STAKES ARE HIGH

Dominik Birgelen *reveals why the defence sector needs to act now to plug the cyber security skills gap*

Cyber security skills shortage has become a pressing global issue, with the defence sector among the hardest hit. As warfare evolves in the digital space, defence organisations are under immense pressure to protect their systems against increasingly sophisticated attacks. The emergence of new attack vectors using adaptive AI and advanced technologies means that defence organisations are now facing an urgent need for skilled cyber security experts to safeguard mission-critical systems and sensitive data.

For defence organisations, the stakes are extremely high. A successful cyber security breach can cause significant damage to government and defence entities – compromising national security, disrupting military operations and exposing intelligence data to hostile actors. The need for trained professionals to combat an evolving cyber threat landscape is evident. However, despite the imminent threat posed to defence operations, the sector continues to struggle to attract, train and retain experienced cyber security professionals.

According to the BAE Systems Digital Intelligence 2022 report, defence organisations in the UK struggled to attract and retain talent, facing external obstacles such as the Great Resignation (38 percent), changes resulting from the COVID-19 pandemic (36 percent) and changes to working patterns (36 percent). Meanwhile, Statista highlights that the share of organisations experiencing a shortfall of skilled IT security employees stood at 85.8 percent in 2024.

A lack of cyber security professionals or upskilled staff can result in a higher likelihood of incurring a cyber attack

According to Statista, companies are unable to secure enough qualified staff due to an insufficient budget. Additionally, the lack of tech education is holding young people from pursuing a career in tech. According to BAE Systems' Digital Intelligence 2024 report, 42 percent of the British public believes a lack of IT and tech education throughout primary and secondary school has hindered a potential career in tech. Undoubtedly, this also impacts cyber security professionals in the defence sector.

This evident gap in skilled cyber security personnel poses a very serious threat to the defence industry, exposing businesses to an evolving and increasingly hazardous threat landscape, making the urgency for action even greater.

Several factors can contribute to persistent cyber security skills shortage, especially within the defence sector. The rapid digitalisation of defence operations and the rise of advanced threats have exceeded the availability of trained professionals leaving critical roles vacant in key areas like cloud security, artificial intelligence (AI) and machine learning. Lengthy background checks and security clearance processes have created further challenges in the recruitment process. Clearance protocols – while essential for national security – can often extend the time needed to onboard qualified candidates, causing delays in addressing critical positions.

The demanding nature of the role can also lead to burnout further impacting the retention of skilled cyber security personnel. Private sector opportunities can also create significant challenges by offering higher salaries, flexible work arrangements and better benefits that defence organisations might struggle to compete with. The evolving demands of the cyber threat landscape mean that new professionals need to be adept at understanding the

85.8% OF ORGANISATIONS EXPERIENCED A SHORTFALL OF SKILLED IT SECURITY STAFF IN 2024

cyber landscape and how to tackle emerging issues. A lack of skilled graduates further compounds this problem. According to Statista, security controls like endpoint, network and application implementation ranked among the biggest skill gaps among recent cyber security university graduates in both 2023 and 2024.

A lack of cyber security professionals or upskilled staff can result in a higher likelihood of incurring a cyber attack, which can cause disruptions to defence processes and compromise the security of pertinent national data. Defence companies handle vast amounts of sensitive military and defence data, making them lucrative targets for cyber terrorists. The global cost of cyber crime is expected to surge in the next four years, rising from £7.45-trillion in 2024 to £11.02-trillion by 2028. As cyber threats continue to grow in complexity and frequency, the defence sector must remain vigilant and proactive to safeguard critical military assets and information.

To effectively bridge the cyber security skills gap, defence organisations need to implement strategies that attract, retain and develop top talent. Building a resilient team requires a combination of proactive recruitment strategies, investment in education and developing key relationships with academic and private-sector bodies. Defence organisations must allocate sufficient resources to recruit professionals with a technical understanding of complex technologies, such as AI and machine learning.

Budgetary constraints and a decline in defence spending have further complicated this challenge. The UK allocated approximately £56.8-billion on defence between 2023 and 2024, which is a notable decrease compared with the £59-billion spent in the previous year. With constrained budgets, defence bodies need to maximise the impact of their resources effectively in order to maintain operational efficiency, while retaining essential cyber security talent. Streamlining the recruitment process, including security clearance

protocols, is also crucial to ensuring that capable cyber security professionals can be onboarded swiftly without compromising national security.

As cyber threats evolve rapidly, defence workforces must adapt to counteract increasingly sophisticated tactics like brute force attacks, social engineering and digital intrusions. These threats have the potential to cripple IT systems and compromise critical defence data. According to Reuters, in May 2024 the UK's Ministry of Defence suffered a significant breach of its payroll system, exposing the names and bank details of military personnel in the Royal Navy, Army and Royal Air Force.

CYBER SECURITY SKILLS SHORTAGE HAS VERY QUICKLY BECOME A PRESSING GLOBAL ISSUE

With cyber attacks becoming increasingly unpredictable and severe, defence organisations need to embrace a holistic approach, combining advanced technologies with skilled cyber security teams that are capable of monitoring, assessing and addressing threats before they develop. By prioritising these measures, defence bodies can strengthen their cyber security posture, safeguard sensitive information and ensure the continuity of critical operations.

While human expertise remains irreplaceable, technologies like AI can play a key role in empowering humans to address defence cyber security challenges. Advanced AI tools can automate threat detection, enabling faster incident response and identifying emerging risks that might otherwise go unnoticed. By streamlining processes, AI can help minimise damage during an attack and uncover potential risks by rapidly analysing vast amounts of data and identifying patterns that might indicate potential vulnerabilities. To maximise AI benefits, defence organisations must upskill workforces in interpreting AI-driven insights and utilising them to make strategic decisions.

To address the skills shortage effectively, defence organisations must adopt a multi-faceted approach. Investing in training and upskilling is critical. Defence organisations must develop specialised programmes and upskilling initiatives tailored to defence-specific cyber security challenges. This can help equip staff with the skills needed to tackle complex threats effectively. Collaborating with certification bodies can also help defence organisations safeguard their systems while meeting regulatory requirements and aligning with emerging guidelines. Fostering industry partnerships with technological bodies, universities and government agencies can also help defence bodies gain access to shared resources, training programmes and talent pools.

The cyber security skills gap is a pressing issue that demands immediate action, especially within the defence sector. Bridging the skills gap is not just about protecting systems, but also safeguarding national security and ensuring operational resilience for critical defence operations. As evolving cyber security attacks continue to threaten the safety and security of defence operations, businesses operating in the sector need to act quickly. By investing in training, leveraging AI and fostering collaboration across industries, defence organisations can build a robust cyber security workforce and ensure a safer and more secure future ●

DOMINIK BIRGELEN
is CEO of oneclick Group AG.

The rapid digitalisation of defence operations and the rise of advanced threats have exceeded the availability of trained professionals leaving critical roles vacant in key areas