otpbank PRIVATE BANKING

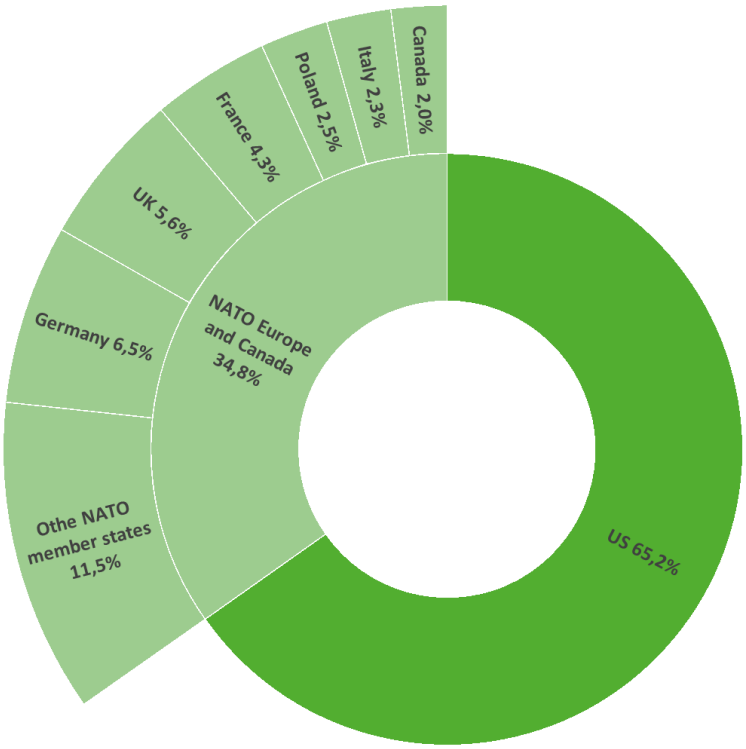
otp Global Markets

Market Snapshot

Since Donald Trump's election, US proposal of raising the level of defense spending required of NATO member states from the current 2% of GDP to 5%, has come up several times. As well as traditional defense spending this would also include infrastructure and cybersecurity spending. The latter could benefit significantly from the initiative, as it currently accounts for a very low proportion of defense spending. We have examined who the potential winners might be.

At the ongoing NATO summit in The Hague on 24–25 June, member states may decide to increase their defense spending targets to 5% of GDP by 2035. Although the initiative was proposed by the United States, most major European powers agree on its necessity, with only Spain yet to commit. The primary objective is to enhance Europe's defense capabilities, given that the continent currently accounts for only a third of NATO countries' defense spending.

Distribution of NATO defense spending among member countries (2024)



Source: NATO, OTP Multi-Asset Research

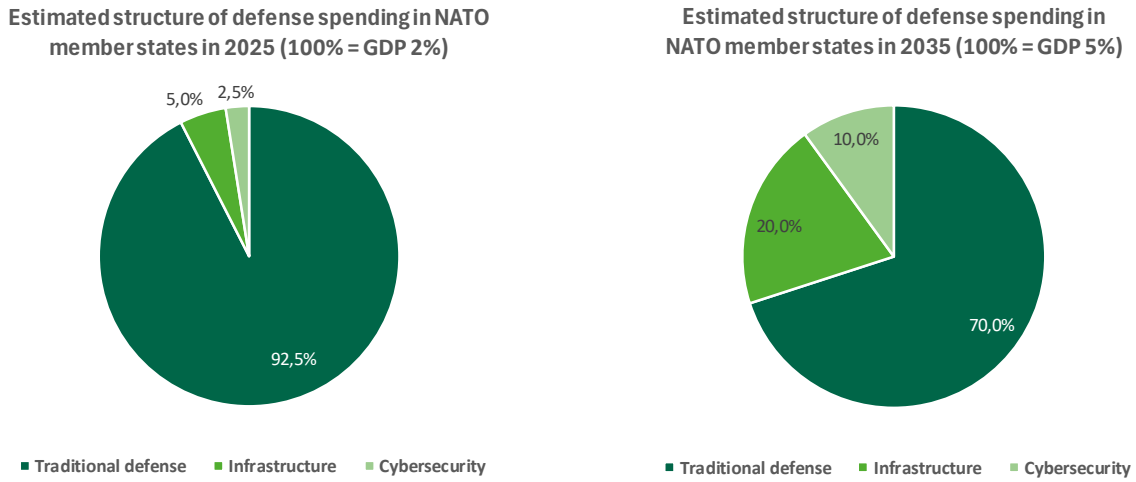
However, in addition to traditional defense, the new plan would expand the scope of defense spending. in preparation for hybrid warfare. Based on a proposal by NATO Secretary General Mark Rutte, 3.5% of GDP would be allocated for purely military purposes, with a further 1.5% earmarked for defense

infrastructure and cyber defense. Although the latter category is not yet finalized, it could be expanded to encompass broader security objectives, potentially including the space industry. While it is difficult to provide an accurate estimate of the expected level of government cyber defense spending, it is possible to outline the potential demand for the industry from government orders in the coming years.

Dynamic growth in cyber defense

Countries in the North Atlantic Alliance currently spend an average of 5% of their defense budgets on infrastructure development, although there are significant differences between countries. Thanks to its favourable geographical location, the US does not need to spend much on defense infrastructure in relative terms; these costs account for only 1.7% of its budget. By contrast, Estonia and Lithuania spend nearly 10%.

By contrast, the US government plans to spend $27.5 billion on cyber defense this year, accounting for just 2.6% of its total defense budget. In Germany, this figure is 2%. Based on the current cost structure, spending is divided roughly two-thirds to one-third between infrastructure and cyber defense. Together, these currently account for only 7.5% of total defense spending. However, according to the new draft, these two areas could account for 30% by 2035.



Source: OTP Multi-Asset Research

In this scenario, if the proposal were adopted in its current form, cybersecurity spending (accounting for 10% of the total defense budget) would amount to roughly 0.5% of GDP. Based on comments from the US, the deadline for achieving the targets could be 2035, although this date may be pushed back to make the requirement more acceptable and achievable for all European member states. Based on our calculations, this would equate to around $425 billion worth of government contracts for the cyber defense industry from NATO member states by 2035. Furthermore, the compound annual growth rate (CAGR) of

government cyber defense spending would approach 26.5% over the 10-year period from 2025. These estimates were made using the IMF's nominal GDP forecast.

Sensitivity analysis of the weight of cyber defense spending - NATO							
Cyber security expenditure as a percentage of GDP	0,25%	0,30%*	0,40%	**0,50%**	0,60%	0,70%	0,75%
Government cyber defense spending (USD billion)	212,4	254,9*	339,9	**424,9**	509,8	594,8	637,3
Government cyber defense spending CAGR until 2035	18,0%	20,2%*	23,7%	**26,5%**	28,8%	30,8%	31,7%

**in the worst-case scenario*

Source: OTP Multi-Asset Research

For comparison, Gartner's analysis puts the current total value of the global cyber defense market at around $212 billion. Analysts expect the industry to grow at a CAGR of around 13% over the next 5–7 years. We estimate that increasing cyber defense spending to 0.5% of GDP among NATO member states would grow the industry to around $1 trillion by 2035, resulting in a CAGR of 17% over the next ten years. In this scenario, the government revenue share within the sector, currently below 20%, could double by the middle of the next decade.

If 5% is not manageable by the countries

Even if the majority of member states do not accept an increase in defense spending to 5% of GDP, then, given the current geopolitical tensions, NATO could expect at least 3% of GDP by 2035. Assuming a similar distribution of defense spending, cyber defense spending by governments would account for 0.3% of GDP – still representing nearly $255 billion and a CAGR of 20.2%.

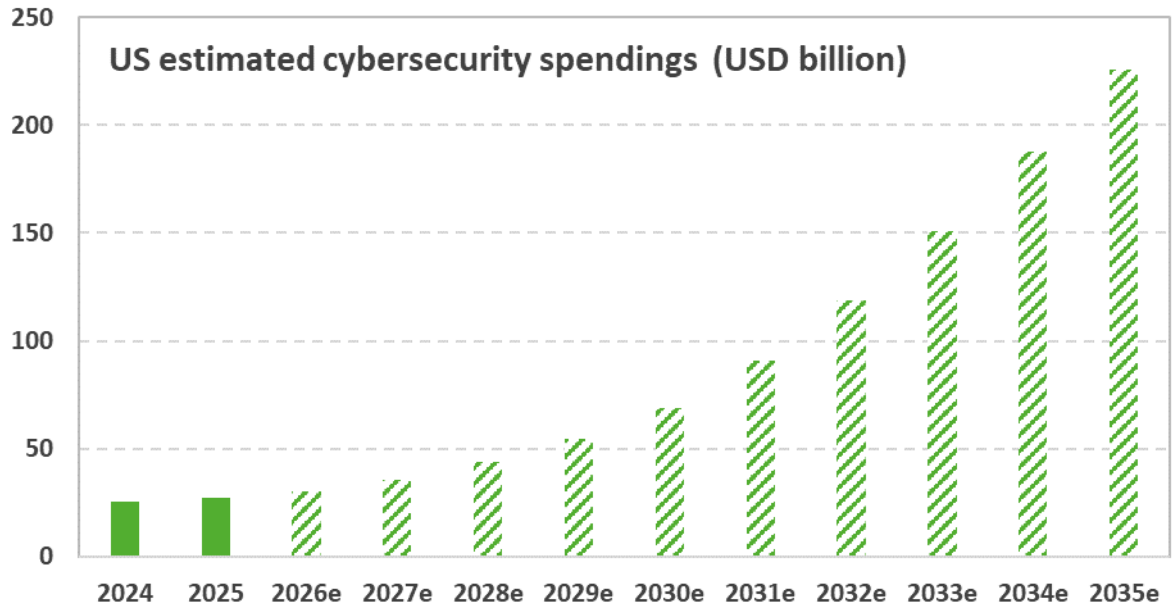
In this case, the industry's total size could grow to around $837 billion by 2035, achieving a CAGR of around 15%. However, it is important to note that this scenario reflects an extremely cautious approach. It only anticipates a modest increase in the GDP contribution of NATO member states and allows a relatively long period of ten years to achieve this. Nevertheless, even in this pessimistic scenario, it can be said that current market expectations for growth in the cyber defense market are overly conservative.

Who can benefit from this?

Given the strategic importance of cybersecurity, it is highly likely that NATO countries will prioritise suppliers within the alliance in this area. This practice indirectly strengthens Western technology and defense industry players through related government spending. As with traditional defense spending, the US plays a leading role in cyber defense within NATO, and this is expected to continue thanks to its significant economic clout. However, while military spending is close to 3.4% of GDP – just below the 3.5% target – cyber defense spending is less than 0.1% of GDP, indicating significant potential for growth.

By contrast, Europe lags far behind in terms of traditional defense, an area in which it is trying to catch up by announcing new arm race programmes. Consequently, the share prices of European defense companies have soared over the past year and a half. It is difficult to say whether the new NATO plan will cause a similar increase in share prices for US cyber defense companies. In any case, according to our

calculations, US government spending on cybersecurity could increase gradually from the current $27.5 billion to around $226 billion by 2035, representing significant potential for those operating in the sector.



Source: OTP Multi-Asset Research

The US government's cyber defense market has a major advantage over Europe's in that it is not fragmented. Due to the different cybersecurity needs and priorities of individual European countries, it is more difficult for a single company to obtain multiple government contracts, and these contracts may also be smaller in size than those in the United States. Furthermore, the industry is dominated by US companies that serve European customers as well, meaning they may receive European government orders too. Consequently, the lion's share of profits is expected to be generated overseas.

Beneficiaries could include companies that already have significant government contracts. One such company is Leidos, which provides US defense agencies with military IT infrastructure, AI-driven defense solutions and "Zero Trust" cyber security services. Booz Allen Hamilton, meanwhile, is a major supplier of defense algorithms and simulations to the US government and is leading the US 'AI for Defense' project. Palantir is also worth mentioning, as although it does not provide cyber defense services, it uses AI-based data analysis to assist with military decision-making and target identification – areas that are also strategically important for security. These companies already derive most of their revenue from government contracts.

Market Snapshot

Furthermore, companies that currently receive only a small proportion of government orders may also benefit, as they are likely to receive more as the defense budget increases. Examples of such companies include CrowdStrike, a provider of cloud-based and endpoint security solutions, and Palo Alto, a leader in the transition to the Zero Trust model.

Finally, it is worth mentioning that companies whose products or services are aligned with the government's development goals may also benefit from increased government spending on cybersecurity. They may win future orders, even if they are not currently awarded any. According to the Biden administration's goals, federal agencies must replace their cyber defense programmes with ones that can detect threats faster, provide automated responses to them and use AI tools. SentinelOne's Singularity platform aligns closely with this vision, as it automatically detects, investigates and responds to threats in real time using AI. With a market capitalization of only around USD 5–6 billion, potential government orders could provide the company with significant growth opportunities.

Leidos technical picture: From a technical and timing perspective, Leidos may be the most interesting of the companies mentioned. A reversal pattern may be forming on the chart. For a head-and-shoulders reversal pattern to form, it really needs to close above the 162.5 level. If this happens, significant upside potential would be opened up, with a target level of around 200. However, closing below the previous swing low of 140 could cause problems and could represent the risk management level.

otpbank PRIVATE BANKING

otp Global Markets

Market Snapshot

OTPMultiAsset published on TradingView.com, Jun 25, 2025 11:37 UTC+2

TradingView

otpbank PRIVATE BANKING

otp Global Markets

Market Snapshot

István Kecskeméti
Senior Analyst

Dávid Sándor
Chief Investment Strategist

Ádám Békési
Analyst

2025.06.25.