand for cybersecurity and a slowdown in investment growth.
- The state partially met the growing needs in the field of cybersecurity at the expense of public sector workers and mobilisation.

- The acceleration of market growth in 2021 was influenced by an increase in cybercrime, drawn attention to cybersecurity, and continued business activity due to quarantine restructuring.
- The largest growth was seen in the field of **cloud security (+76%)**, as companies increasingly relied on cloud services for remote work.

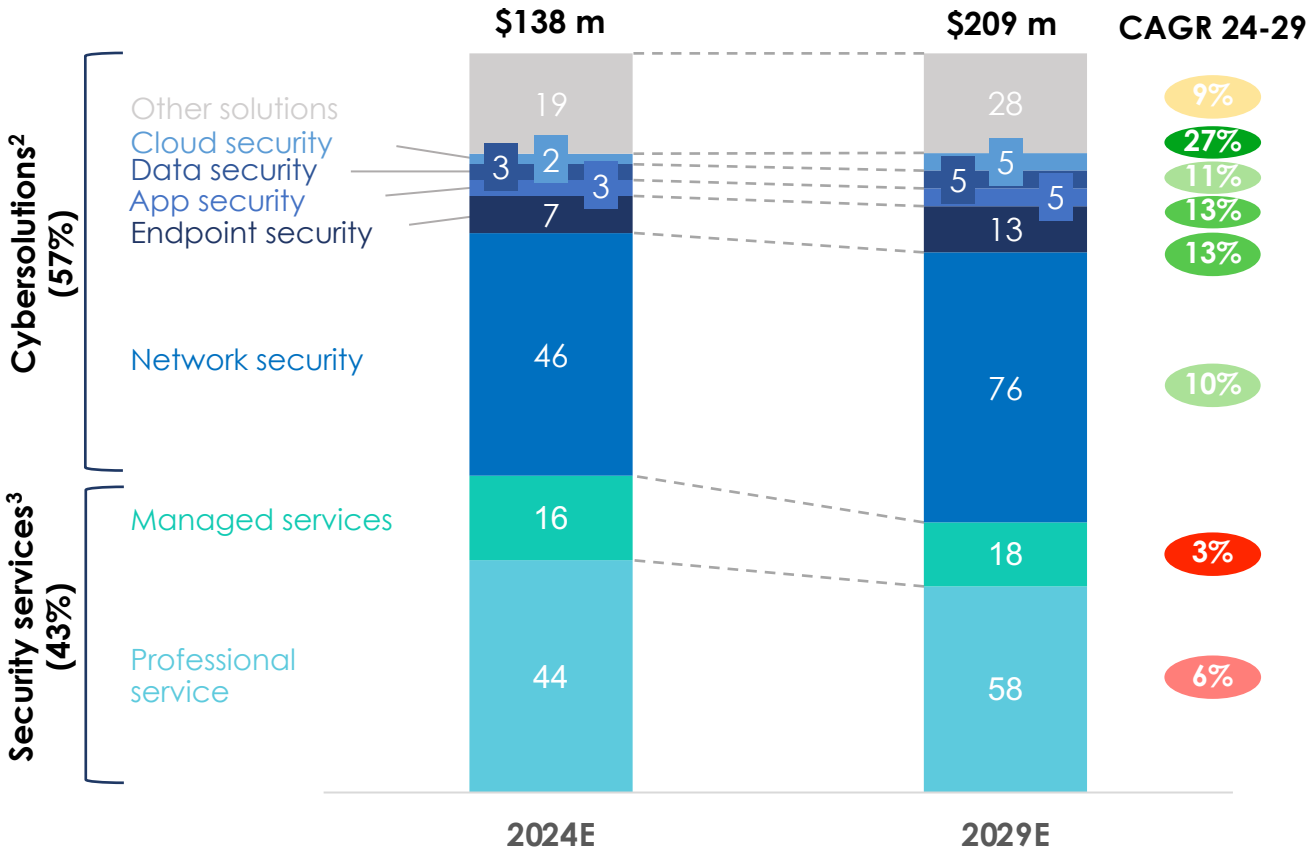
- In 2020, under the impact of COVID-19, businesses faced financial challenges and budget constraints, prioritising core operational processes over cybersecurity investments.
- Resources have been reallocated to support remote work, resulting in reduced spending on advanced cybersecurity solutions.

* The data sample considers companies from B2B, B2C, and B2G segments. Market dynamics are represented through the eyes of consumers of cybersecurity services and products. Data is based on companies' cybersecurity spendings // Sources: Statista, Cyber Safety Unit, Expert interviews, DataDriven Analysis.

The network security segment dominates the market, but cloud, application, and endpoint security are growing promptly

Size and growth of the Ukrainian cybersecurity market by segments

2024E and 2029E , in million USD, CAGR in %.



Main Conclusions

- While the global cybersecurity market is prevailed by the security services segment with a share of **53% in 2024**, the Ukrainian market is dominated by cyber solutions **with a share of 57%**. This is due to the following factors:
  - **Increasing the frequency and scale of cyberattacks:** the war has increased the number and complexity of cyberattacks on Ukraine, which has led to the rapid implementation of automated solutions such as data encryption, automated threat detection.
  - **The need for immediate solutions:** the threat of large-scale cyberattacks has forced companies to prioritise ready-made cyber solutions over the systematic implementation of personalised solutions.
  - **Shortage of personnel:** a limited number of specialists has resulted in the use of automated solutions that requires less human intervention.
- **By 2029 the cyber solutions segment** will outrange the security services segment in the global market and become dominant (**55% vs. 45%,** respectively). Ukraine is a trendsetter, because it is ahead of other countries in cyber expertise because of its work in R&D.

Notes: 1.mainly audit and consulting services; 2. comprehensive services for the overall enhancement of the company's protection; 3. individual products that meet specific cybersecurity needs and risks // Sources: Statista, DataDriven Analysis.

Digitalisation and the growing risk of real losses from cyberattacks are the main driving forces of the market in Ukraine

Comprehensive digitalisation

As businesses and governments adopt digital solutions, they face an increased risk of cyber threats that requires strong cybersecurity measures to protect sensitive data and ensure smooth operations.

Growth in cyber attack activities

The actual being in a state of cyber warfare is the main reason for the rise in the number of cyberattacks. Organisations across all sectors face increased risks to their operations and data security, forcing them to invest in advanced cybersecurity solutions.

Increase in risk of real costs

Cyberattacks such as ransomware, data breaches disrupt business operations, lead to downtime, and often require significant recovery costs. In addition to financial losses, companies may face reduced revenues, reputational damage, and loss of customer trust.

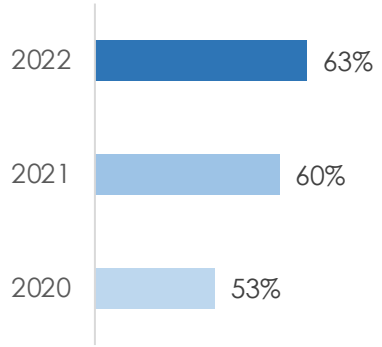
Market stimulation by donors

During a full-scale aggression the development of the industry largely depends on financing from ITA (for example, USAID projects) or direct support from global and national companies. Their support is still essential in terms of limited state involvement.

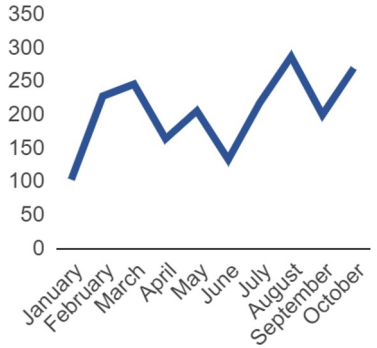
Growth in AI popularity

The growing capabilities of AI products opens up opportunities for cyberattacks of new power and intensity. AI also enables to strengthen security measures, allowing faster threat detection, data analysis, and automation of protection mechanisms.

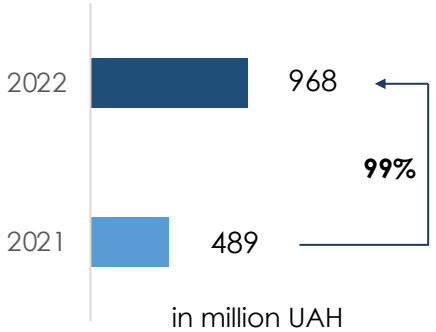
Use of digital public services in Ukraine



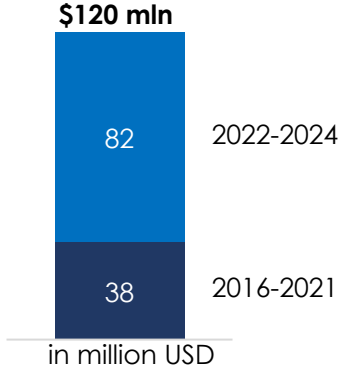
Number of Russian cyber attacks on Ukraine in 2023



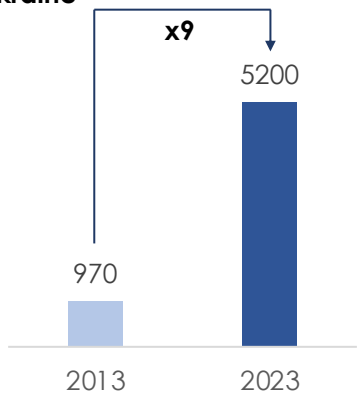
Losses of Ukrainian citizens from cybercrime



U.S. Cybersecurity Assistance to Ukraine for 2016-2024



Number of AI/ML specialists in Ukraine

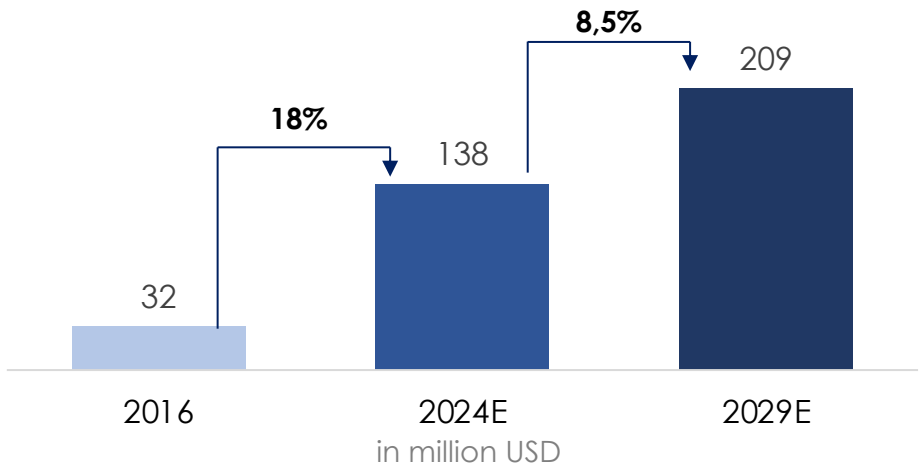


Sources: Statista, UNDP, The AI Ecosystem of Ukraine, €MA Research, Forbes Ukraine, Minister of Digital Transformation, Expert Interviews.

However, market growth is expected to slow down over the next 5 years

Comparison of market growth rates in Ukraine in the past and future

Forecast if ongoing armed conflict continues



The slowdown in growth is expected due to:

- Reduction of donor funding.
- The end of the war which may lead to a decrease in risk expectations in the field of cybersecurity, a weakened economy and the lack of own financial resources to invest in cybersecurity measures.
- Workforce crisis and shortage of young specialists under the military situation and postwar period.

Main trends in Ukrainian cybersecurity

Innovations	• **Artificial intelligence** applied to detect threats and automate response. • **Blockchain:** secures data transmission and prevents DDoS attacks thanks to a decentralised verification system.
Market segments	• **Network security** will continue to lead the market, maintaining a share of 36% until 2029. • **Cloud security** will be the fastest growing segment because of the flexibility and ease of implementation of cloud security services.
Market players' share	• **Ukrainian software developers** will keep going behind international companies in terms of complexity of solutions due to objective reasons. Heavier dependence on international providers will occur.
Consumption patterns	• **Zero trust principle:** a security model that involves thorough verification of devices and users, granting the minimum necessary rights, and monitoring behavior when accessing data or services, implemented as a policy within the digital infrastructure.

Sources: Statista, Wezom, DataDriven Analysis, Expert Interviews.

Positive and negative trends in the cybersecurity market

Market strengths

Unique experience in countering full-scale cyberwar

- Massive cyberattacks on critical infrastructure networks, telecommunications and financial institutions since the beginning of Russian invasion resulted in high threat awareness.
- Ukraine's experience in actual cyberwar provides valuable information that should be shared with foreign partners.

Shifts in the digital ecosystem

- A long-term trend towards digitalisation of public sector functions as well as private sector services and business processes led to a constant generation of demand for cybersecurity products and services.

International technical assistance

- Foreign governments have aroused their interest in supporting the functioning of Ukrainian cybersecurity since the beginning of the full-scale invasion.
- USAID set a goal to grant $38 million aid, and in 2024 provided $500 000 of direct grant assistance to Ukrainian initiatives.
- The European Union in cooperation with E-riigi Akadeemia Sihtasutus (Estonia) has allocated $10 million for grant assistance to strengthen national cybersecurity.

Market weaknesses

Absence of consistent funding

- The unfavourable investment climate is complicated by war risks and low cybersecurity awareness.

Supply fragmentation in the market

- New cybersecurity startups often avoid cooperation with colleagues and do not tend to join business clusters.

Incomplete legal regulation of the sector

- The implementation of best practices in national legislation in the field of cybersecurity and information protection isn't complete yet and concerns particular issues. Thus this fact also deters the development of cybersecurity culture in both private and public sectors.
- Cyber defence requirements for the public sector and critical infrastructure, that are main consumers of products and services, do not fully comply with best practices, while the implementation of the requirements is still fragmented.

Sources: DataDriven Analysis, Interfax, Forbes, Microsoft Digital defence Report, Aspen Institute, PwC, Cybersecurity Strategy of Ukraine.

Challenges and prospects in the cybersecurity market

Market development opportunities

Market diversification

- The list of today's challenges and tools for implementing cybersecurity, both in the world and in Ukraine, is not completed and is expanding with the development of digital technologies.
- Information and narrative security, as well as OSINT practices are integrated consistently into the concept of "cybersecurity", which increases the sector of activity.

Potential increase in demand

- Progress in digitalisation is one of main challenges and reasons for changing approaches to security management and protection measures.
- The European integration refers to the gradual implementation of national and sectoral security practices, compliance with standards for digital products and services. In addition, this process will lead to the higher demand for implementation of organisational and technical security measures.

Conditions for new solutions implementation

- Wartime cyber threats and Ukraine's incomplete cybersecurity architecture make local markets great for testing experimental solutions in this area.
- Cybersecurity service providers have the chance to train their products on unique data and test them for resilience in the terms of today's challenges.

Risks for the market

Workforce shortage

- The convenience of outsourcing to foreign companies, wartime and the long-term outflow of talent abroad are the key reasons for the shortage of qualified employees in domestic companies.
- The problem of training specialists remains relevant. The quality of higher education often does not meet the needs and challenges these days.

The danger of cyberattacks from abroad

- In 2023 Ukraine accounted for the largest share of state-sponsored cyberattacks in Europe.
- Due to the war with Russia and political conflict with its allies (Iran and North Korea), the number and variety of cyberattacks from abroad, especially on critical sectors of the economy, is likely to increase.

System dependence on foreign supplies

- The operation of digital systems in Ukraine is possible thanks to the presence of foreign manufacturers and suppliers on the market.
- The Ukrainian market has difficulties in the production of hardware, which makes it quite vulnerable.

Sources: DataDriven analysis, Microsoft Digital Defence Report, Oxford University, National Cybersecurity Strategy.

2. Technologies

The following technologies will drive the greatest market growth over the next 5 years

Segrement*	Growth by 2029	Features
Cloud security	**+3,78** million USD or **226%**	• Segment that covers the protection of environments and data hosted in the cloud. • The adoption of cloud services is projected to grow, while the predominance of traditional methods of data storage in some business sectors will continue. • Projected growth leader in percentage terms.
Endpoint security	**+6,08** million USD or **85,8%**	• Segment refers to the protection of devices connected to the corporate network. • Along with the increase in the prevalence of remote work, this segment is expected to grow steadily (the second indicator, both in percentage and monetary terms).
Network security	**+29,4** million USD or **63,5%**	• Network security is a set of measures and capacities aimed at preventing unauthorised penetration into the network. • It is expected to grow steadily, accounting for the largest market share in quantitative terms.
Other	**+14,03** million USD or **58,1%**	• In addition, it includes the security of applications, data, etc. • There will be proportional moderate growth, as well as an increase in the use of advanced information technology in various business sectors.

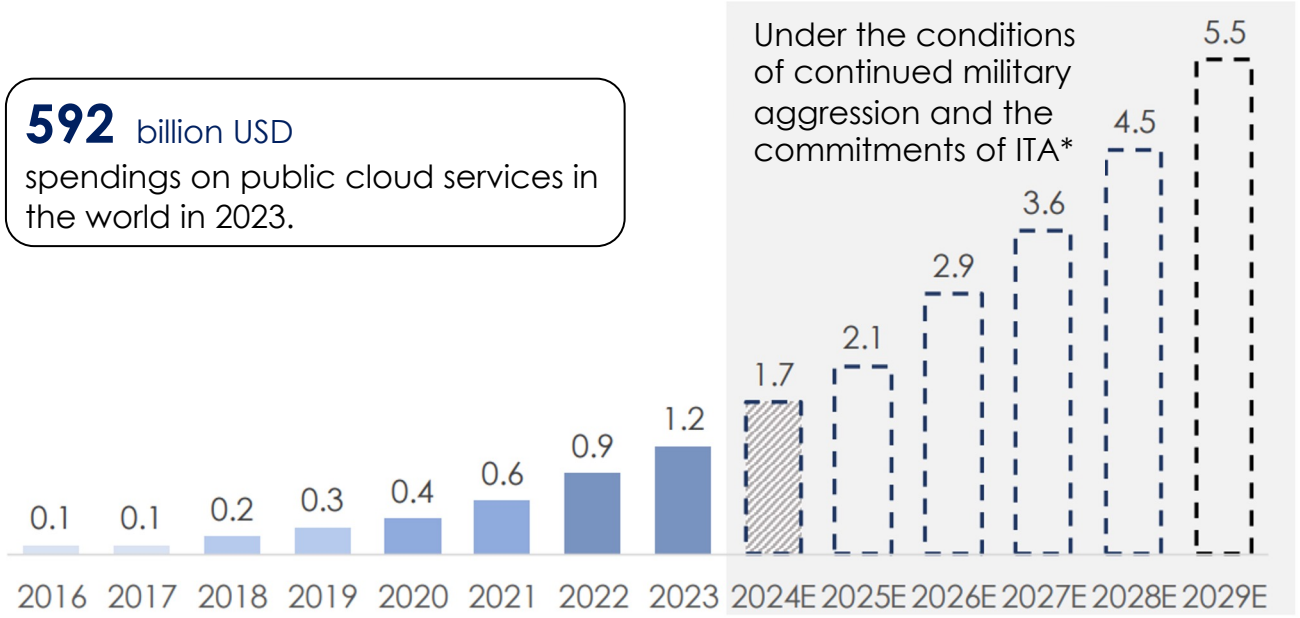
Notes: * The following segments will provide the largest market growth (security of cloud services – the largest relative growth, network security – the largest absolute growth, endpoint security – the second largest relative growth) // Sources: Statista, Expert interviews, DataDriven analysis.

Cloud security market tripled to $1.7 million during the full-scale invasion

Volume of the cloud security market in Ukraine 2016-2029E

Market size, in millions USD at the current exchange rate

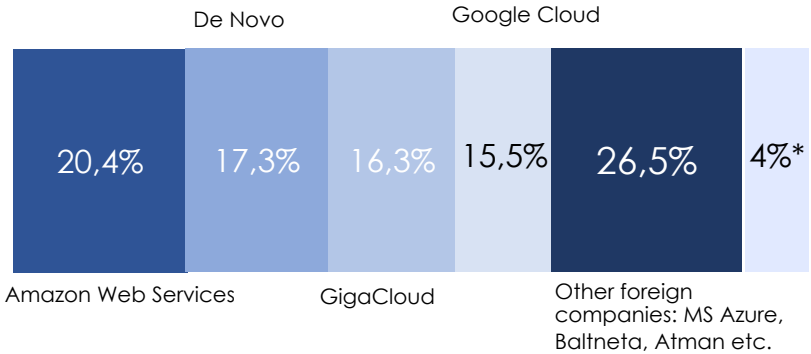
592 billion USD
spendings on public cloud services in the world in 2023.



Due to the likelihood of damage to services and systems during the Russian invasion, companies began transferring IT infrastructure to cloud services. After the beginning of the Russian invasion, the National Bank of Ukraine allowed financial institutions to move data and systems outside the country, which increased the demand for cloud services.

The current volume of cloud security market does not take into account significant volumes of solutions provided to government agencies free of charge within the framework of international technical assistance (ITA). After the end of hostilities and decreased amount of ITA, authorities will pay for the services, which will lead to an increase in the overall size of the cloud security market.

Share of companies in the cloud services market of Ukraine in 2022

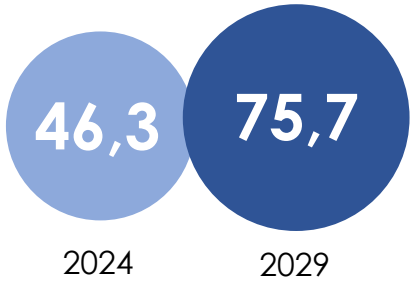


***Other Ukrainian companies: Ucloud, Parkovyi, etc.**

Notes: International technical assistance. Sources: Statista, Gartner, MTB.

Network and endpoint security segments will grow by 70% overall by 2029

Security of infrastructure and network

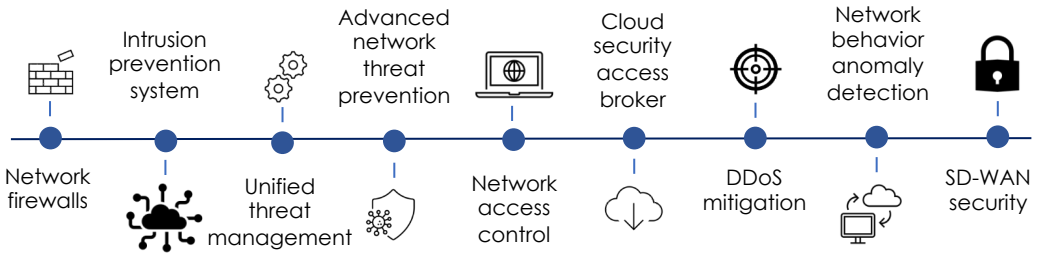


expected growth of the network security market in Ukraine, million USD

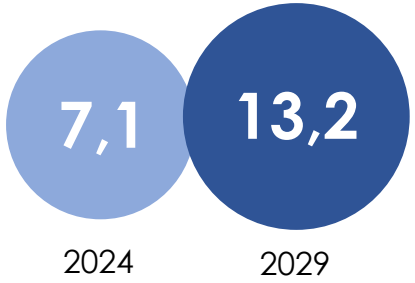
24,9 billion USD

expected global network security market size in 2024

9 elements of network security



Endpoint security



expected growth of the endpoint security market in Ukraine, million USD

Key players in Ukraine

Zillya, UnderDefense, CROWDSTRIKE, cisco, OCTAVA DEFENCE, ISSP, SentinelOne, IT.Integrator

Top 4 endpoint security trends

- Evolution of Zero Trust technologies
- AI deployment
- Strengthening protection for remote staff
- Integration of EDR / XDR

Main drivers

- Growth of cyber threats.
- Digital transformation and increase of dependence on endpoint devices.
- Remote & Hybrid work.

Sources: Statista, DataDriven analysis.

The use of artificial intelligence (AI) is one of the key innovations in the industry

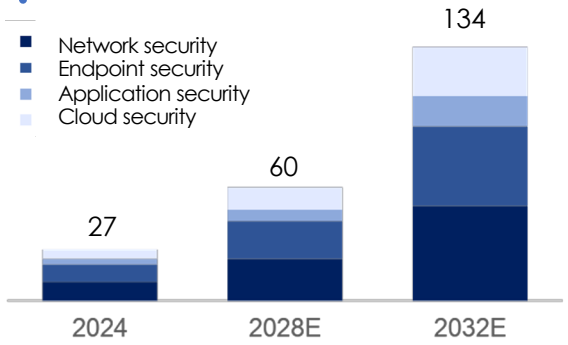
163

Global cybersecurity AI market size in 2033, billion USD

Network and endpoint security are showing significant growth, making them the largest segments in the AI cybersecurity market.

AI market in cybersecurity

billion USD



Currently*, there is no specific legislation on AI in Ukraine, but there are a number of soft laws that provide general guidelines for the implementation of such technologies

Pilot initiatives are being implemented (in particular, the Declaration on the Responsible Use of AI from the Ministry of Digital Transformation). During European integration processes, including the introduction of AI regulation in the field of cybersecurity, it is important to take into account Ukraine's ability to be competitive in comparison with the aggressor state during the implementation and application of such solutions.

Major AI advantages

Automation of routine tasks
- can track violations or anomalies automatically and respond to them without human intervention.

Cost-effectiveness
- helps minimize human mistakes, which is one of the main causes of cybersecurity breaches.

Speed up threat reduction

Main AI threats

Rise in cybercrime cases
- cybercriminals use AI actively to improve their attack methods.

Dependence on accurate data
- Data bias or insufficiency can lead to false positives, missed threats, or unfair targeting of specific users.

Speed up finding zero-day vulnerabilities

* As for Jan 2025

Sources: Ministry of Digital Transformation of Ukraine, Market.US.

3. Ecosystem

Major players in the cybersecurity market

Ukrainian cybersecurity ecosystem is actively growing now. At this stage there are the following features:

- **Partnership between the state, business, and international structures:** the private sector interacts with the state (for example, the State Service of Special Communications, the NBU, the NCSCC, the Security Service of Ukraine, the Ministry of Defence) and international structures for joint threat monitoring, data exchange, response, and training.
- **Closed community:** the domestic cybersecurity market seems to be even more closed and isolated than the global one, which makes it difficult for new players and startups to enter it.
- **Significant practical experience:** Ukrainian cybersecurity specialists have exceptional expertise in protecting against DDoS attacks and other types of cyberattacks, formed by wide experience in responding to Russian cyber aggression. Their practical experience in protecting critical infrastructure distinguishes them from regional competitors.

Notes: The sample of companies is illustrative.
Sources: DataDriven Analysis, Expert Interviews.

Different types of commercial players that are represented in the Ukrainian cybersecurity market

Distributors

AXOFT, bako tech, CLICO, COREWIN, ficha, FORT SOFT, headtechnology (it · security · distribution · services), iiTD (INTELLIGENT IT DISTRIBUTION), MUK (Classics of distribution), Oberig it, SoftKey, Softlist, SoftOnline, SOFTPROM

System integrators

IT.Integrator, ESKA (Integration), LANTEC, InDev (LAB), ACCORD GROUP, CBIT IT, Winncom Technologies, SECURITY, SiBiS, INTRA SYSTEMS, wise it, ISSP, seeton, integrity systems, netwave (networks for life), AM BITS, IT-Solutions (Інновації, що змінюють)

Professional Services[2]

iterasec, a ed pack, SOFTSERV, KPMG, BSG, CYBER UNIT, HackCtrl, Nova Digital, DataArt, EVE.calls, datamix, GlobalLogic, EY, pwc, PECB, TechMagic, apriorit, IO GUARDS, infopulse, Yalantis, CyberLab, <epam>, Support Your App, Deloitte., TÜV SÜD, RNB TEAM, RELEVANT, MODUS X, adaptiq, PakuriTy, ASTERS, Zazmic, astarios, UnderDefense, SOC PRIME

Vendors[3]

Small (>50 people)

COSSACK LABS, Evolveum, CQR, Plug the leak, PROTECTIMUS, LABYRINTH, DECEPTION, respeecher, Mantis Analytics, EVE.calls, A42.tech, Cybrex, CYBERJAB, OCTAVA DEFENCE, osavul, EXTRACTOR, SET CYBER LABS, FS (feel secured)

Medium (50-100 people)

Zillya (АНТИВІРУС), Syteca

Big (100<people)

BROADCOM, f5, Microsoft, Trellix, FORTINET, IBM, cisco, CROWDSTRIKE, TREND MICRO, eset, Check Point, paloalto NETWORKS

Notes: 1. The sample of companies is illustrative. 2. The category covers two types of companies: business consulting (audit, legal support) and technical consulting (IT solutions, internal projects, etc.). 3. Companies were divided into categories according to the number of employees.

Professional services market is strengthening and becoming an important part of the cybersecurity sector in Ukraine

Segmentation of professional services

Management and assessment

Includes building a cybersecurity management system, policy development and implementation, risk assessment, status assessment, audit, compliance check, certification, data protection impact assessment, etc.

Testing and vulnerabilities

Testing, threat intelligence and analysis, vulnerability management, code/web and application security analysis.

Other services

Include response planning, response management and investigation, training and training, monitoring.

Segment dynamics

Sources of funding

- Taking into account the high share of the need for attracting professional services from the public sector, the main source of funding for such services in Ukraine remains donor assistance.

Opportunities

- The need to comply with best practices and safety compliance requirements at the national and industry level is predicted to increase the demand for professional services.
- The uniqueness of specialists' experience in the Ukrainian market can be spread to international markets.

Trends

- Growing demand for external consultants to receive recommendations for strategic planning, risk management and cyber risk management.
- Strengthening protection requirements for critical infrastructure, as well as industry compliance requirements.

60% of the largest domestic system integrators provide cybersecurity services

System integrators are full-cycle cybersecurity service companies that specialise in implementing various security technologies into a single solution. They provide comprehensive services to ensure complete business protection from cyber threats.

Types of services

Solution development

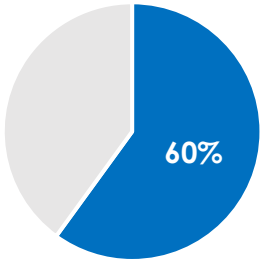
Development of a secure architecture and implementation of individual cybersecurity solutions.

Implementation and support

Comprehensive services from tasks to entire projects and maintenance of the company's infrastructure.

Trainings

Cybersecurity training for all skill levels, providing programs in sub-sectors as well.



Number of system integrators providing cybersecurity services of the top 35 players

- **Services used by system integrators:** mainly rely on the services of international vendors such as Cisco, IBM and Microsoft, etc. They often avoid the use of domestic services due to limited functionality.
- **Service affordability:** the services provided by system integrators are often too expensive for small and medium-sized enterprises, making them affordable overall to large companies with significant budgets.

Notes: 1. The sample of companies is illustrative.

Ukrainian vendors should look for a competitive advantage over international companies

The Ukrainian cybersecurity market is largely dominated by international companies that provide cutting-edge solutions and services. These players offer comprehensive cybersecurity tools that are increasingly being implemented by businesses and government organisations across the country. Domestic developers need to look for a competitive advantage over global companies.

Vendor size[1]	Needs	Examples[2]
Up to 50 employees	• Positioning and recognition needs. • The need to ensure the stability of the client portfolio and solve the insufficiency of qualified resources to meet new requests. • Lack of experience, which makes it difficult to attract investment. • The need to hire more cybersecurity professionals to meet customer needs.	COSSACK LABS, respeecher, Plug the leak, CYBERJAB, Cybrex, LABYRINTH, Mantis Analytics, FS feel secured, PROTECTIMUS, A42.tech, osavul, DECEPTION, SETCYBER LABS, CQR, OCTAVA DEFENCE, EXTRACTOR
From 50 to 100 employees	• Engaging a sufficient number of qualified specialists to expand a team: most companies on the market have up to 50 employees. • The need to ensure the stability of the client portfolio. • The need to attract additional financial resources to ensure growth. • The needs of structuring business activities and reviewing operational processes.	Zillya АНТИВІРУС, Syteca
Over 100 employees	• Scaling with access to international markets, which requires increasing the size of teams by hiring new specialists. • The need to strengthen regulatory compliance procedures in relevant markets of other jurisdictions. • The need to improve and extend operations for international growth while managing performance risks.	

Notes: 1. This slide presents Ukrainian vendors registered or with ultimate beneficiaries in Ukraine. The distribution of companies by size is conditional. 2. The sample of companies is illustrative // Sources: DataDriven analysis, Expert interviews.

International vendors dominate on Ukrainian market: more than 100 companies are presented

Notes: The sample of companies is illustrative.

Distributors mostly cooperate with international vendors because of wide range of solutions

A cybersecurity distributor acts as an intermediary between cybersecurity solution providers and resellers, partners, or system integrators. They buy cybersecurity products such as firewalls, antivirus software, and encryption tools from vendors and distribute them to other businesses in the supply chain.

Types of services

Software procurement: procurement of cybersecurity solutions from international and domestic suppliers, providing customers with access to the latest tools.

Logistics: deals with transportation and storage of cybersecurity products, ensuring timely delivery to intermediaries and end users.

Additional services: provide technical support, installation services, product training, and ongoing customer service.

Partnerships

Distributors mostly cooperate with global vendors because they provide the access to the most modern solutions for the local market.

Examples

Market challenges

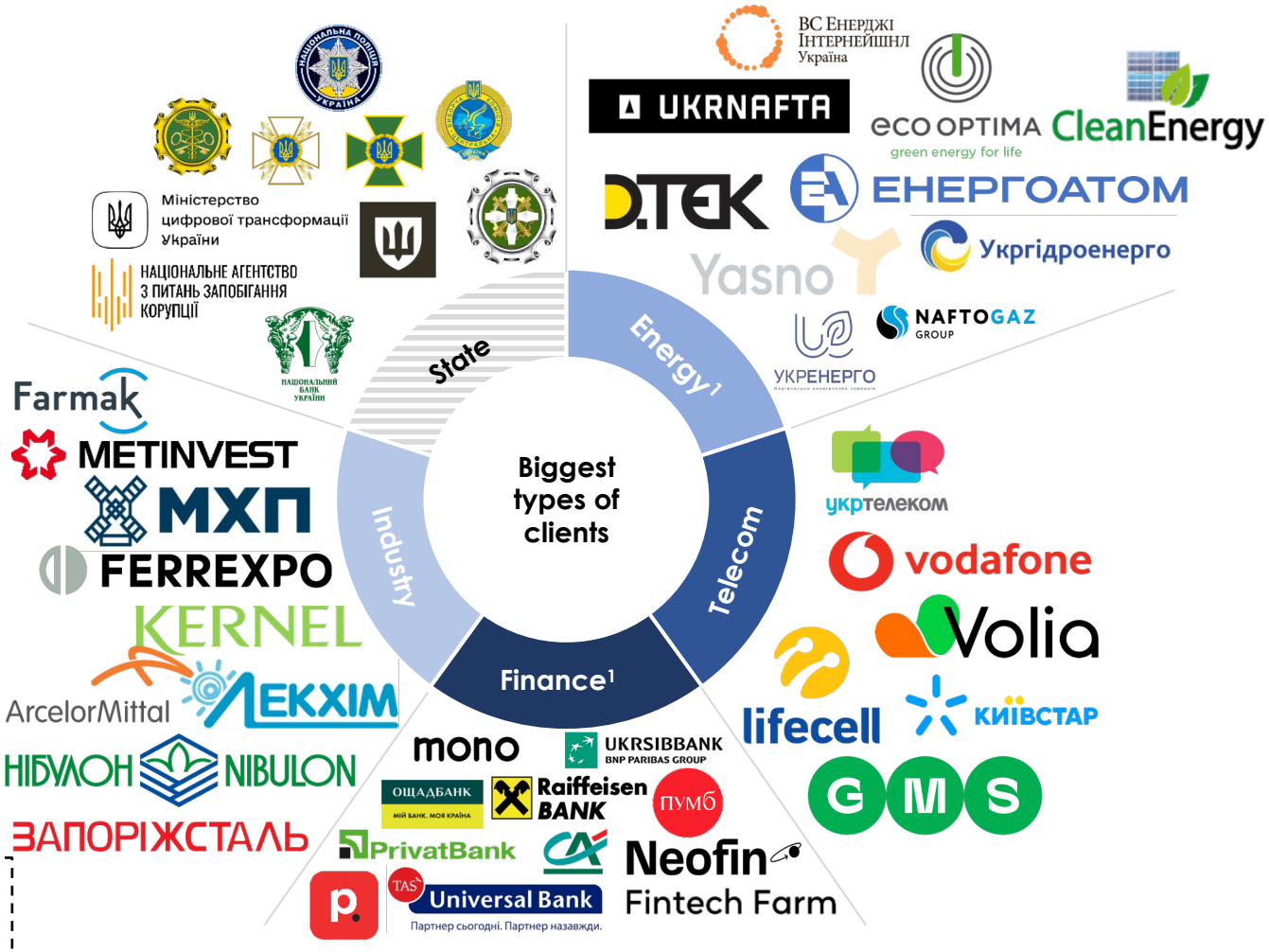
Supply chain disruptions: ongoing logistical challenges caused by factors such as the war in Ukraine make it difficult for distributors to ensure that the delivery of cybersecurity products will be done in time.

Limited number of local vendors: the market is dominated by international vendors, so distributors mainly deal with foreign products, which may limit the capabilities of domestic vendors.

Notes: The sample of companies is illustrative.
Sources: Expert interviews, DataDriven analysis.

Finance, telecom and energy are the largest commercial consumers of products and services in Ukrainian cybersecurity

- Since June 2022 Ukrainian businesses have faced an unprecedented increase in the number of cyberattacks. **Telecom, state information resources, energy, finance, industry** are among the main targets.
- Each client has unique needs based on the nature of the activity and specific threats:
  - **Finance:** the priorities are data protection, transaction security, compliance with industry standards (such as PCI DSS), and robust protection against fraud, phishing, and ransomware attacks.
  - **Telecom:** the priorities are the protection of network infrastructure, the prevention of DDoS attacks, and data protection.
  - **Industry:** the priorities are to protect industrial control systems (PSS) and ensure business continuity.
  - **State:** the priorities are the construction and modernization of protection systems in which state information resources are processed, including information with limited access, organisational and technical measures for cyber protection of critical information infrastructure, improvement of regulatory documents for the introduction of best practices.
  - **Energy:** the priorities are the protection of energy systems and energy supply chains, the security of operational technologies.



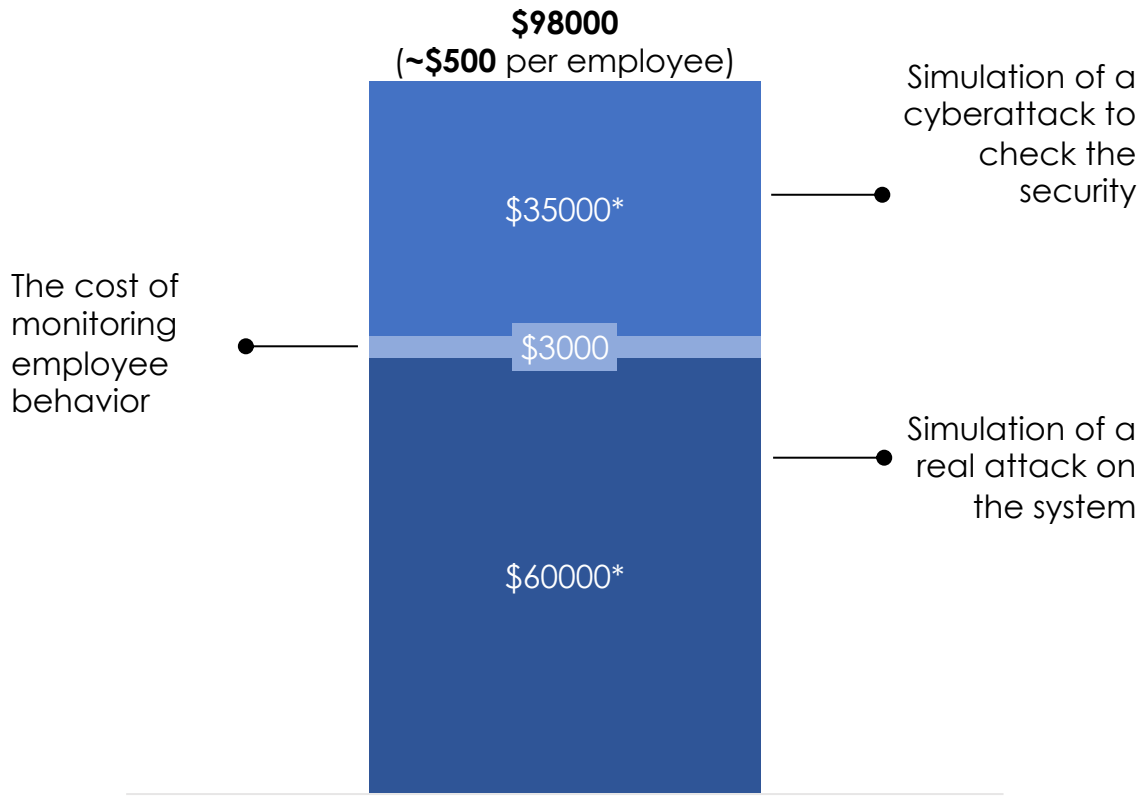
State holds the largest share among all consumers on the market
In the commercial market[1] the distribution is as follows:
1. Finance, 2. Telecommunication, 3. Energy, 4. Industry

Notes: 1. Although some companies are state-owned (e.g. Sberbank), they operate as commercial enterprises, so they have been included in the relevant categories of private players. 2. The sample of companies is illustrative // Sources: Forbes Ukraine, Expert interviews, DataDriven Analysis.

Depending on the size, companies can spend from 10 to 50% of their annual budget on cybersecurity

Cyber defence spendings of a company in Ukraine in 2023

(On the example of a company with 200 employees)



Level of use of cybersecurity services among companies

63% companies use the services of foreign vendors

37% companies work only with Ukrainian vendors

61% customers did not receive an offer to cooperate from Ukrainian vendors

% spendings on cybersecurity out of the total annual budget of companies

10-15% on average large companies* spend cybersecurity out of their annual budget

>20% on average small companies* that provide many customers with critical data spend

* Small companies – companies with up to 50 employees; large companies are companies with more than 250 employees.
Sources: Forbes Ukraine, Expert interviews, DataDriven analysis, USAID.

Formal education remains the object of criticism, while professional skill-development courses fill in the gaps

Key Conclusions

- Despite the fact that there are **55 public universities*** offering **educational programs in cybersecurity** (specialty No. 125), and at least **16 private IT schools** provide specialised programs, the quality gap between public and private education is significant. The ratio of public and private programs of **3.5:1** shows that quantity does not equal quality.
  - **Lack of practical skills:** many universities do not provide students with the necessary practical skills in cybersecurity, which results in a lack of hands-on experience and specialised knowledge required in the field of cybersecurity.
  - **Transition to general IT roles:** due to insufficient training, many students end up working in general IT roles such as front-end or back-end development.
  - **Private companies fill in the gaps:** they offer a wide range of practical programs and specialised courses, training in cybersecurity, taking into account the requirements of professional standards and industry.

Notes: *only the main universities were included in the analysis of public universities, excluding their affiliates.
Sources: Expert Interviews, DataDriven Analysis

Cybersecurity industry in Ukraine requires stimulation

- International assistance programs, which are the main source of financing the consumption of products and services in the field of cybersecurity, mostly prefer to select companies from their national market, ignoring the availability of offers on the Ukrainian market. The continuation of such a policy on a large scale is a reason for the possible degradation of the Ukrainian market;
- State should adopt programs and implement measures that could ensure the development of the competitiveness of the national industry. In addition to the possible localisation of R&D activities in the field of cybersecurity, the activity is carried out, inter alia, by obtaining unique information in the context of cyber aggression against Ukraine;
- It is advisable for the state not only to declaratively recognise, but to implement the principle of development of public-private partnership as one of the priorities of the state policy in the field of cybersecurity;
- Industries should consolidate its efforts through conferences, committees, clubs to promote the interests and interaction of all cybersecurity stakeholders in Ukraine consistently.

Associations[2] / Clubs

71% are members of professional groups on social media (Slack, Telegram, LinkedIn, etc.)

19% are members of specialised working groups and committees

EBA European Business Association

NATIONAL CYBERSECURITY CLUSTER

IT Ukraine Association

CISCA scientific cybersecurity association

Conferences

63% specialists participate in large-scale cybersecurity conferences

44% sector employees attend professional cybersecurity forums

DEFCON

REGIONAL CYBER RESILIENCE FORUM: LVIV

KYIV INTERNATIONAL CYBER RESILIENCE FORUM 2025

Expert Security

PCSITS

Notes: 1. The sample of associations, clubs and conferences is illustrative. 2. Associations with existing cybersecurity committees (EBA, IT Ukraine) were also added to the list. Sources: Berezha Security Group, Ukrainian Cybersecurity Market Review 2021, Expert interviews.

The main part of donor support is accounted for public sector, telecommunications and finance

Amount of funding by donors for cybersecurity

~$200 million

was allocated by Ukraine's partner countries for the development of cybersecurity infrastructure in Ukraine.

~$120 million

was allocated to Ukraine from the United States, especially through USAID, which is still the largest donor in cybersecurity field.

- Cybersecurity donors in Ukraine are focused on funding government initiatives, as well as businesses aimed at strengthening cybersecurity infrastructure and protecting critical facilities.
- The government receives support for the implementation of government projects, such as strengthening cyber defence and critical infrastructure protection, such as from **USAID, the UK and Danish governments.**
- In the business sector donors grant funding to telecommunications and finance projects that aim to improve cybersecurity solutions and ensure the smooth operation of companies.
- Although education is not a priority, some indirect support can be provided through government projects, such as the establishment of **Cyberlab**, **with EU support**.

USAID Grant Program to strengthen cybersecurity of critical infrastructure

$500K

a general grant support fund announced by **USAID** in **September 2024** to implement effective solutions to strengthen preparedness and reduce the vulnerability of Ukraine's critical infrastructure in cybersecurity.

Notes: The sample of donor organisations is illustrative

4. Investments

Young Ukrainian startups in the industry have growth potential especially because of focus on services and SMEs[1]

Funding opportunities for young startups

BRAVE1 UKRAINIAN DEFENSE INNOVATIONS

USAID FROM THE AMERICAN PEOPLE

USF

Ukrainian cybersecurity startups are able to get grants from Brave1 in the amount **of $12,000 to $194,000**, from USAID in the amount **of $20,000 to $150,000**, and from USF up **to $35,000** to develop their ideas and initial solutions.

Promising areas for the development of cybersecurity

- Since international vendors dominate most of the cybersecurity market, Ukrainian startups should focus on underdeveloped segments.
- Providing cyber defence solutions for sectors such as **education, small and medium-sized businesses, and community organisations** – especially those with limited internal resources – is an available option to grow for young startups.
- By focusing on markets with a low number of provided solutions, startups can occupy their niche, in which vendors show a lower level of activity.

Young Ukrainian cybersecurity startups with further growth potential

CYBER UNIT | SET CYBER LABS | LABYRINTH Better protection. Less complexity. More confidence. | CQR

A42.tech | DECEPTION Advanced Cyber Track | Dzerkalo Innovatins | Cybrex

CYBERJAB | LD | Plug the leak | EXTRACTOR

Notes: 1. Small and Medium Business. 2. The sample of startups is illustrative.
Sources: Brave1, USAID, Vector, Expert interviews, DataDriven analysis.

However, there are a number of obstacles to invest in late-stage security startups

Investments in cybersecurity in Ukraine show mixed results with some successes. At the same time, limited company activity and investment interest hinder growth.

Lack of innovation in startups

- Most vendors rely on existing solutions rather than developing innovative products.
- In fact, there are no powerful scientific centers in Ukraine capable of developing high-level innovations.

Industry complexity

- The cybersecurity industry is considered by investors as highly technical and complex, requiring specialised knowledge.
- The level of specialised education in Ukrainian universities does not meet the requirements of the time, which is why the talents of young teams often raise doubts for investors.

Shortage of specialised teams

- Ukraine lacks fully specialised cybersecurity teams (most players are part of broader IT teams).
- Participation in such startups is risky in terms of career prospects.

Absence of competitive advantage

- To compete with global solutions, local startups need to develop a unique competitive advantage.
- There were no notable success stories of cybersecurity startups in Ukraine, unlike sectors such as defence-tech.

Sources: Expert Interviews, DataDriven Analysis.

Despite the barriers in the sector, there are examples of successful startups with capital raising from investment funds

Osavul – a startup, founded in February 2022, that positions itself as representative of the "Information / Narrative Security" sector. The platform deals with customers in five countries, analyses text, video, and audio data on websites and social media to detect online threats. The company also plans to expand its operations from the B2G market to the B2B market.

Funding

$1 million	SMRK VC Fund
$3 million	SMRK VC Fund, 42 CAP, u.ventures

Mantis Analytics - a startup that helps organisaations expand safely using artificial intelligence. The platform provides **situational awareness** and **asset protection** and allows monitoring risks in real-time. The **Mantis Incident Feed** product helps enrich user data to detect threats.

Fundng

$240 thousand	NEZLAMNI
$50 thousand	ZAS VENTURES
$30 thousand	

SOC Prime – a startup founded by Ukrainians in the field of **cyber threat detection**. SOC Prime offers a marketplace of threat detection solutions ("Spotify for cybersecurity"), which lets organisations find and implement the necessary defence mechanisms. Developers monetise their content and customers gain access to innovative products.

Funding

Serie A investor pool ($13 million)

dnx ventures, Rembrandt Venture Partners, streamlined, Atlantic Bridge

A startup with Ukrainian founders, while Ukraine accounts for ~1% of sales

*Soc Prime was founded and based in Ukraine from 2015 to 2021, but after receiving Serie A funding, it relocated to the United States.
Sources: AIN, Osavul, Forbes Ukraine, Expert interviews, DataDriven Analysis.

5. About us

DataDriven provides research and consulting services that help work in the Ukrainian market

DataDriven is a generalist consulting firm…

Research

Leveraging our long experience in collecting, analysing, and interpreting data, alongside creating tangible and data-based recommendations for public and private actors.

Consulting

Applying deep knowledge of Ukrainian politics and business to benefit our clients. Paving out a way for the world to deal with Ukraine and Ukrainian enterprises to open the world.

…with a particular expertise in technologies of dual use…

Our public reports include:

- **Ukrainian commercial demining market** (April *2024*)

- **Ukrainian defence tech market** *(September 2024)*

- **Ukraine's unmanned surface vessels: impacts on sea warfare** *(October 2024)*
- **AI in demining** *(Drafting, 2025)*

…advising several types of clients:

Equipment manufacturers
(market entry, partnership facilitation, risk assessment, vendor due diligence)

Investment funds
(due diligence, market insights, portfolio support))

Startups
(expansion, technology validation, access to finance)

More information on dual-use, defence and demining practices here

6. Sources and Methodology

General methodology

Main sources of information

- Public sources such as official website of state institutions and agencies
- Officially published materials of public research
- Reputable Ukrainian and international media sources
- A short survey among investors and manufacturers / startups carried out by DataDriven
- Interviews with investors, startups and other industry stakeholders

Interview approach

- Interviews included both confidential and public conversations with representatives of the regulator, investors, start-up teams and independent experts.
- Interviews were complemented by baseline questionnaires, distributed through direct contact with representatives and industry associations.

Forecast approach

- Our data analysis allowed us to transform a set of statistical quantitative data into a qualitative assessment.
- At the same time, we took into account a wide range of market trends that could affect market development in different time frames.
- A special attention was paid to integrating the insights from a comprehensive set of interviewed stakeholders who are currently shaping the market.

Methodology of market sizing and ecosystem mapping

	**Sources & Data**	• **Size of cybersecurity market in Ukraine**: Statista • **Size of cyber solutions segment in Ukraine:** Statista • **Size of cybersecurity services in Ukraine:** Statista • **Size of world cybersecurity market:** Statista • **Size of cybersecurity market in Poland:** Statista
	**Methodology**	• **Market size assessment:** – **Data sampling**: considers companies from B2B, B2C, and B2G segments. The data is based on companies' cybersecurity spendings (excluding VAT and the number of cyberattacks). – **Market size modelling**: top-down approach – the overall size of the market is estimated from the macro level, based on the data from the global market, which is then projected onto the local market; bottom-up approach– the market size is built by aggregating data from individual companies and segments of the local market. Key sources include financial reports from leading companies, national statistics and data from security organisations, as well as country-specific metrics such as GDP and internet penetration rates. – **Forecasting:** a variety of forecasting methods (e.g. exponential smoothing, ARIMA) are used using indicators such as GDP, the number of Internet users and the level of digitalization. – **Currency:** the current exchange rate according to the NBU. • **Ecosystem mapping:** – **Ukrainian vendors:** companies in the field of cybersecurity in case of official legal registration in Ukraine or the presence of Ukrainian beneficiaries. – **International vendors:** cybersecurity companies that do not fall under the above criteria, but provide services to the authorities in Ukraine through distributors or system integrators.

This study is prepared only with the aim to familiarise with the cybersecurity market in Ukraine and does not possess any investment advice or recommendation for making any financial or investment decisions. The information presented in the report may be incomplete or change over time. Before making any investment decisions, we recommend reaching out to professional investment or financial experts for more detailed advice.

office@datadriven.group

DataDriven | Research & Consulting

Kyiv Paris London