Cyber Warfare - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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 estimated at USD 92.33 billion in 2025, and is expected to reach USD 221.08 billion by 2030, at a CAGR of 19.08% during the forecast period (2025-2030).

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, including viruses, email attachments, pop-up windows, instant messages, and other forms of deception on the internet.

The growth in the number of cyberattacks 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.

International organizations and governments prioritize strengthening national security by increasing the cyber security capabilities of various countries, such as the United States and India, due to increased security challenges within cyberspace in recent years. According to a survey by the Center for Internet Security, cyberattacks on state and local governments increased from 2022 to 2023. The center found that malware attacks increased by 148%, while ransomware incidents were 51% more prominent during the first eight months of 2023.

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. The country has created an International Counter Ransomware Taskforce in collaboration with its finance and legal affairs ministries.

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 businesses 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 cyberattacks and fraud during and after the pandemic has created an opportunity for cyber warfare solutions due to their application in minimizing the cyber risks and fueled the market during the post-pandemic period.

Cyber Warfare Market Trends

Defense is Expected to be the Largest End-user Industry

- The defense segment is expected to hold a significant market share in the cyber warfare market. The defense industry is investing heavily in digital security units to moderate and discourage potential risks from country and state programmers. The rise of innovations and the Internet of Things (IoT) in the resistance are expected to be the driving components for the use of the digital fighting framework in the defense industry.
- There has been 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. Countries have developed new technologies, such as unmanned vehicles and hypersonic weapons, to keep pace with modern defense advancements.
- These advancements are highly dependent on data and connectivity, making them susceptible to breaches and attacks. Technological advancements in the defense industry may present opportunities as well as 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 adjusted its cyber response to the growing threat of nation-state adversaries. This was in line with its latest National Cyber Strategy (NCS) published in December 2022. After introducing the National Protective Security Authority, the government decided to communicate about its offensive cyber capabilities. The National Cyber Force (NCF) of the country shared the principles under which it conducts covert offensive cyber operations.
- Additionally, the increasing defense expenditure of various countries in the past few years has created growth potential for adopting cyber warfare solutions. For instance, according to the data from SIPRI, military spending worldwide significantly rose from USD 1.80 billion in 2017 to USD 2.44 billion in 2023.
- North America 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 adopting cyber warfare solutions in the region's defense industry.

North America is Expected to Hold Significant Market Share

- The digitalization trends in the public and private sector organizations of the United States and Canada are raising the vulnerability of the region's digital infrastructures by exposing digital services to cyberattacks. This scenario would fuel the adoption of cyber warfare solutions in North America due to their capability to protect, detect, and prevent cyber threats.

- The global rivalry between the United States, Russia, and China for geo-political reasons has led to increased cyberattacks on the IT infrastructures and functions of the United States due to the trend of cyber wars. For instance, in June 2023, the Cybersecurity and Infrastructure Security Agency, a government-owned agency of the United States, stated that US federal government agencies were hit in a global cyberattack by Russian cybercriminals, and the US Department of Energy was victimized among the multiple federal agencies breached in the hacking campaign.
- The governments of the United States and Canada are investing in their strategic priorities to strengthen their cyber security defense and offense to be competitive in cyberspace. This may create an opportunity for market vendors, such as General Dynamics and Boeing, in the North American market due to their expertise in providing cyber warfare solutions.
- Innovation, Science and Economic Development Canada 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 introduced this network with a vision to support research and development in the Canadian cybersecurity space by collaborating with the country's post-secondary institutions, the private sector, and other partners to accelerate the growth of innovative cybersecurity products and services, fueling the commercialization of cyber warfare solutions in the country during the forecast period.
- The 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 addition, the four cyber security laws proposed in 2023 in the United States by the New York State Department of Financial Services (NYDFS) aim to strengthen the cyber defense mechanism of the region's financial sector, which 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. The players in the market are adopting strategies, such as partnerships and acquisitions, to enhance their product offerings and gain a competitive advantage.

- In November 2023, BAE Systems Detica launched CyberReveal, its defense-grade cyber security product, to the commercial market for companies to use in-house for the first time. CyberReveal is an analytics and investigation product that provides companies with intelligence to protect their valuable property and sensitive commercial information from being stolen or compromised by cybercriminals.
- In April 2023, Siemens and Leonardo signed an MoU to provide cybersecurity solutions for infrastructures 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.

Additional Benefits:

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

Table of Contents:

1 INTRODUCTION
1.1 Study Assumptions and Market Definition

1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHTS
4.1 Market Overview
4.2 Industry Attractiveness - Porter's Five Forces Analysis
4.2.1 Bargaining Power of Suppliers
4.2.2 Bargaining Power of Buyers
4.2.3 Threat of New Entrants
4.2.4 Threat of Substitutes
4.2.5 Intensity of Competitive Rivalry
4.3 Value Chain Analysis
4.4 Assessment of the Impact of COVID-19 on the Market

5 MARKET DYNAMICS
5.1 Market Drivers
5.1.1 Increasing Concerns Regarding National Security
5.1.2 Increase in Defense Spending
5.2 Market Challenges
5.2.1 Lack of Cyber Warfare Professionals

6 MARKET SEGMENTATION
6.1 By End-user Industry
6.1.1 Defense
6.1.2 Aerospace
6.1.3 BFSI
6.1.4 Corporate
6.1.5 Power and Utilities
6.1.6 Government
6.1.7 Other End-user Industries
6.2 By Geography***
6.2.1 North America
6.2.2 Europe
6.2.3 Asia
6.2.4 Australia and New Zealand
6.2.5 Latin America
6.2.6 Middle East and Africa

7 COMPETITIVE LANDSCAPE
7.1 Company Profiles*
7.1.1 BAE Systems PLC
7.1.2 The Boeing Company
7.1.3 General Dynamic Corporation
7.1.4 Lockheed Martin Corporation

7.1.5 Raytheon Technologies Corporation
7.1.6 Mandiant Inc. (fireeye Inc.)
7.1.7 Leonardo SpA
7.1.8 Booz Allen Hamilton Inc.
7.1.9 DXC Technology Company
7.1.10 Airbus SE

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

Cyber Warfare - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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	2026-03-01
		Signature