FRONTIER TECH INVESTOR

The 5G Warrior

ARCHIVED

Important risk warnings: Before investing you should consider carefully the risks involved, including those described below. If you have any doubt as to suitability or taxation implications, seek independent financial advice.

General - Your capital is at risk when you invest in shares, never risk more than you can afford to lose. Past performance and forecasts are not reliable indicators of future results. There is no guarantee dividends will be paid. Bid/offer spreads, commissions, fees and other charges can reduce returns from investments.

Small cap shares - Shares recommended may be small company shares. These can be relatively illiquid meaning they are hard to trade and can have a large bid/offer spread. If you need to sell soon after you bought, you might get back less that you paid. This makes them riskier than other investments. Small companies may not pay a dividend.

Overseas shares - Some recommendations may be denominated in a currency other than sterling. The return from these may increase or decrease as a result of currency fluctuations. Any dividends will be taxed at source in the country of issue.

Taxation - Profits from share dealing are a form of capital gain and subject to taxation. Tax treatment depends on individual circumstances and may be subject to change in the future. Figures quoted in this promotion do not take dealing costs or taxation into account.

Investment Director: Sam Volkering and Eoin Treacy. Editors or contributors may have an interest in shares recommended. Full details of our complaints procedure and terms and conditions can be found on our website: www.southbankresearch.com.

Editors or contributors may have an interest in shares recommended. Full details of our complaints procedure and terms and conditions can be found on our website: www.southbankresearch.com.

Frontier Tech Investor is issued by Southbank Investment Research Limited. Registered in England and Wales No 9539630. VAT No GB629 7287 94.

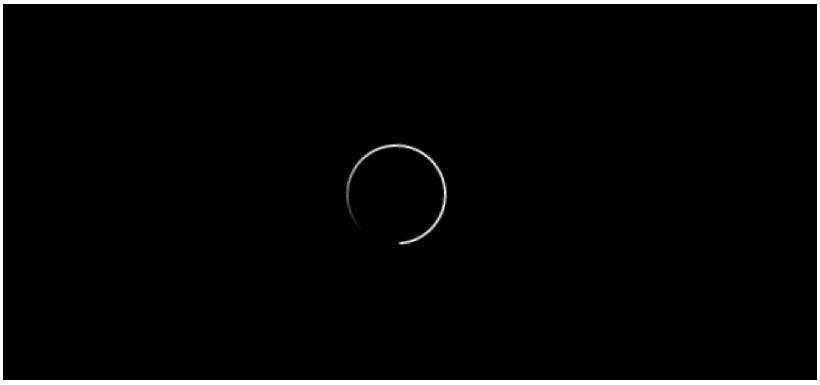
Registered Office: 2nd floor, Crowne House, 56/58 Southwark Street, London SE1 1UN. Southbank Investment Research Limited is authorised and regulated by the Financial Conduct Authority. FCA No 706697. https://register.fca.org.uk/.

© 2020 Southbank Investment Research Ltd.

...continued on next page...

Stock Alert: this 5G "warrior stock" could soar in 2020

I'm going to show you a simple picture. I want you to guess what it is.



Source: How-To Geek

I told you it was a simple picture.

So, do you know what it is? Maybe during lockdown you've seen this more frequently than you'd like?

I know I've seen it more in the last couple of months than I care to remember.

If you don't know what it is, I'll help you out. It's the "buffering" image you see when your streaming service is trying to connect to the streaming service databases.

Of course, when you see it on your streaming service, it's not a static image – that little self-chasing circle just spins around, and around, and around… and around. It's annoyingly endless as you wait what feels like forever for the streaming site to connect.

And different applications have different images. It might be circulating dots, that long line, sometimes a colourful spinning wheel like Apple has. It comes in various forms and guises. But it all means one thing…

You aren't connected and you can't access the services that you want to.

It's highly frustrating. And a more common occurrence during lockdown as the nation's connectivity infrastructure was placed under increasing strain as millions were forced to work from home. In rural areas in particular it's been found that productivity has worsened as "hours" have been added to work days because of slow speeds.

…continued on next page…

We've built a society where our reliance on the connected world has never been greater.

When you're trying to get around town these days and you want to grab a taxi, how often are you just hailing one on the street? Or are you using an app like Uber, Gett, or a minicab-specific app where you can order and pay online now?

When it's time for a takeaway meal, what is the first thing you do? Head to the kitchen drawer for the local menu that found its way through the letter box? Or on to Just Eat, Uber Eats or Deliveroo to grab those pizzas or Chinese through the app?

And the movie you want to watch. Where's that coming from? It isn't Blockbuster. And it isn't the local DVD store. Not any more. It's from Netflix, Prime, Disney+, Apple TV+ or Google Movies – or one of the huge number of movie streaming services.

When you want to keep abreast of the latest daily updates or information in real time, what do you look to? Facebook? Instagram? Twitter? Or perhaps one of the "news" websites or native apps to get your dosage of what they want you to know about what's going on.

What happens when you can't get access? What would you do if you were effectively cut off from the digital world? You've no doubt heard of computer rage. Well what about streaming rage? App rage? Buffering rage?

These things are all relatively superficial "surface level" examples of the kinds of applications we use and rely on day to day. But the world we live in is increasingly in the "cloud".

The cloud, of course, isn't the big white fluffy bundles of particles in the sky. The cloud as we know it is data accessible at all times via connected, often wireless networks. But the reality is the cloud is just data on a database in a data centre that's asked for, retrieved and delivered at any given time to a user.

Those Netflix movies aren't in your TV. They're in a data centre. Your Zoom call is pulling data from data centres and delivering it at light speed around the world. Your Facebook data, your Google data, your Box data, Dropbox data – it's all in a database somewhere.

Hence you have to ask yourself, with such reliance on a connected, cloud-based, wireless data-heavy world, what happens when we can't access it? What happens when a company can't deliver its service to you when you need it?

The damage that can be done is almost unquantifiable. You might only be unable to access your data for a day but the cost to the business you're using is massive. That's because while you might be impacted, there's a good chance millions of others around the world are impacted too.

...continued on next page...

That's a cost to the business because of this downtime. A cost to their reputation, sales, future sales, profits, maybe stock price even. It's also a cost to economies as productivity drops by those affected. Lost working hours, sales and profits to the businesses that are also suffering from the inability to access the data they need when they need it.

The point is that the world is only heading one way with the creation, consumption and distribution of data – up. And we're only going to be able to create it, store it, send it and consume more of it faster and faster as the years tick by.

This will be driven by ever more complex and sophisticated devices as well as hyper-connected wireless networks, a lot of which will be driven by 5G technology for the next decade, 6G technology after that, 7G technology after that and so on.

Now this opens up a massive financial opportunity in itself. Hyper-connected networks and richer, faster, more effective data and information is an economic boom in itself. And like we saw with the explosion of 3G and 4G, there's the potential to create all-new industry, to create new efficiencies and effectiveness of existing industry and to generate economic development with each communications leap forward.

But while the next generation, 5G, holds incredible promise and in my view will deliver exhilarating returns for investors, we also need to understand the immense risks that 5G is going to bring.

Rise of the printer and baby monitor

Dyn is a domain name service (DNS) operator. And in 2016 Dyn suffered a massive distributed denial of service (DDoS) attack.

If you're unfamiliar with a DDoS attack, it's a malicious cyber-attack which floods a website or online service with traffic requests. A good way to think about it is if you've got ten people trying to get through a hallway, you can all move relatively freely through it – there's no real hold-up with that level of traffic. But if you had 100,000 people trying to all get through that same hallway at once, everyone would get stuck and not be able to go anywhere.

This is what a DDoS attack aims to achieve. By sending fake requests to a site or service, it overloads the site/service to a point that normal, regular users trying to get access can't. And when we talk about a flood, we should probably say a tsunami of traffic.

The 2016 Dyn DDoS attack is rumoured to have been in the magnitude of 1.2 terabits per second albeit, Dyn was unable to verify that figure. 1.2 Tbps is astronomically high.

...continued on next page...

As a point of comparison, a service provider like BT has speeds of 67 megabits per second. 1.2 Tbps is roughly 1.2 million Mbps – almost 18,000 times faster than your home service.

Dyn noted that compared to usual traffic the attack was in the vicinity of 40 to 50 times higher than usual. What made this particular attack quite scary is that it originated from around 150,000 Internet of Things (IoT) devices that had been compromised by the Mirai botnet.

The sorts of devices the botnet infected included video cameras, smart TVs, radios, printers and according to Cloudflare, "even baby monitors". This attack disrupted services like Airbnb, Netflix Amazon, The New York Times, PayPal, Soundcloud and Twitter. These services were unavailable for extended periods of time, because of this DDoS attack.

Think about that. Baby monitors taking down Amazon. This clearly made some of these big tech firms sit up. Even as recently as this February, Amazon noted an attack on its AWS platform that was in the vicinity of 2.3 Tbps.

These attacks are only going to get bigger, faster and potentially more devastating to businesses that aren't prepared for it.

And this is the kind of reality that online organisations, applications and services are faced with *now*.

When we step full force into this next decade of 5G hyper-connectivity, that threat potential rises exponentially in line with the rise in connectivity and the proliferation of IoT devices.

Hence DDoS protection and managing the risks that come with a hyper-connected world is perhaps one of the most (if not the most) important aspect of 5G that no one is really paying any significant attention to… yet.

But I believe that's going to change when the next major attack occurs. An attack that will be along 5G networks, that will be several times larger and more disruptive to our online world than the Mirai botnet DDoS attack on Dyn ever was.

According to a blog post by cybersecurity firm Corero,

> *5G will make it even easier for hackers to launch ever larger volumetric attacks, and we may witness the first 10 terabits per second attacks sometime in the not too distant future. In the meantime, the increased bandwidth of 5G networks means that future botnets will not need to harness as many mobile or IoT devices, to have the same crippling effects on their targets.*

10 Tbps – that's the kind of threat that's facing organisations in a 5G-connected world. On top of this, the International Data Corporation estimates there will

be around 41.6 billion IoT devices by 2025 generating a staggering 79.4 ZB (zettabytes) of data.

This is what a hyper-connected, always online, autonomous, "smart" world looks like under the hood. And if the right protection measures aren't taken into account, then we may all be at the mercy of those who wish to tear it all down.

Introducing your *Frontier Tech Investor* bonus 5G recommendation…

While that might seem like a bleak picture, there is an upside to all of this.

Yes, there are real threats that you need to understand in a 5G-connected world. But the good news is that forward-thinking companies are aware of the real risks that 5G brings and are putting measures in place to protect our connected world from these threats.

These are the gatekeepers, the defenders of our hyper-connected world. And while these leaps in connectivity aren't possible without the hardware that delivers them, it's also not possible without the companies to protect them.

In 2019 A10 Networks undertook a survey of the mobile industry where 63% of respondents said that when it comes to the most important security advances and capabilities for the future in a 5G world, advanced DDoS protection to address larger and more sophisticated attacks was a top priority.

This tells us that companies are aware more than ever of the threat facing their online businesses. And they're looking to the *5G defenders* to ensure they've got the best, most capable fortress around them to keep out the enemy.

Which is why your bonus 5G recommendation is **Corero Network Security plc (LSE:CNS).**

Corero Network Security (Corero) is a cyber defence company with a speciality in DDoS attack prevention "on-premises and in the cloud".

Corero is listed on the London Stock Exchange as part of the AIM sub-market. It has a current stock price of 4.96p with an approximate market cap of £26.5 million.

Its flagship product, "SmartWall", is an autonomous DDoS platform that can detect a threat in seconds, to mitigate it and ensure that a business can continue to maintain operations, even through an attack.

In March this year Corero released its yearly DDoS trends report. The company noted in the introduction that,

...continued on next page...

> *Our increasingly Internet-connected world grows more complex every year, due to faster connections, the widespread adoption of Internet of Things (IoT) devices, and the explosion of cloud services. Simultaneously, Distributed Denial of Service (DDoS) threats have become more sophisticated, more frequent, and larger.*

It continues,

> *DDoS attacks are considered one of the most serious threats to business continuity. Downtime, or increased latency, can significantly impact brand reputation, customer trust and revenue. Plus, within Europe, the introduction of the GDPR and NIS legislation has significantly increased the risk of punitive fines.*

And even though the really big attacks are now shifting into the Tbps ranges, the more common and regular DDoS attacks are actually far smaller, and shorter, but can still be potentially as damaging.

Corero found that,

> *… the continuing trend is that the average volume of attacks is increasing. In January of 2019 there was a report of a DDoS SYN attack which resulted in an overwhelming deluge of 500 million packets per second. Having said that, lower-volume, short attacks continue to dominate, with 98% occurring at less than 10Gbps and 85% lasting less than 10 minutes.*

SmartWall runs as an always on real-time monitoring service. That means it can detect incoming threats or attacks in seconds and provide instant analysis on the traffic, enabling protection to run and allowing usual traffic while deterring the threat and logging and recording the threats to build a database of intelligence for future or ongoing threats.

It's almost like a 24/7, 365 patrolling army of digital knights at the gates of the city instantly repelling threats while letting the innocents through. And once they've fought off the attack, they lock them up so when the same attackers come again they'll know even faster next time what to expect.

Corero isn't just a potential leader in DDoS protection either. It's already rolling out its offering with businesses all over the world and with big technology partners like the US$7 billion networking giant Juniper Networks (NYSE:JNPR).

In late 2018 Corero and Juniper entered a global partnership agreement where Juniper would integrate Corero's SmartWall protection into its MX Series 5G Universal Routing Platform.

At the time, Juniper Networks explained,

> *"Providers are facing the challenge of securing increasingly complex*

...continued on next page...

> *and exponentially faster networks. By leveraging Corero's SmartWall DDoS detection and mitigation technology to automatically control Juniper's SDN-enabled MX Series, we are able to offer an integrated solution that protects the Provider Edge against the increasing risk posed by DDoS attacks. Juniper's expanded relationship with Corero provides our customers with additional security options to make the self-driving network a reality."*

I anticipate that in the aftermath of the 2020 global Covid-19 crisis there will be an ever increasing demand for online and cloud services. And that as we move into a 5G world, the need to protect those services will be paramount.

Within that I see Corero being a significant player in the space for DDoS protection and its ongoing partnership with Juniper Networks to assist in the rollout of SmartWall services to new customers, taking the company forward in a post-Covid-19 world.

Financials and risks

For the full year 2019 Corero reported group revenues of $9.7 million of which over 60% was reoccurring revenues. That's a good sign as it lays a strong platform for the business to build on its new customer base as well the underlying health of its cash flows.

Still, the company reported a $6.6 million loss for the year. Yet it's not an immediate concern. And we would expect that in 2020 the full-year results aren't at the same level of 2019. But in 2021 I am expecting the company to take a strong step forward towards a financially sound business.

The good news is also that at the end of 2019 it had received further investment from Juniper to the tune of $1.4 million and had net cash of $5.4 million. So it was in a strong position leading into the 2020 crisis and appears to have come through it relatively unscathed.

CEO (at the time) Ashley Stephenson said of the results,

> *"Whilst the current macroeconomic climate is impacted as a result of COVID-19, we remain confident in the long term resilience of our business, the importance of our SmartWall solutions across our key telecommunication and cloud provider markets, and our ability to support our global customer base during what is a challenging period for everyone."*

Now I say "at the time" because Stephenson is moving to the chief technology officer role on 1 July and incoming CEO Lionel Chmilewsky will be taking the CEO reins in his place. Again, we see this as a good sign, as the company looks to expand its customer base and drive growth.

...continued on next page...

So far in 2020 the company has also announced contract wins of $1 million, $2 million and another $1.5 million in just the first six months of the year. This ranges from telco and network service providers in the US and Europe to internet and mobile providers here in the UK. All wins signing up for the SmartWall DDoS protection in its different forms.

But while the company looks to growth and new opportunities, you need to also consider the risks involved before looking to invest.

For a start, the company runs a loss. All the contracts in the world won't make up for a perpetual loss-making enterprise. We would expect to see in the next 18 months a move towards profitability. Even if losses are still incoming, a reduction in losses, growth in revenues and the indication it will be able to deliver profit to shareholders is something we want to see.

It is cashed up and has investment from Juniper. But the risk of future capital raises, which could dilute holdings, is a real possibility. I don't expect one soon, but should it need access to capital, as it has before, it may be on the cards.

There's also the need to continue to be a market leader and have best-in-class technology offerings for its customers. It needs to stay ahead of the DDoS game to ensure its services perform as expected.

Hence there's great technology risk here. If SmartWall isn't able to deliver the expected defence and outcomes its customers need, it would be a significant blow to the company. Or should a competitor be able to deliver better, more advanced and cost-competitive solutions, that would make it increasingly difficult for the company to operate and bring in new customers with contract wins.

It is still a relatively small company, and there's also general market risk. Should we see another crisis unfold off the back of this Covid-19 crisis and markets take another big hit, Corero's stock wouldn't be immune to further falls.

We saw this in March when the stock saw significant price falls in line with the wider markets. Also worth noting is that over the last year the stock has been highly volatile ranging from as low as 2.35p and as high as 7.47p.

I think the trend for the stock is higher and that it can start to gather momentum into the second half of 2020 and into 2021, delivering great potential for shareholders. But expect there to be volatility along the way.

Action to take

Corero Network Security plc (LSE:CNS) trades on the London Stock Exchange as part of the AIM sub-market with a current market cap of around £26.5 million and a stock price of 4.96p.

...continued on next page...

Trading volumes are around 70,000 per day on average which makes this an illiquid stock. That means once we release this recommendation there may be a bit of a buying frenzy in the market at the open the next day.

We set a buy-up-to limit to ensure you don't overpay for the stock and get caught up in any bidding wars. Likewise if the stock does trade over our recommended buy-up-to price we suggest applying some patience to wait for it to settle back under the buy-up-to which often happens with illiquid stocks.

It also means that exiting a position may be more difficult in the market due to the reduced volumes. However, this is a long-term play in a company that's deploying protection for a hyper-connected world with an increasing threat of DDoS attack.

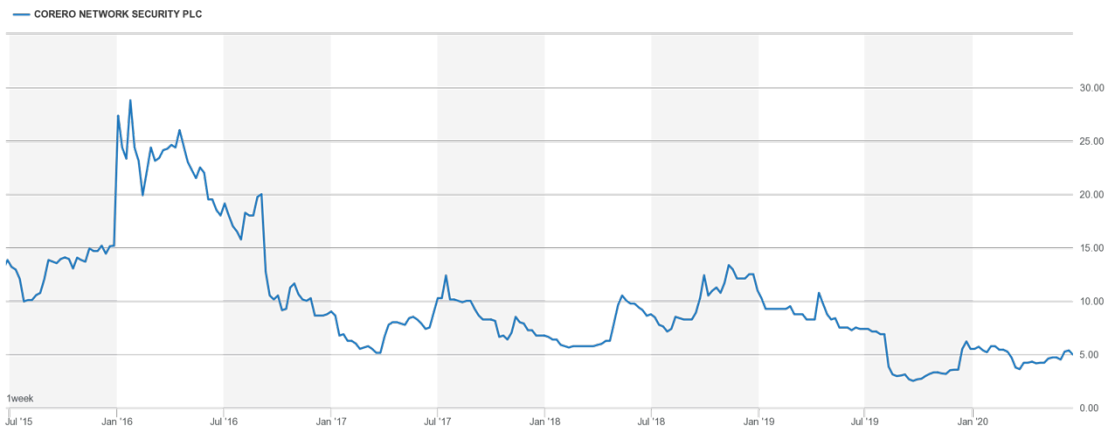
I think that makes the company one of the most underrated and, yes, important companies in the UK markets today and a perfect way to play the incoming 5G mega trend.

Buying instructions: BUY Corero Network Security plc (LSE:CNS) current price 4.96p, buy-up-to 6.45p. If the stock trades over the buy-up-to do not buy and wait for a more suitable entry price.

To avoid potential downside capital risk but also help to secure potential profit, we recommend using a trailing stop/loss conditional order set at 40% below your entry price.

Action to take: buy Corero Security Plc

Ticker: CNS LN
Price as of 25.06.20: 4.96 GBp
Market cap: £26.50 million
52-week high/ low: 6.10p/ 0.024p
Buy up to: 6.45p



Please make sure you review the latest advice before purchasing. Click here for the latest portfolio.

Sam Volkering
Co-editor, *Frontier Tech Investor*