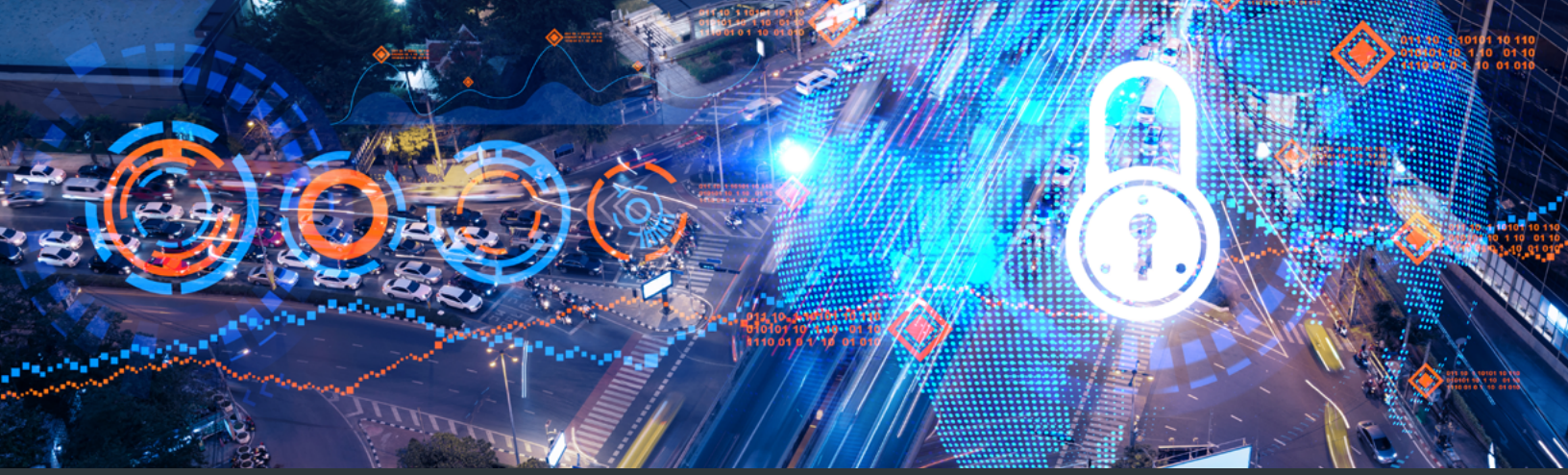


PROTECTING CRITICAL INFRASTRUCTURE: THE CRUCIAL ROLE OF CYBERSECURITY

ABIresearch
THE TECH INTELLIGENCE EXPERTS℠



Introduction

The systems and services that make society run and shape our daily lives– energy, banking, healthcare, communications, etc. – are all essential. However, they are also all vulnerable to cyberattacks. If these connected systems were to be compromised by a malicious actor, the consequences could be catastrophic.

That's why governments, utilities, and key stakeholders across many industries are researching and investing in Critical Infrastructure (CI) cybersecurity applications and services. In fact, according to ABI Research's latest forecast, CI accounts for 60% of overall global cybersecurity spending, which will equate to roughly US$235 billion in 2027.



Our latest Critical Infrastructure Security Market Data report offers a detailed breakdown of digital security spending across eight key sectors: defense, energy, finance, health, Information and Communication Technology (ICT), public security, transport, and water & waste management. Here are some critical highlights and key trends illuminated by that data.

Introduction 2

Key Market Expectations 3

Sector Spotlight

- *Defense Sector* 5
- *Energy Sector* 6
- *Information and Communications Technology (ICT) Sector* 7
- *Financial Sector* 8

Next Steps 9





Key Market Expectations

As the cyberthreat continues to grow for CI stakeholders and geopolitical tensions heat up, ABI Research foresees the following market dynamics developing:



Cybersecurity consumers will increasingly seek to secure Operation Technology (OT), connected devices, and critical software supply chains. This means services such as firewalls, unidirectional gateways, and Software Bill of Materials (SBOM) management will be in high demand to curb cyberthreats.



By 2027, the defense market will spend the most on cybersecurity. Along with more spending, governments are also increasing their footprint in cybersecurity regulation and strategy. Governments, including the United States, are also pushing for cyber-offensive operations instead of a purely defensive strategy, which could lead to new areas of CI security spending and expansion.



The United States and the European Union (EU) are encouraging industries to adopt secure-by-design principles. This means new business opportunities for cybersecurity vendors, as well as hardware and software providers offering services that ensure compliance with government regulations. For example, the United States recently released its National Cybersecurity Strategy, demanding that stakeholders must "ensure that systems are designed to fail safely and recover quickly."



Information and Communications Technology (ICT) currently spends the most on CI cybersecurity. The growth of 5G is expected to maintain and expand demand for ICT security starting in 2025 and beyond. Cybersecurity vendors should also recognize that securing remote networks has been a key pillar of ICT operators' operations, especially as the sector will continue to embrace some levels of remote work in the foreseeable future.



Key Market Expectations



Cybersecurity spending in the transport sector was significantly affected during the pandemic, when many sectors ground to a halt (most notably, the aviation industry). However, the sector is now showing signs of recovery, especially in the aviation industry, where there has been a surge in demand. The market presents significant opportunities for vendors that offer services tailored to markets with special sector-specific needs, such as rail, shipping, and aviation.



In general, budgetary trends, along with the growing interest of government regulators in securing CI, coupled with geopolitical tensions and state involvement in offensive cyberwarfare, indicate a burgeoning market for players in the cybersecurity landscape. These include industrial vendors, hardware and software Original Equipment Manufacturers (OEMs), and system integrators that can design and implement systems that are resilient to cyberattacks.



The recent release of Washington's offensive cybersecurity strategy may result in the emergence of new areas of conflict between the United States and its geopolitical rivals. This, in turn, could lead to the growing monetization of cyberwarfare, similar to conventional defense markets.

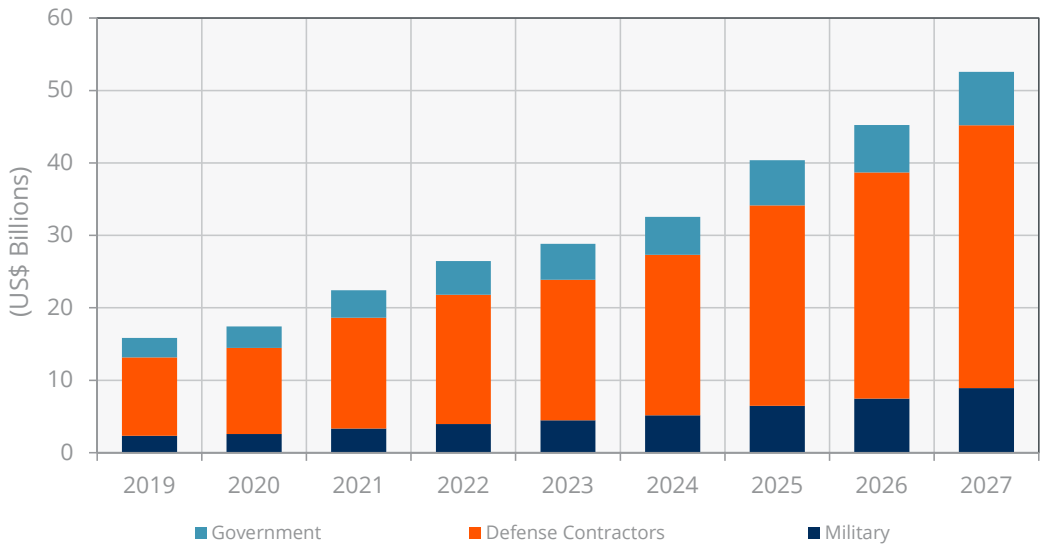
Sector Spotlight

Defense Sector

ABI RESEARCH FORECAST

Out of all the CI sectors, the defense sector will spend the most by 2027. In 2023, the defense sector worldwide is expected to invest a grand total of US$28.8 billion in cybersecurity technologies and services. This doesn't come as much of a surprise considering defense has historically been well-funded, using funds for everything from national security and intelligence efforts to cyber war games simulation. Breaking down the cybersecurity spending on CI defense, contractors account for 67% of that spending, with government and military spending lagging behind.

The chart below depicts defense CI cybersecurity spending by sub-sector.



KEY TRENDS TO WATCH

The armed conflict between Russia and Ukraine has raised alarms for CI stakeholders about the potential for conflict to bleed into cyberspace. These concerns will spur even larger cybersecurity budgets from organizations with a vested interest in CI security, notably the North Atlantic Treaty Organization (NATO) and the European Union (EU). While cyberattacks carried out in the Russia-Ukraine conflict have mainly been limited to common Distributed Denial of Service (DDoS) attacks, ransomware distribution, and fake news/propaganda, the threat to connected infrastructure is expected to grow as malicious actors aim to hijack physical controls.

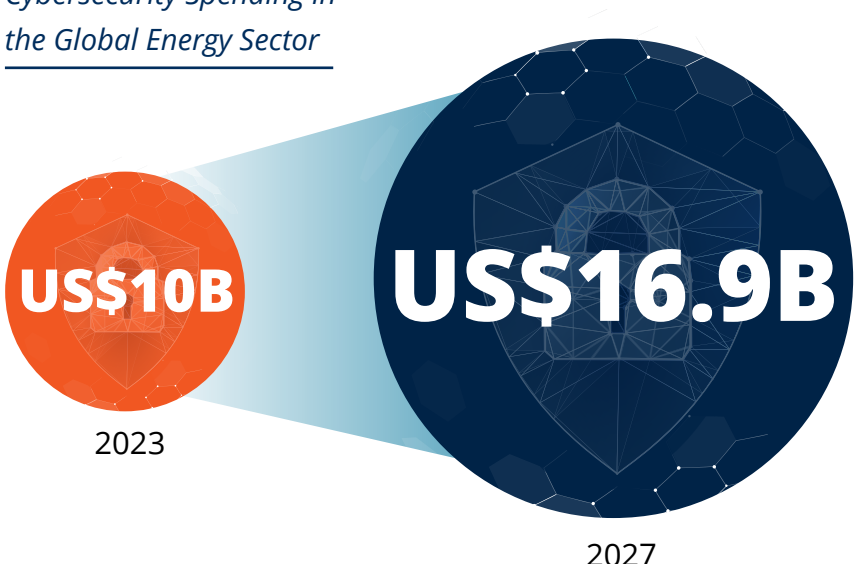
Sector Spotlight

Energy Sector

ABI RESEARCH FORECAST

Annual cybersecurity spending in the global energy sector is projected to increase from US$10 billion in 2023 to US$16.9 billion in 2027.

Cybersecurity Spending in the Global Energy Sector



KEY TRENDS TO WATCH

Cyberattacks targeting the Ukrainian power grid date back to years before the 2022 Russian invasion, but the full-fledged conflict now exacerbates the threat even further (including for countries supporting Ukraine). But besides that, cybersecurity stakeholders in the energy sector are also heavily influenced by the sanctions placed on Russia, notably for European countries dependent on Russia for oil and gas.

Moreover, the pressures to tackle climate change will see energy utilities continue to transition away from fossil fuels and invest in renewable sources of power generation. The transition also means more digitization and connected systems, which, in turn, will further stimulate cybersecurity spending to safeguard the new infrastructure.

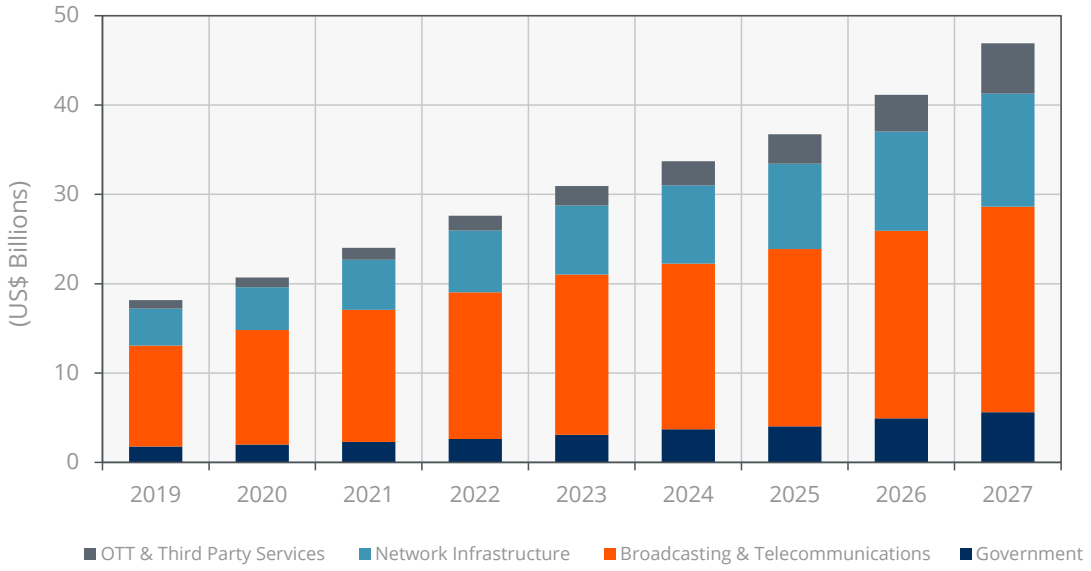
Sector Spotlight

Information and Communications Technology (ICT) Sector

ABI RESEARCH FORECAST

Information and Communications Technology (ICT) is strongly intertwined with critical infrastructure, so protecting it is a salient aspect of CI cybersecurity. That's why ICT teams are currently the biggest spenders on cybersecurity, expected to invest US$30.9 billion in security in 2023. By 2027, the ICT sector will only be outspent by the defense sector. Broadcasting & telecommunications represents 58% of all spending in ICT, followed by network infrastructure, government, and Over-the-Top (OTT) & third-party services.

The chart below depicts defense ICT CI cybersecurity spending by sub-sector.



KEY TRENDS TO WATCH

One of the main catalysts for the recent boost in cybersecurity spending in the ICT sector was the ubiquitousness of work-from-home policies fueled by the COVID-19 pandemic lockdowns. As millions more people work from home, securing remote networks has been a key pillar of ICT operators' operations. Additionally, the growth of 5G is expected to stimulate even more demand for ICT security starting in 2025 and beyond.

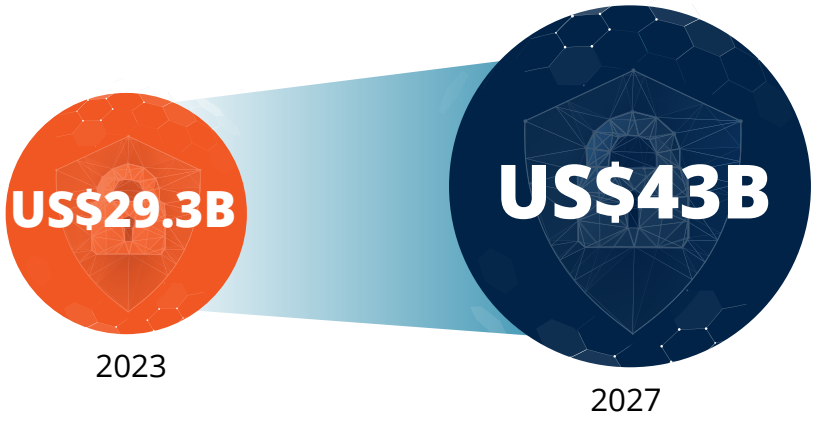
Sector Spotlight

Financial Sector

ABI RESEARCH FORECAST

The financial industry, given its significantly data-sensitive nature, currently outspends all but the ICT sector on cybersecurity. In 2023, financial firms will invest US$29.

Financial Firms Investment in Cybersecurity



KEY TRENDS TO WATCH

Investment in cybersecurity within the financial sector has traditionally been stable, although a looming 2023 recession could potentially shift budgets around. Financial services are becoming more and more digitized, so security is and will continue to be a top priority. The biggest focus areas for the sector include protecting networks and electronic transactions, combating fraud, and reinforcing internal organizational protection mechanisms (e.g., perimeter security and incident response).



Next Steps



Do you want a clearer assessment of where CI industries allocate their cybersecurity budgets?

Including other sectors not included in this report?
For a far more detailed overview, download ABI Research's CI Security market data report.

This content is part of the company's Cybersecurity Applications and Smart Urban Infrastructure Research Services. To learn more about any of our Cyber & Digital Security services, or to discuss your specific needs and challenges with our experts, contact us today.

CONTACT US

ABIresearch
THE TECH INTELLIGENCE EXPERTS™

Published July, 2023

157 Columbus Avenue
New York, NY 10023
Tel: +1 516-624-2500
www.abiresearch.com

ABOUT ABI RESEARCH

ABI Research is a global technology intelligence firm delivering actionable research and strategic guidance to technology leaders, innovators, and decision makers around the world. Our research focuses on the transformative technologies that are dramatically reshaping industries, economies, and workforces today. ABI Research's global team of analysts publish groundbreaking studies often years ahead of other technology advisory firms, empowering our clients to stay ahead of their markets and their competitors.

© 2023 ABI Research. Used by permission. Disclaimer: Permission granted to reference, reprint or reissue ABI products is expressly not an endorsement of any kind for any company, product, or strategy. ABI Research is an independent producer of market analysis and insight and this ABI Research product is the result of objective research by ABI Research staff at the time of data collection. ABI Research was not compensated in any way to produce this information and the opinions of ABI Research or its analysts on any subject are continually revised based on the most current data available. The information contained herein has been obtained from sources believed to be reliable. ABI Research disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.