ISSN 1756-3240

February 2023

GMC

Linked in YouTube

Global Military COMMUNICATIONS

Defending against cyber threats

New horizons for defense

Digital backbone

Q&A Rivada Space Networks

Front cover photo courtesy of Bits And Splits/Shutterstock

SATELLITE Evolution Group

Global Military Communications is part of the Satellite Evolution Group portfolio

Camellia Chan, CEO and founder of X-PHY, a Flexxon brand

A digital backbone: how it strengthens and weakens national defence

Governments are engaged in an arms race against cybercriminals to implement measures which support the construction of a firm digital backbone. Underpinning this strategy is the effectiveness of Zero Trust models at all levels, working in tandem with advancements in AL and ML, and a change in approach about where they're deployed, to combat next-generation cyber challenges from individual and state actors.

Camellia Chan, CEO and founder of X-PHY, a Flexxon brand

For many of us, cybersecurity tends to be viewed at an individual level. We have antivirus software installed in our computers and frequently hear of people around us falling prey to cyber-attacks. Likewise, organisations use cybersecurity solutions to protect their most critical data, investing in technology and employee training to mitigate the repercussions should they be targeted by cyber criminals.

No different are the risks associated with data protection for national governments – and the geopolitical landscape is as volatile as it has been for decades. The war in Ukraine has placed the world on high alert, but other conflicts across the world are forcing nations to evaluate their defences to ensure they are better prepared for attacks of whatever form. This means defence strategies have in recent years evolved from the physical, to the digital.

Malware, DDoS, and the war in Ukraine

The Russian invasion of Ukraine has been a war on all fronts, with Russian incursions increasingly being supplemented with cyber-sabotage on Ukrainian digital infrastructure. It is a sophisticated and necessarily modern form of military crusade, where the arrival of military forces brings with it a wave of targeted cyberattacks intended to de-stabilise and threaten the region.

Of all methods, Distributed Denial of Service attacks (DDoS) have been a favourite Russian tactic even before the physical invasion took place. DDoS is a form of cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users. These types of attacks present a significant national security risk since they are most effective on high-profile web servers such as banks. In Ukraine, DDoS floods reached an all-time high during the first quarter of 2022, primarily targeting critical infrastructure facilities of Ukrainian enterprises.

But what is the real impact of this military strategy? By using a combination of cyber and missile strikes, the effective transportation of weapons and essential supplies can be heavily affected. According to research by Microsoft, of the roughly 50 Ukrainian organisations targeted by Russian malware since February 2022, 55 percent were critical infrastructure organisations. If anything, this illustrates the importance of a concerted effort by national governments to lay cybersecurity foundations in place.

The need to fortify the digital backbone

Ensuring that your digital infrastructure is bulletproof stands above the factionalism of day-to-day political life. The UK Ministry of Defence's digital strategy is an example of the critical need to consider digital capabilities, and more importantly identify any weaknesses. Among other things, the strategy explores the need for a 'digital backbone' to empower all future abilities in a structured and consistent manner.

In the US, the White House established the Cyber Safety Review Board, a panel of experts charged with examining hacking incidents that threaten US national security. In Singapore, a fourth branch of the military was inaugurated in October 2022. Named the Digital and Intelligence Service (DIS), its role is to combat digital threats on the cyber terrain.

A digital backbone has become an essential arm in the

Photo courtesy X-PHY

maintenance of national stability. It can both empower and weaken a nation's defence if not properly protected. So, as the character of digital competition and conflict has reached new heights, investments into the availability and protection of our most critical data is essential. Part of this involves using a holistic approach, ensuring that there is an equal level of attention to each digital security risk. If we fail to give proper duty of care to cybersecurity standards, for instance, critical investments in other parts of our digital infrastructure will be threatened.

Adopting a Zero Trust framework with the support of AI

Of the weaknesses facing individuals, organisations, and governments, the capacity for human error is the most significant. In 2022, World Economic Forum (WEF) research calculated that human error was responsible for 95 percent of cybersecurity issues globally, with individuals and organisations remaining one step behind increasingly sophisticated cyber criminals. So, to guarantee that you are covering all bases with cybersecurity standards, it would be practical to assume that criminal actors have already gained entry to your systems.

Adopting a Zero Trust framework is necessary, where internal and external users are continuously validated to ensure that suspicious activity can be flagged and acted on in real time. It has been defined by the WEF as a 'data-centric approach that continuously treats everything as an unknown'. For organisations and national governments with highly classified information, Zero Trust should be a non-negotiable arm of a cybersecurity arsenal. When combined with regular and updated training for employees on the risks associated with cyber-attacks, staff (who are vital to the protection of citizens) will be better educated in spotting suspicious activity when it happens.

Understandably, the potential for human error can never be fully eliminated. But with Artificial Intelligence (AI), the technology can spot irregularities and suspicious activity quicker than the human eye. Combined with self-learning capabilities in the form of Machine Learning (ML), AI can defend against many types of attacks.

There is also a strong case for bringing critical data back closer to a system's foundations. The use of cloud comes with many benefits, but it also creates a larger attackable surface for criminals to target. Even with the use of Zero Trust, AI and ML, there are so many variables that the technology will be working overtime to monitor for all types of threat signatures and patterns. With a modus operandi of focusing on a known ledger of threats, software defences struggle to accurately identify new forms of attacks.

As such, adding the defence to the more controllable physical layer allows for the AI to monitor a simple read and write pattern, enabling a far more accurate, reliable, and speedy response to incursions to the data storage level.

Lessons for defence at the digital frontier

As the defence sector reframes itself around Industry 4.0, an unprecedented battlefield has opened for cyber criminals. Whether acting at an individual or institutional level, cybersecurity risk continues to evolve and diversify. We are seeing a wave of global initiatives intended to combat this risk in the wake of its application to geopolitical conflicts, but are they enough? **GMC**

Photo courtesy Bits And Splits/Shutterstock