Cyber Warfare - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 114 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Cyber Warfare Market size is expected to grow from USD 77.54 billion in 2024 to USD 185.65 billion by 2029, at a CAGR of 19.08% during the forecast period.

Cyberwarfare involves offensive and defensive operations, such as cyberattacks, espionage, and sabotage. The number of cyberattacks worldwide is increasing significantly. Cyberwarfare uses all vectors accessible to cybercriminals. These include viruses, email attachments, pop-up windows, instant messages, and other forms of dant messages, and other forms of deception on the internet.

Key Highlights
-The growth in the number of cyber attacks worldwide has the potential to damage the Internet-linked digital infrastructure of various government or private sector enterprises, raising the need for both offensive and defensive applications of cyber warfare solutions, which would create an opportunity for market growth.
-The priority in strengthening national security by international organizations and governments through increasing the cyber security capabilities of various countries, such as the USA, India, etc., due to increased security challenges within cyberspace during the forecast period is driving the market growth. For instance, in October 2022, the President of the USA announced a new US National Security Strategy to strengthen the country's position by including elements of national power such as diplomacy, development cooperation, economic statecraft, intelligence, and defense, which would increase the demand for cyber warfare solutions due to their applications in country's intelligence and defense sector.
-Additionally, developing countries, such as China and India, have been strategizing to increase their countries' capabilities in cyber defense, supporting market growth. For instance, in February 2023, India planned to launch the National Cyber Security Strategy 2023 by updating the old strategy of 2013, and the country has created an International counter Ransomware Taskforce

in collaboration with the Finance and legal affairs ministries of the country.
-However, the increasing demand for cyber warfare solutions has increased the demand for cyber security professionals worldwide, which has created a gap in the skilled cyber security workforce due to the sudden rise in demand, challenging the market growth.
-COVID-19 caused significant disruption to business on a global scale. It accelerated the growth of cyber criminal activities in private and government enterprises supported by digital transformation with the increase in internet use for work, retail, recreation, and education, driving a surge in online traffic. The increase in cyber-attacks and frauds during the pandemic has created an opportunity for cyber warfare solutions due to their application in minimizing the cyber risks and fueled the market during and in the post-pandemic period.

Cyber Warfare Market Trends

Defense Sector to be the Largest End User

- The defense sector is expected to hold a significant market share in the cyber warfare market. The defense sector is investing heavily in digital security units to moderate and discourage the potential risk from a country and state programmer. The rise of innovations and the Internet of Things (IoT) in the resistance is foreseen to be the driving component for the use of the digital fighting framework in the defense segment.
- There is significant growth in investment in cybersecurity solutions to avoid theft of intellectual property and compromising systems that are used to monitor and control the country's defense systems and capabilities. To keep pace with modern defense advancements, countries have developed new technologies such as unmanned vehicles and hypersonic weapons. These advancements are highly dependent on data and connectivity, making them susceptible to breaches and attacks. Recent technological advancements in the defense sector present opportunities and risks for international peace and security. Thus, there is a growing necessity for countries to focus on developing countermeasures by adopting cyber warfare solutions to safeguard critical information.
- Moreover, while defensive cyber operations are necessary to protect a network, governments worldwide also focus on Offensive Cyber Operations (OCOs) in military planning. In April 2023, the UK government continued to adjust its cyber response to the growing threat posed by nation-state adversaries, in line with its latest National Cyber Strategy (NCS), published in December 2022. After introducing the National Protective Security Authority (NPSA), the government decided to open up on its offensive cyber capabilities. The National Cyber Force (NCF) shared the principles under which it conducts covert offensive cyber operations in a first-of-its-kind guide.
- Additionally, the increasing defense expenditure of various countries in the past few years has further created growth potential for adopting cyber warfare solutions. For instance, according to the data from SIPRI IMF, in 2022, military spending worldwide amounted to USD 2.24 trillion US dollars, the highest during the period under consideration. Military spending worldwide significantly rose from USD 1.79 billion in 2011 to USD 2.24 billion in 2022. The United States accounted for nearly 40% of total military expenditures nation worldwide, coupled with high adoption of advanced technologies in the defense and military sector.
- The North American Region is expected to be a prominent market for adopting cyber warfare solutions in the coming years. The significant presence of major market vendors, coupled with a substantial rise in military expenditure in the past few years, indicates growth potential for the adoption of cyber warfare solutions in the defense sector of the region. For instance, according to the SIPRI Military Expenditure Database, military spending in the United States rose from USD 633.83 billion in 2015 to USD 876.94 billion in 2022.

North America is Expected to Hold Significant Market Share

- The digitalization trends in the public and private sector organizations of the USA and Canada are raising the vulnerability of the region's digital infrastructures by exposing the digital services to cyber attacks, which would fuel the adoption of cyber warfare solutions in North America due to their capability in protecting, detecting, and preventing Cyber threats.
- The global rivalry between the USA with Russia, and China for geo-political reasons has led to increased cyber attacks on the USA's IT infrastructures and functions due to the trend of cyber wars, which has created a demand for the market during the forecast period. For instance, in June 2023, the Cybersecurity and Infrastructure Security Agency, a government-owned agency of the USA, stated that US federal government agencies had been hit in a global cyberattack by Russian cybercriminals, and the Department of Energy of the USA had been victimized among the multiple federal agencies breached in the hacking campaign.
- The governments of the USA and Canada are investing in their strategic priorities in strengthening their cyber security defense and offense to be competitive in the cyberspaces, which is creating an opportunity for the market vendors, such as General Dynamics, Boeing, etc., in the North American market due to their expertise in providing cyber warfare solutions.
- Additionally, Innovation, Science and Economic Development Canada has established a non-repayable contribution agreement with selected applicants to form a Cyber Security Innovation Network in Canada with USD 80 million over four years (2021-22 to 2024-25). The Canadian government has introduced this network with a vision to support research and development in the Canadian cyber security space by collaborating with the country's post-secondary institutions, the private sector, and other partners to accelerate the growth of innovative cyber security products and services, fueling the commercialization of cyber warfare solutions in the country during the forecast period.
- The Banking, Financial Services and Insurance (BFSI) sector of the region is significantly contributing to the market share of the North American cyber warfare market because financial sectors of the region have prioritized their strategy in strengthening cyber security to fight against the increasing number of cyber attacks in the region's financial sector. In addition, the four cyber security laws proposed in 2023 in the USA, such as the New York State Department of Financial Services (NYDFS) rules to strengthen the cyber defense mechanism of the region's financial sector, would create an opportunity for market growth.

Cyber Warfare Industry Overview

The cyber warfare market is highly fragmented, with the presence of major players like BAE Systems PLC, The Boeing Company, General Dynamic Corporation, Lockheed Martin Corporation, and Raytheon Technologies Corporation. Players in the market are adopting strategies such as partnerships and acquisitions to enhance their product offerings and gain sustainable competitive advantage.

In April 2023, An MoU was signed by Siemens and Leonardo to provide cybersecurity solutions for infrastructure in the industrial, oil and gas, and energy sectors. The companies stated that the intervention's primary focus would be on the resilience of the automation and connectivity systems against incidents and cyberattacks that monitor and oversee critical infrastructures' assets, machinery, and procedures.

In October 2022, Booz Allen Hamilton Inc. announced its acquisition of EverWatch. EverWatch Corp., a portfolio firm of Enlightenment Capital, enhances Booz Allen's comprehensive cybersecurity solutions with its highly qualified staff, emphasis on mission-critical classified programs, and knowledge in specialized software development, cyber, and analytics.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Cyber Warfare - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 114 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-04
		Signature