Successful cyber attacks can compromise missions and reduce the ability of a military force to function effectively

Picture credit: US Dept Defense

# EVOLVING THREAT

**Dominik Birgelen** *reveals the importance of the Cloud to national defence*

**Cloud computing is an on-demand delivery of IT resources using an internet connection. In other words, instead of investing money in buying and maintaining the physical data centres and servers, organisations can enjoy the same services from a cloud provider based on their needs. This not only saves organisations money, but also a huge amount of time. In addition, cloud computing offers a wider operational and financial flexibility with a reduced requirement of maintenance and support. Therefore, cloud investment serves as a new way for organisations to moderate IT operational costs, deploy services faster and be responsive to the growing demands of the institution.**

The evolution of cloud technology was traditionally valued for its cost-saving abilities however, it is now invested in for its facilitation for future innovation. Cloud-based technologies also allow institutions to implement critical cybersecurity measures that prove extremely difficult to penetrate including shielded logins, disconnecting the end user environment and Zero Trust Architecture (ZTA).

Cloud technology has continued to establish itself across a number of verticals. As the technology has continued to evolve and become more complex, it has been increasingly utilised for its security capabilities. Just a few years ago, associating cloud technology with defence would have been unheard of, but now the technology has proven to be a secure and flexible resource for defence agencies.

Powered by the growing need for greater agility and scalable solutions to respond to an ever-evolving threat landscape, implementing a cloud infrastructure is meeting the needs for many defence organisations. The environment in which the defence sector operates must be in line with the space we live in. Defence organisations must be able to adapt to constantly changing technologies in order to keep up to date with the reality. Outdated and legacy IT systems need to be replaced with new technologies such as the cloud to achieve the objectives in a secure, cost-effective and timely manner.

Keeping in mind that defence agencies have a large responsibility of ensuring safety, security of the nation cannot be taken for granted. Cloud technologies are a secure place to start. According to a recent survey of 2,000 executives, 95 percent asserted their companies have a five-year cloud strategy in place whereas 89 percent considered implementing it as a competitive advantage.

In order to be able to deter the suspicious aggressors and gain a competitive edge in the battlefield, the defence organisations need to embrace the transformation. The transformation; from outdated to advanced technologies, from physical to virtual infrastructure and from on-premise technologies to cloud offerings.

Moreover, the national defence of the United Kingdom is already recognising the importance of the cloud. The Ministry of Defence in the UK – in common with the UK government as a whole – has adopted a 'cloud-first approach' under which purchases through the cloud are expected to be the first option considered by public sector buyers of IT products and services.

The shift to cloud storage allows defence intelligence analysts and professionals to zero in on potential suspects. This provides more speed and flexibility and aggregates more data, which boosts the possibility of identifying the difficult suspects to get to. The advanced cloud services also allow the exchange of information more easily from different overseas locations and are capable of powering specialist applications such as speech recognition.

According to the UK government, increased data sharing and exploitation across security classifications are supported by a multi cloud hosting environment. Which also enables mobile access to defence systems and rapid development and scaling of applications to meet increasing demands and possibilities.

There is no doubt that for defence agencies the priority is always to get the right information at the right time to predict and prevent any possible harm. In today's era there is an infinite amount of information available than ever before – thanks to growing technology, remote sensors, cybersecurity and surveillance.

The cloud with its offerings – such as scalability and processing power – can turn huge amounts of data into useful insights in a timely manner. The defence sector is leveraging significant agility, speed and cost benefits offered by cloud technologies. By leaving complex repetitive tasks to the cloud, the highly skilled IT staff can focus on performing activities, which provide more value.

What's more, defence organisations are involved in the management of critical supply chains such as the procurement of the defence equipment. The cloud in this aspect can provide a combination of mobility, analytics, and advanced sensor technologies, improving efficiency and security of the supply chain.

Defence organisations need to be better connected going beyond their separate systems to exchange information across the world. Cloud technologies can enable these organisations to shift beyond physical systems making them more secure and cost effective.

Defence companies, alongside their bespoke applications, are increasingly leveraging commercial off-the-shelf software (COTS) systems to better run their operations. Considering the fact that these technologies are cloud based, it becomes vital for defence organisations to move to cloud computing to access the latest versions of these technologies. To add more, cloud technology in itself saves companies a lot of money, however, utilising a serverless cloud can result in the drop of infrastructure costs on an average by as much as 70 to 80 percent.

CLOUD TECHNOLOGY HAS PROVEN TO BE A SECURE AND FLEXIBLE RESOURCE FOR DEFENCE AGENCIES

Development costs in the defence environment are mostly dominated by the tooling costs alone, which includes software development and system maintenance. Cloud-based technologies not only help reduce tooling time – but at the same time enable companies to reduce overall tooling costs. This is facilitated by saving prior configurations and by being integral to calibrating machine tools on the production floor.

The pandemic has made it clear that virtualisation of applications must be prioritised across the defence department including data centres with cloud-compatible infrastructure supporting applications. It is vital to consider the virtualisation of legacy applications most of which require costly maintenance.

There is no doubt that the UK government has recognised the need for "secure access" to the data regardless of the time and place. However, the factor has often been overlooked that human resources (HR) of the defence needs the cloud as much as any other department needs. Besides providing necessary infrastructure for the overseas missions, defence forces are also responsible for serving families that are stationed off-shore and veterans who are located in different parts of the world. HR management becomes more important when viewed from a wider perspective. Worldwide, the initiatives to centralise their HR functions are being taken by the defence forces who aim to transform their operations digitally in order to perform their duties in a secure way.

The centralised model can enable the defence sector to connect several HR initiatives and technology across the enterprise making the service delivery more secure, consistent and appropriate. All this can result in the effective management of interactions between end users and HR offerings such as workforce planning, payroll, pensions *etc*. Hence, by embracing a more human resources-centric approach of the cloud, defence can boost its operational excellence.

According to Google, Data sovereignty provides customers with a mechanism to prevent the data being accessed by the provider, approving access only for specific provider behaviours that customers consider necessary. According to data rules set by the UK

▶

government, defence players must practice sovereignty over data including ownership and accountability. To put it another way, defence organisations must; be aware of where the data is stored, how it is used, and set its policies regardless of who has custody of it.

There is a range of cloud providers who can enable data sovereignty by keeping the encryption keys outside the cloud, which provides customers with a power to control and decide who can access the data. One of the prominent examples of which is a recent cloud contract between UK spy agencies and a US tech company AWS (Amazon Web Services). The deal is expected to ignite concerns of data sovereignty because regardless of Amazon being a US company, the data will be held in the UK without giving access to Amazon to the information on the cloud platform.

## ADVANCED CLOUD SERVICES ALLOW A FAST EXCHANGE OF INFO FROM DIFFERENT LOCATIONS

Cloud technology can serve as a facilitator of the secure transformation of sensitive information across the world during missions between forces and allies. This can increase the effectiveness and ability to respond quickly. All in all, contributing to a wider perspective of data sovereignty.

The National Cyber Security Centre (NCSC) also advises on migrating to a ZTA through knowing your architecture, including users, devices and services. This is to ensure critical components are more isolated. Successful cyber attacks can compromise missions and reduce the ability of a military force to function effectively. Hence, implementing secure cloud-based defences are absolutely essential when defending systems networks against hostile actors with malicious motivations. Malware and phishing attacks exploit vulnerabilities on unpatched computers that are the common cause of data breaches.

It is here that a ZTA comes into its own. With a policy that questions every entry attempt, no actor who wants access to defence resources or services in the network is trusted from the outset. What's more, the state-of-the-art solution checks users each time they log in, but their trust status is continuously queried during the sessions. As soon as a slight red flag is reported, the granted access is automatically interrupted and revoked. A cloud-based system that authenticates all individuals, inside or out makes the optimum security solution for defence organisations.

Additionally, cloud offerings such as virtual desktop solutions enhance the security by moving data into a structured backend away from the end user. The centralisation of the data is crucial for consistent and undisrupted user experience. An integrated approach to the data tagging with identity and access management ensures that the data is closely controlled and properly identified. The cloud offering minimises the transmission of malware attacks by the virtue of a protected operating system at every login.

On the other hand, the cloud can also protect data during any crash in the device as the data is always stored in the backend. Defence agencies hold a lot of sensitive data – which they cannot afford to lose – the cloud in this sense helps them keep their data secure. Additionally, there is a number of regular security audits performed by cloud providers in order to make sure that crucial information is not put at risk.

On the whole, data is at the core of all defence operations. Such data needs to be secured with the best possible technologies so that defence institutions are prepared for the vagaries of the sector. Where powerful technologies like artificial intelligence and robotics are transforming the operations in the present era, the fact cannot be overlooked that outdated IT infrastructures are incapable of handling sheer volume of data. Cloud offerings on the other hand, are capable of much-needed scalability ●

**Dominik Birgelen** is the CEO and Co-Founder of virtual workspace provider, oneclick AG. Dominik is a serial entrepreneur. He currently wears several hats within oneclick such as overseeing sales, marketing and business development.

**A display showing real-time cyber attacks, including information on the attack's origin, type and target**

ATTACK TYPES

| | PORT | SERVICE TYPE |
|---|---|---|
| 14 | 25 | ○ smtp |
| 04 | 23 | ○ telnet |
| 74 | 8080 | ○ http-alt |

ATTACK TARGETS

| # | COUNTRY |
|---|---|
| 724 | United States |
| 351 | United Arab Emirates |
| 45 | Spain |

LIVE ATTACKS

| TIMESTAMP | ATTACKER | ATTACKER IP | ATTACKER GEO | TARGET GEO | ATT |
|---|---|---|---|---|---|
| 10:29:27.662 | American National Insurance Co | 50.200.102.48 | League City, US | De Kalb Junction... | https |
| 10:29:27.443 | Microsoft Corporation | 157.56.111.253 | Redmond, US | De Kalb Junction... | smtp |
| 10:29:27.219 | Chinanet Hubei Province Network | 116.211.0.90 | Wuhan, CN | Dubai, AE | http-al |

Picture credit: US Dept Defense