C-130 Hercules supplying mission critical humanitarian missions. Photo courtesy Marshall Aerospace

# The new homefront - how military and security providers are defending against COVID-19

The fight against COVID-19 has been a war of its own, with very real sacrifices and hardships. Unlike the wars we have known, this conflict is one we all fight, in our own mundane little ways, and the role of businesses in that struggle is a considerable one. It's time we recognised the actions of those corporations who have fought to keep us safe.

*Laurence Russell, News & Social Editor, Global Military Communications*

**During the great wars, there was a simple expression in Britain that went "I'm doing my bit."**

It was a sentiment that quietly acknowledged the then seemingly impossible challenge of bringing peace to Europe and maintaining the sovereignty of its nations. A titanic effort for which every citizen, civilian and soldier held some small personal responsibility which they hoped would be added together to be enough to turn the tide. In the midst of one of history's most notable pandemics, we are reminded of that culture once again, in which every household must understand that doing the right thing in fighting overwhelming odds is not something that one can wait for others to shoulder, but rather a monumental shared burden. While individual efforts have an impact, there have been larger contributions made by the businesses around us. Across the world, we have seen the most responsible of our captains of industry recognising the need to leverage their resources for the greater good in a time of true crisis.

**Marshall Aerospace fights pandemic by ensuring supply availability and resilience**

In the UK, Marshall Aerospace and Defence Group have been working to maintain their C-130 Hercules transport aircraft fleets worldwide. The craft is known as a go-to platform for humanitarian missions, which have been rapidly prioritised as the COVID-19 pandemic grew in severity, including medevac repatriation missions and remote supply deployment.

At a time when transport and infrastructure have been so deprived that it has ground to a halt in certain regions, sophisticated humanitarian action is of the utmost importance. In times of crisis, it falls to charitable NGOs and conscientious militaries to confront the catastrophe and defend populations, which Marshall has been eager to assist with.

Chief Executive Officer Alistair McPhee explained: "We are always incredibly proud of the work that we do to protect people in critical situations and that has never been more relevant than right now. Armed forces are being called upon to support the capacity needs of health services across the globe. So, it is vitally important that we are able to stand ready to help in whatever capacity we can over the weeks and months ahead and I really want to take this opportunity to pay tribute to the team, in particular our frontline employees, who are doing an amazing job in very difficult circumstances to make sure we don't and won't let our customers down."

Marshall Aerospace and Defence Group have also been involved in supporting a taskforce of UK experts in developing and manufacturing the exovent, a type of non-invasive iron lung ventilator which safely aids respiration without compression of the chest.

The task force's leading clinician Dr Malcolm Coulthard said: "The team has been working flat out for days. We started out looking at negative pressure ventilator technology thinking that it would allow us to produce literally thousands of ventilators very quickly and cheaply to cope with the tsunami of people with pneumonia that may be upon us because of the Covid-19

virus. However, as soon as we looked into the science and the literature it immediately became apparent that this will allow us to produce less-invasive devices than the conventional units in current use, possibly better for patients' hearts, at a fraction of the price, using off-the-shelf parts."

While not all alternative ventilators boasted about in global news have shown favourable results, exovent continues to deliver on its promises, providing much-needed support to the critically strained NHS by addressing the ventilator shortage.

## Marlink provides telemedicine equipment, fuelling further development

The pandemic has also motivated a surge in telemedicine technology. In the face of such a virulent global disaster, research and development of telemedicine technologies have rapidly increased. Allowing healthcare professionals to diagnose and treat from a remote location offers an ideal solution, not least because of rampant shortages of personal protective equipment (PPE).

As part of their #StrongerTogether initiative, Marlink had equipped the French Service d'Aide Médicale Ugente (SAMU) with its XChange Telemed healthcare diagnosis kits allowing medical teams to establish remote medical stations in rural environments, allowing for virtual treatment without the need to create a transmission vector.

This also allows SAMU to better measure the pandemic outside of urban centres by allowing responders to connect to remote stations around the country. Marlink is also able to supply blood pressure analysers and oximeters with the kit to give doctors more tools for diagnosis.

Tore Morten Olsen, President or Maritime at Marlink explained: "As the Coronavirus outbreak continues to cause serious health impacts and business disruption globally, XChange Telemed is helping to reduce risks through early detection and faster treatment."

With necessity likely to nurture further research into telemedicine technologies, presently available products such as the XChange Telemed kit acutely demonstrate the remarkable advantages to remote diagnosis and treatment.

## Telenor offers a lifeline to struggling global infrastructure

The continued availability of lifesaving products is invaluable to holding the world together in this era of catastrophe, however some companies have exhibited an even greater degree of heroism.

One of the most startling responses to the pandemic has been that of Telenor, a telecommunications company with

*XChange Telemed kits supplied to French emergency medical response. Photo courtesy Marlink*

*Inmarsat and Cobham Emergency PTT*

expertise in network security. Telenor aids the Norwegian Armed Forces Cyber Defence division by sharing expertise and resources to better strengthen digital security to best protect and safeguard the operation of critical infrastructure, national security, and emergency preparedness.

The company has gone above and beyond in its contribution to initiatives to aid the fight against COVID-19. As business, education, and healthcare face terrifying new realities, Telenor has stepped in to invest 15 percent of its revenue into infrastructure and network stability, while offering mobility data to health authorities to aid their prediction and prevention of the contagion and providing online education and network security resources.

Sigve Brekke, President & CEO of Telenor Group stated: "As the pandemic spreads, it's now crucial to keep reliable network and services running. Everyone at Telenor takes this responsibility very seriously, and we are committed to keeping societies and the world connected. However, our social responsibility also goes beyond this. ... At these times, we all need to work together, and Telenor is ready to contribute where we can."

As cybercrime soars with the confusion of worldwide lockdowns and deprived communities begin to crumble under the strain of economic hardship, Telenor distinguishes itself as a shining example of how an organisation ought to respond to the tragedies left by global devastation.

## Sustainable corporations in their finest hour, holding the world together in its time of need

It is our responsibility as members of a civilised society to take action to sustain the systems that keep our world turning, a responsibility which falls in no small part to businesses. The pandemic has shown us which companies are prepared to leverage their resources for the greater good, often in the face of certain economic sacrifices on their part.

When the world returns to business as usual, we should not forget which of these businesses have proved themselves as truly dedicated to the sustainability and safety of their customers.

The war on COVID-19 has been a true call to action for all of us, and though a very unconventional conflict, the battles that have been fought to reclaim our nations as we knew them have inspired examples of remarkable bravery, worthy of being remembered. **GMC**

# The biggest threat to your communications? Your own applications

Cybersecurity is an ever-growing threat across all walks of digital life, for consumers, businesses, government and military alike. What often comes as a surprise is that the biggest threat to organisations could come from the applications their employees deploy.

*Francois Rodriguez, Chief Growth Officer, Adeya*

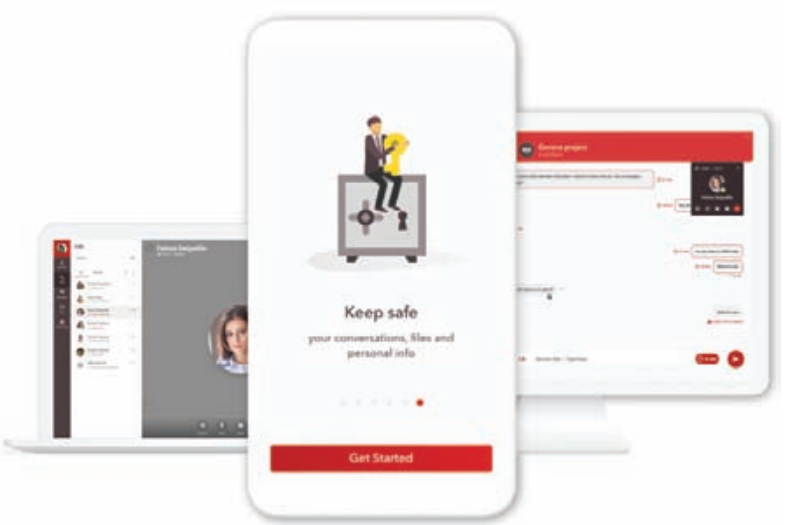
**Most people think of cybersecurity as an external issue.** That the focus is on keeping hackers (whether criminals, hacktivists or foreign governments) out of sensitive data and mission critical applications.

Yet so often the real threat lurks within. Even before the coronavirus pandemic, the issue of Shadow IT, where technology is procured and deployed outside of corporate IT oversight and processes, was a major issue for organisations in all sectors. How much of an issue? Some analysts put it at accounting for anywhere between 30 and 50 percent of IT spend in enterprises.

As organisations wrestle with the impact of COVID-19, the issue of Shadow IT is adding additional complexity to their efforts to secure their newly decentralised workforces – one study found that nearly half (47 percent) of IT security professionals felt that home workers using shadow IT solutions represented a major problem.

## Identifying the threat

As highlighted, Shadow IT is the use of applications and services for work that have been acquired without using corporate IT. In the past, that might have been putting public clouds on credit cards to acquire compute resource quickly for development projects, or, more simply, using a messaging tool such as WhatsApp to communicate with teams.




*All photo courtesy of Adeya*

For those in the public sector, operating in sometimes stricter budget environments than their private sector counterparts, this could be a major challenge when faced with balancing the need to work with cost concerns.

Now, the threat has been compounded by the need for organisations across all industries, under prepared for mass remote working, to keep operating outside of the office. To that end, there has been the rapid deployment of free or freemium communication tools, with the likes of Zoom becoming a major trend and feature in lock-down life. While it may be fine for keeping in touch with friends and families, the fact of the matter is that these apps simply do not have the enterprise-level data privacy and security organisations require. Anyone looking for evidence only has to look at the security issues Zoom itself has faced as its popularity has exploded.

## Why all businesses need military-grade encryption

For private sector businesses, this lax approach to security can have significant financial repercussions – for government organisations, whether in the military, healthcare or public administration, the consequences could go so far as to threaten lives. That is why all organisations handling sensitive or mission critical data should be deploying military-grade encryption.

It is evident that bad actors are seeking to capitalise on the chaos and confusion of the pandemic – the World Health Organization (WHO) has reported a five-fold increase on cyber-attacks targeting its staff and infrastructure, while Interpol has also highlighted how criminals are going after hospitals and other health providers with ransomware.

As such, it is critical that organisations have the ability to protect their data, devices, and applications. These break down into two areas – behavioural and technological.

The former is really a matter of education – making sure that employees understand what they need to be vigilant of, and how everyone is responsible for an organisation's cybersecurity. Just as they would not give out their physical credentials to allow a stranger into their place of work, so they should be applying the same rigour and consideration when it comes to their digital activities. That covers an understanding of social engineering and how to combat it (including not clicking on links and interrogating sources of emails and messages, particularly ones claiming too-go-to-be-true news and offers), to having better passwords, not using shortcuts and thinking about why the tools they want to use may not be officially sanctioned.

From a technology perspective, as with any procurement process, it is really about using the right tools for the job. The reason Shadow IT is such an issue is that the applications being used do not have the same policies, approaches and

requirements that enterprise-grade services do. Even when they claim to have the right features on offer, such as end-to-end encryption, it quickly becomes apparent that is not always the case when interrogated. Those that claim to have that level of protection often have a small window where data, rather than staying encrypted from device to device, is decrypted on a server before being re-protected and sent on to the receiving endpoint.

It is a small window, but enough for an attacker to get in and cause havoc. As discussed previously, for a private sector organisation, that could result in a significant business impact; for a public sector function, it could be worse.

That is why, when considering tools, it is important to only choose those that meet the stringent requirements an organisation has. For end-to-end encryption, that means military-grade, with cryptography support that can be tailored to specific demands, in-built obfuscation to prevent the reverse engineering of code, public key generation and trusted identity as standard. These are all elements designed to frustrate attacks without compromising an organisation's ability to continue operating.

## Countering an ever-present threat with sophisticated technology

Threats are everywhere, and the current confusion and chaos is perfect cover to cause significant damage to enterprises and institutions across all sectors. All organisations, no matter how small or how unsensitive they think their data is, have a responsibility to their customers, employees and other stakeholders to take the necessary steps to secure both themselves and their systems.

That means aligning the need to keep working with security requirements, and choosing tools that enable that, compromising on neither. It's the deployment of the appropriate resources, with security at the fore, rather than the ones that are easiest to get hold of.

**GMC**