Cyber Weapons Market Size Expected to Reach $23.7 Billion by 2031

The cyber weapons market was valued at $9.2 billion in 2021, and is estimated to reach $23.7 billion by 2031, growing at a CAGR of 10.1% from 2022 to 2031.

WILMINGTON, DE, UNITED STATES, September 4, 2025 /EINPresswire.com/ -- North America currently dominated the global cyber weapons market in 2021. This is primarily due to an increase in government spending to keep cyberspace stable. Lot of research and debates indicate that some nations and organizations in North America have created and employed cyber weapons. The development and use of cyber weapons has received significant attention from the American government and military. Canada has also been actively involved in the development of cyber weapons and has established Cyber Operators, which cooperate with other government departments and agencies as well as Canada's allies, to increase the ability of the Department of National Defense and the Canadian Armed Forces to maintain a secure cyber environment.

Get a Sample PDF Report to understand our report before you purchase:
https://www.alliedmarketresearch.com/request-sample/A50260

Key players operating in the global cyber weapons market include BAE Systems, Booz Allen Hamilton Inc., Broadcom, Cisco Systems, FireEye Inc., General Dynamics Corporation, Kasperksky Lab, Lockheed Martin Corporation, Mandiant, and Raytheon Technologies Corporation.

The use of cyber weapons has grown significantly as the U.S. attempts to develop new tools and capacities for national security and defence. The National Security Agency (NSA) and Cyber Command are at the center of the American government's significant investments in the creation of cyberweapons. The development of cyber weapons has been fueled by both the rise in reliance on digital infrastructure and the threat of cyberattacks from other countries, criminal groups, and other entities. The U.S. government accessed crucial data from other countries using cyber weapons. According to Interesting Engineering, in September 2022, the U.S. National Security Agency's (NSA) cyber-warfare unit used 41 different types of weapons to steal critical technology data from a Chinese space and aviation university. This data included the configuration of critical network equipment, network management information, and critical operational information. Specific information regarding their creation and use is not made available to the general public because the use of cyber weapons by the U.S. is highly classified. Also, it is evident that cyber weapons have grown in importance as a tool in the U.S. national

security strategy, which has fueled the growth of the cyber weapons business in the country.

Make a Direct Purchase: https://www.alliedmarketresearch.com/checkout-final/a731acffdd67d64856554966a51925d7

On the basis of application, the global cyber weapons market is segmented into national defense systems, public utility, automated transportation systems, smart power grid, industrial control systems, financial systems, communication networks, and others. The development of international trade and the improvement of living standards have been facilitated by transportation infrastructure. Communities all over the world are connecting more than ever because of huge advancements in the flow of people and things. Yet, the presence of various control systems and auxiliary systems is increasing the interconnection and complexity of transportation networks. The use of communications and IT has increased the effectiveness and functionality of transportation networks, but it has also raised the possibility of vulnerabilities. Attacks using cyber weapons on transportation networks can take a variety of shapes and have a range of possibilities and outcomes. A popular attack method that overburdens the system and causes a denial-of-service (DoS) for the entire system is traffic redirection to the server. A different type of cyber weapon effect is the theft of personal information, which can result in the displacement of expensive and/or dangerous commodities like explosives, radioactive agents, chemical, and biological chemicals, which is problematic for the transportation industry. Terrorists might utilise these materials, if they were stolen, to make bombs and other deadly weapons. Automated transportation systems that integrate cyber weapons are used to prevent or respond to such incidents, which supports the market's growth.

Significant factors that impact the growth of the cyber weapons market comprises the rise in the need for infrastructure protection, advancements in technologies such as AI and ML, a significant rise in international conflicts, and an increase in expenditure for cyber weapons by government and commercial entities. However, factors such as the high cost of the development of cyber weapons and technical difficulties in the deployment of effective cyber weapons are expected to hamper the market growth. Furthermore, the rise in demand for defense intelligence and surveillance in military operations and the increase in presence of relevant digital equipment across cyber warfare are expected to create new growth opportunities for the market during the forecast period.

Furthermore, cyberattacks in all their forms are currently a significant problem on a global scale. Cyber weapons are easy to use anywhere in the world, low risk, cheap, and very effective. This new category of weapons is available to many states, terrorist or extremist groups, non-state actors, and even private persons to strike public utilities. Cybercrime organizations efficiently produce cyber weapons to thwart or defend against such attacks. Together with nation-states and non-state groups, newcomers also possess unparalleled espionage and surveillance capabilities. They frequently act as the start of unlawful actions against public services that result in damage, interruption, and monetary gain. This is anticipated to fuel market expansion during the forecast period.

To Ask About Report Availability or Customization, Click Here:
https://www.alliedmarketresearch.com/purchase-enquiry/A50260

COVID-19 Impact Analysis

Furthermore, cybersecurity needs to get greater attention, due to regulatory restrictions brought on by the coronavirus and the increased cyber danger faced by remote workers. For instance, the fact that 47% of people who work from home have fallen victim to phishing scams shows this. The coronavirus pandemic is seen by cybercriminals as an opportunity to ramp up their criminal activity by preying on remote workers and the public's intense interest in coronavirus news, such as fraudulent fake coronavirus-related websites.

KEY FINDINGS OF THE STUDY

By type, the offensive segment is anticipated to exhibit significant growth in the near future.
By application, the communication network segment is anticipated to exhibit significant growth in the near future.
By end user, the corporate segment is anticipated to exhibit significant growth in the near future.
By region, Asia-Pacific is anticipated to register the highest CAGR during the forecast period.

David Correa
Allied Market Research
+ +1 800-792-5285
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X
