FRONTIER TECH INVESTOR

ISSUE NO. 3 JULY 2016

Cyberwars: A global conflict no one can avoid

Introducing our top pick to play the cybercrime epidemic

Eoin Treacy

My credit card information has been stolen five times in the last two years. The first was because Home Depot's system was hacked. Then it was Target's customer support system. The third was because Anthem, my health insurer was hacked. The fourth was because my details were lifted from a card machine at a restaurant and the remaining one I have no idea about.

My card is insured but I have every confidence my name, address, social security number and other personal details are out there on the web for any nefarious party to access. That's regardless of how diligent I am at home with implementing a tight cyber security protocol on my computer, shredding all documents that go in the bin and only shopping on reputable websites.

However much I might like to dispense with my credit, bank and store cards it's just not possible. Think of how difficult it would be to function in today's society with only cash to get by. For example, you can forget about foreign holidays. Flights can't be booked with cash.

I was out shopping with my wife and daughters one Saturday morning last year when I got a call from the credit monitoring team at my bank asking if I had just booked two flights to Bangkok. Last month my wife got a call asking if she was in New York and had just been shopping at Macys. On both occasions our stolen credit card details were being used to secure goods and services and it was only because we insisted on replacing all our cards following every breach that we could quickly be absolved of any responsibility. It's enormously time consuming and worrisome to go through the whole palaver of replacing one's cards and yet it is something we can do little to avoid.

Regardless of the risk, the only time I have to go to visit physical

Intelligence bulletin

AI agent outwits flying ace

An artificial intelligence agent designed in collaboration with the US Air Force has beaten a top flying ace in a series of simulation dogfights. ALPHA – designed by Nick Ernest of the University of Cincinnati – isn't the first AI to defeat a human pilot, but according to its victim, it is the best. "I was surprised at how aware and reactive it was", said US Air Force Colonel Gene Lee. "It seemed to be aware of my intentions and reacting instantly to my changes in flight and my missile deployment. It knew how to defeat the shot I was taking. It moved instantly between defensive and offensive actions as needed."

Boffins design robot backside

Researchers at Imperial College London have designed a hyper-realistic robot posterior to help doctors train for prostate exams. Recruiting patients to act as guinea pigs for the procedure is notoriously difficult, and multiple studies have shown that volunteering for a prostate exam can prove a psychological burden. The robotic bottom – principally research by Fernando Bello – consists of a silicon thimble connected to small robotic arms. The resistance created by these arms is said to "accurately recreate the sensation of being inside a real anus".

location is when I visit the barber, doctor, dentist or vet. Otherwise it is when we go to a restaurant and spend some walking around the shops afterwards. I can have my dry cleaning and groceries delivered. I can shop for clothing and consumables online and when I take an Uber I don't need to pay upfront. Everywhere I shop in person takes my credit card and since I get cash back on purchases I have no incentive to use cash. The problem is that all this convenience comes at a price. Every time I use my card I'm at risk of having my details stolen.

These kinds of things have a big impact on my life. Perhaps you've been unfortunate enough to be on the wrong end of a hack personally too. You wouldn't be alone. Almost everyone has had some experience of cybercrime.

And that's the theme we're looking at in this month's *Frontier Tech Investor*. There's a cyber war going on. We're all at risk. And not just as individuals: cybercrime threatens everyone from you and me to global corporations to entire nations. Today, we'll look at what's happening and I'll introduce you to a company leading the fight for the good guys.

Is the system secure?

It's hard *not* to share your details "with the system" these days. The simple fact is the more heavily I rely on the digital marketplace the greater the risk is that my information will be stolen through no fault of my own. However Governments are very keen on promoting a cashless society because it is so easy to track electronic purchases. That helps them exert greater control over the economy, monitor the actions of suspicious individuals and perhaps the greatest motivation is to raise more tax.

According to the World Bank the two countries with the smallest shadow economies are Switzerland (8.5%) and the USA (8.6%) with the UK in 7th place at 12.5%. However when we consider that the GDP of the UK is $2.678 trillion USD, then the shadow economy represents $335 billion. For the USA it amounts to $1.54 trillion USD. That's an awfully large pot of money any government would love to be able to get its hands on. By eliminating cash they widen the pool of transactions that can be taxed, reduce avoidance of taxation and take greater control over the economy.

Governments want us to use electronic methods to spend our money, Credit ratings agencies make sure we have to build a reputation so that we can achieve the goal of home, car or boat ownership. Credit card companies reward us for using their cards so it all seems to be a virtuous circle until one realises it's completely porous. The risk of identity theft or worse grows with almost every transaction. So it's no surprise that identity theft is one of the fastest growing crimes.

That's the threat on the individual level. But on the national level the threat is perhaps even more profound.

Just last month details came to light of an audacious effort by

hackers to steal $951 million from Bangladesh's central bank. When one thinks of Bangladesh it isn't because it is a rich country. In fact if the criminals had not made a spelling mistake on the SWIFT transfer order the transaction might just have gone through and would have represented a damaging blow to the country's balance of payments. One of the reasons Bangladesh was an attractive target was exactly because it is a poor country with antiquated security protocols which gave the hackers access to the international currency transfer system.

There is no honour among thieves and they got away with $81 million from the Bangladesh heist. Authorities are scrambling to play catch up and having concluded their investigation have no idea who is responsible. If criminals are willing to commit such a crime against a small country it highlights there is no limit to what they are willing to do in the pursuit of profit.

Cybercrime threatens us individually and nationally

The reality is that cyber criminals are a proactive and audacious bunch who not only target individuals but also anyone they think has a capacity to pay. Ransomware is the most modern form of extortion there is. A group of hackers infiltrates your network and takes control of your company's server. They lock you out and hold your network hostage until a ransom is paid. Some of their favourite targets are hospitals and police departments because they cannot function without their databases and real lives are at risk. They also have access to the public purse and therefore are deemed to have the money to pay.

Imagine you find yourself in hospital and the doctor who is going to perform a life changing procedure for you cannot access your file because he has been locked out of the network. That's just not a risk a hospital can take since patients entrust them with their medical histories and they are some of our most precious commodities.

I was talking with a business owner last year who had been the subject of a ransomware attack. His business was an online clothing wholesale operation and they lost contact with all of their suppliers and clients for more than a week and ending up paying the hackers $25000. The FBI got involved but after six months had found no one to press charges against. For a small company that was a heavy blow and resulted in two people having to be let go in order to make ends meet.

And sometimes ransomware criminals are not after money.

Increasingly young people are having their personal email and photo backups hacked so that they can be exploited by sexual predators. For example two men were indicted in the USA last year for developing a piece of software that could automatically hack into a user's account and steal any nude photos it found. These were then used to extort money, favours or additional compromising photos from the target. Imagine how you would feel if you or your daughter became the subject of that type of extortion. It hardly bears thinking about.

Cybercrime Squared

Most of us understand cybercrime in the "data" sense – having our personal details stolen and used for criminal purposes. But there's another side to the story that's only now developing.

The internet is at our fingertips whenever we want it and right now it acts as a resource for us to share information, absorb entertainment and store our most cherished memories. However there is another side to the Internet that is just now reaching its explosive growth phase. The Internet of Things. In short that means within the next few years every single piece of machinery and consumer electronics is going to have an IP address and will be connected to the internet.

Your toaster will be able to talk to your coffee pot which will tell the airfryer to get busy on your breakfast while you brush your

teeth. That toothbrush could have an inbuilt sensor which will be able to report your health stats to your teledoctor while also keeping your dentist updated on your oral hygiene. When the toaster runs out of the bread, the coffee machine out of your favourite capsules or the fryer out of eggs they will simply order replacements from Google or Amazon who will take care of delivering new groceries the same day.

On the way to work you are probably already going to be catching up on email, building spreadsheets, completing a piece of graphic design or preparing RFVs because you won't have to drive yourself but will be chauffeured to your destination in an autonomous vehicle. When you relax in a bar after work you don't worry about forgetting your wallet because your ID will be your phone or another device will act as your payment method.

The Internet of Things is going to result in the range of threats we are exposed exploding. With sensors and Wi-Fi in just about all machines in our homes, schools, places of business, utilities and household meters, in our cars, buses, trains and planes. The potential for ransomware attacks to take an altogether more sinister perspective is very real indeed.

For example can you imagine a scenario where a ransomware operator takes control of your car and threatens to kill you unless you hand over your bank details or perform some lewd or illegal act for their gratification. How about if they took control of the school bus with your kids inside or the plane your wife is travelling home in? If you think it's impossible, think again. Anything connected to the internet can be contacted and influenced via the internet.

Just in case you might think this is all pie in the sky let me introduce you to Stuxnet, the world's first purpose cyber weapon, reputedly built jointly by the US and Israeli militaries. It was primarily used to infect Iranian nuclear development facility at Natanz and crippled the facility once it gained access. Here is the really worrying aspect to this development: it was probably developed by a team of between 5 and 30 over a period of up to six months. Relative to the cost of deploying single cruise missile not to mention an aircraft carrier cyberwarfare represents a highly cost effect way to prosecute a military operation.

The reason Apple would not help the FBI unlock the San Bernardino terrorist attacker's phone is because they are aware of the fact that once a method exists to crack the security of a network it is only a matter of time before interested parties learn how it is done. If we have learned anything all it is that once something exists in a digital space it will be there forever. This raises substantial risks for our personal information, intellectual property, state secrets and wellbeing of corporations.

We're all caught in the crossfire of a cyberwar

As all this wasn't scary enough have you ever asked yourself how could such large respected companies like Home Depot, Target, Sony, Anthem or Adobe Systems be so foolish as to allow themselves to be so easily exploited by hackers. The answer is depressingly simple. It's cheaper to be hacked than to invest in preventing it.

Target's data breach cost it $162 million after insurance helped soften the blow. That equally 0.1% of its sales in 2014. Home Depot's breach resulted in a loss of $28 million or 0.01% of sales. Sony lost about $15 million from its hack not least because *The Interview* wasn't a very good movie to begin with. Considering the additional employees, infrastructure, maintenance and root and branch reform of a company's culture that would be required to offset the risk these types of companies have little incentive to invest in cybersecurity.

This is a remarkably short-sighted perspective but it is nonetheless pervasive among a certain class of company; namely those that trade on delivering a real world service rather than jealously protecting their intellectual property. For example when was the last time you heard of Google, Amazon or Facebook being hacked? You haven't because they invest heavily in combatting hackers.

When the US Federal government's Offer of Personnel Management was hacked last year it represented an altogether different dimension. This represented a major resource for a foreign power to gain access to. It is believed that China now has the personal details

of 22.1 million US government employees together with their security clearance. It's one thing for Bangladesh's central bank to be hacked but this represented a major breach of a key US government piece of infrastructure. Retailers might look on a breach as the cost of doing business but governments have to develop other priorities. The stakes are just too high.

Backing the good guys

This is scary stuff. I don't pretend otherwise. But it also has implications for us as investors: **it means any company that can fight the good fight when it comes to cyberwarfare is sitting on a potential goldmine.**

Any conflict has both defensive and offensive characteristics. The primary route taken by most people is the defensive route where they employ a strict routine in the kinds of sites they visit and subscribe to anti-virus software services which protects their personal computer from unwanted programs. Unfortunately governments don't have that luxury. Protecting a nation's vital infrastructure, military interests, corporate intellectual property and citizenry cannot simply be defended. An offensive strategy is also required.

Leidos is global defense contractor headquartered in the USA and with strong ties to the US military industrial complex. It was among the first companies to help develop cruise missiles and developed the first luggage inspection machine to pass FFA tests. It has also been involved in a great deal of nuclear research as it pertains to healthcare as well as everything from designing an America's Cup winning yacht to a solar community. The company was listed on the stock market in 2006 and was split into Leidos and **Science Applications Intelligence Corp** (SAIC) in 2014.

SAIC is our pick for this month. It represents one of the most complete solutions to combatting cybercrime anywhere. Unfortunately it is just as illegal for each of us to pursue hackers as it is for them to pursue us so you cannot simply go out and buy an off the shelf hacker killer. (One can dream!) However companies like SAIC do consult with governments about how to best accomplish this type of project while making the majority of its money from designing and securing networks.

SAIC was one of only six companies chosen in May to participate in Cybercom's $460 million cyber operations contract to develop offensive technologies. This represents a very public foray into offensive technology development by the US government which has until now kept its cyber tactics covert. One of the reasons for making such a public statement is to send a message particularly to Russia and China that it is not willing to stand idly by while whole swathes of US data are stolen.

SAIC has a number of business lines such as Big Data & Analytics, Cloud, IT Managed Services, Networks and Communications, Software and Mobility Services, and Logistics but they are all offered with from a basis of enhancing the companies cybersecurity offering. After all why invest hundreds of millions in a new command centre only for it be taken over by hackers later. In the defence sector cybersecurity is increasingly moving front and centre in terms of priorities because it can literally mean the difference between life and death.

SAIC has contracts with the US Government to supply services to Air Force, Army Aviation and Missile Command, Marine Corp Systems Command, the Department of Defense, Homeland Security, NATO, Navy. In all of these endeavours the company's literature stresses reducing costs as a major objective. Considering the cost benefit analysis many organisations go through when they make the decision to adopt more robust cybersecurity measures that's an important fact.

As a result of the growth in government spending on

A cyberwarfare goldmine

cybersecurity SAIC earnings are expected to grow reasonably well but it is also worth pointing out that the company has been beating analyst forecasts as new contracts have been won. As a result of the companies relatively solid cash flows it has been paying a dividend since its IPO which grew at 10.71% last year and the share currently yields 2.13%.

So where's the risk? First off the vast majority of SAIC's contracts are government related. That's necessary when you are working with issues relating to national security but politicians are fickle beings and spending priorities can change. A decrease in spending on cybersecurity and cyber proactivity would represent challenges for SAIC. The company is also competing in a highly competitive field so there is the potential that another company will come up with a better product and that would also represent a challenge for the share but the good thing about cybersecurity is that there is no silver bullet, the threat requires constant monitoring and adaption of solutions.

I rate the share a buy based on the fact that geopolitical tensions are rising, cyberwarfare is a relatively cheap way of expressing a view for a country's leaders and demand for both defense and countermeasures is a growth market. SAIC is among the best at providing the services governments' need. I rate it a buy between $55 and $60, with a stop at $50. My target based on my expectation for impressive future earnings is $75 within the year and $100 in five years.

Name:	**Science Applications International Corp**
Ticker:	**SAIC US**
Current price:	**58.17**
Market Cap:	**$2.607.5M**
52 week high/low:	**61.93/39.28**
Buy between range:	**$55 and $60**
Dividend Yield:	**2.13%**

Data as of 04.07.16

Performance:
2014 +49.77% | 2015 -7.57%

Please note: performance data does not exist for the full five year period.

Cybersecurity stocks – an unusual tech sector

Mischa Frankl-Duval
Research Editor,
Frontier Tech Investor

On the morning of Friday 24th, I sat – along with the rest of the investing world – at my desk, watching most of my screen go red. The majority of the stocks I held were down, shedding single- or double-digit percentages. But there was one notable exception.

A Cybersecurity ETF I'd bought a few months previously was up several percentage points. It had been lagging badly over the last few months – the worst-performing holding I had, in fact – but was having its first significant up day in months as everything around it was falling to pieces.

It was tempting to attribute the sudden bounce in cybersecurity stocks to something akin to conspiracy. National security was a prominent issue during the referendum campaign, with the "In" team claiming Brexit would hinder international co-operation, leaving the UK more vulnerable to terrorism.

Like so much else said during the referendum campaign, this is partially true at best. If the vote did weaken national security, cybersecurity stocks didn't feel it. As Crossword Cybersecurity CEO Tom Ilube explained, it's unlikely that fears over increased cyberattacks were what drove cyber-defence stocks higher:

"Cybersecurity companies collaborate across boundaries, within Europe, and around the world. I can't see anything in the short-term that will change the level of collaboration that goes on.

"The people we're up against collaborate all the time, and they take no account of international boundaries, they can be in all parts of the world, online, and they'll work together to attack companies.

"The last thing cybersecurity companies can do is let those same sort of boundaries get in the way of us working together in order to compete against them. I

don't think Brexit will impact the industry as a whole."

I asked James Butterfill, Head of Research at asset management firm ETF Securities, whether the gains made by his company's ISE Cyber Security ETF could be attributed to post-Brexit panic; were corporations worried that hackers would look to capitalise on political uncertainty?

In two words, probably not.

"I think it's very difficult to infer that at this point. We haven't seen Brexit come up as an issue.

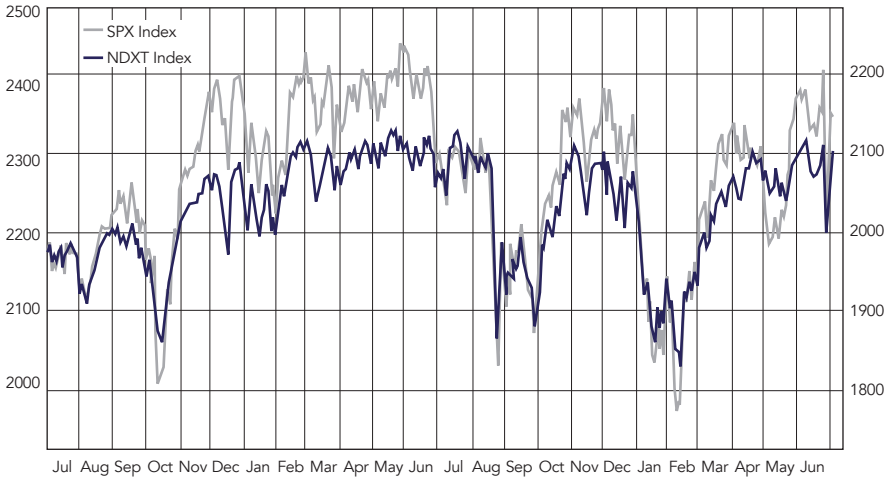
"Until Article 50 is signed, or until Brexit is annulled, we think uncertainty will reign supreme. No-one knows how much impact this will have, and that leads to investors pulling back."

"People tend to flock towards more defensive equities like health, consumer staples, and so on. Funnily enough cybersecurity fits into that. That's another reason it could be performing well."

Cybersecurity stocks aren't up because the political outlook has changed – at least not directly. Their price rising has much more to do with the kind of companies they are.

Cybersecurity companies aren't like other tech firms

Technology is a highly voguish sector, prone to greater volatility than the wider market. Tech markets experience higher peaks and lower troughs than the market at large. The graph below shows the performance of the S&P 500 against the Nasdaq 100 Technology Index (grey line):



Source: Bloomberg

Broadly speaking, the tech sector suffers deeper wounds in a bear market, but outperforms in bull markets. When money is tighter, investors stick to what they know. They invest in reliable, steady stocks (and other instruments) that will bet preserve their capital. Technology companies are often experimental by nature, dealing in products and services that are newer, less perfect, less established. Stocks like those are anathema to worried speculators.

Cybersecurity stocks aren't like that. That isn't to say cybersecurity companies aren't innovative – some certainly are – but the bread and butter of cybersecurity businesses is using functional, unglamorous technology to protect a growing number of mobile, tablet and PC devices. The number of devices connected to the internet is set to double to 30 billion by 2020. Those devices will always need to be protected against unwanted interference.

As well as earning contracts to protect new devices, providers will derive profits by selling subscription services to those whose devices they have already protected. That should provide cybersecurity providers with recurring revenue streams, buttressing them against the kind of fall from grace that sometimes does for more fashion—driven tech companies.

Cybersecurity is something of an anomaly within the tech sector. It's defensive. Its success doesn't rely on enormous breakthroughs or unique inventions, but on much more universal drivers of revenue. Sectors with those qualities are more likely to thrive in a downturn.

Should we see a full-blown recession, investors holding cybersecurity stocks might be amongst the few left smiling. Recession leads to cost-saving exercises – cutting down on staff costs is typically part of that process. Cybersecurity jobs are some of the most prone to automation; a recession would see unemployment rise, and cybersecurity stocks do the same.

Red-light lockdown

Nick O'Connor
Publisher

You're sitting in the back of a taxi, driving through the busy streets of London. Let's say you're heading north over Blackfriars bridge towards Ludgate Circus.

It's a sunny day. It's 10am. The streets are busy with people heading to work. There's a constant stream of people on bikes whizzing past the left window of the car. The traffic is slow. Between looking out of the window and chatting with the driver you check your phone. It's a quiet news day. Everything is calm.

The traffic is slow, though. You peer through the front window. Up ahead, the lights are red. But there's no traffic moving in any direction.

After a minute or so, cars start beeping their horns. The lights are still red. Everywhere. Nothing is moving.

After five minutes of waiting – the lights still haven't changed – your driver starts getting calls over his radio. There are problems everywhere: back behind you in Elephant and Castle. Up ahead on Fleet Street and Farringdon. Westminster is in lockdown. Lights everywhere are stuck on red.

A car ahead tries to make a move through the junction without a green light. The problem is, another car coming in the opposite direction had the exact same idea. There's a collision.

You check your phone for news. There's nothing.

"I'll get out here mate," you say, handing a £10 note to the driver. As he gives you your change his radio cuts out abruptly. You get out of the car. Other people have had the same idea. The streets are busy now. You cross the gridlocked road and walk towards the tube station on the corner of Blackfriars.

As you get there, it's obvious something is wrong here, too. The station doesn't seem to be letting new passengers in – in fact the opposite is true. People are flooding out of the underground and onto the street like water from a blocked drain.

"Barriers are stuck shut," you hear one person say.

"Lifts and escalators have shut down," someone else says.

"Apparently the trains aren't running," another voice in the crowd. "My friend has been stuck on a tube at Sloane Square for fifteen minutes."

There are thousands of people on the streets now. People are abandoning cars and public transport en mass. There's a palpable sense of panic.

Then, all of a sudden, what sounds like every fire alarm in the vicinity goes off at once. It's deafening. People look around at each other, then at their phones, searching for answers.

There's no information on the BBC, Sky, any of the newspapers or even on Twitter. Everything seems strangely calm.

Your phone rings. It's your wife. "I'm at the bank. I think we have a problem. The strangest thing happened–"

But the phone cuts out before she can tell you what's happened. You walk to a nearby cashpoint and put your card in. The machine swallows it. For a second you wait. Then, the screen goes blank before a graphic appears:

Something has gone badly wrong. Your phone still won't connect. There's no opportunity to find out what's happening. There are people everywhere. No one knows what's happening. More people are spilling out onto the street from an office nearby. "Fire alarms going off," someone tells you. "But none of the electric security doors will work properly. We had to break a window."

You don't know it yet, but this is the same situation people have found themselves in all over the

city. Transport is down, the traffic lights are stuck on red, the phone networks have crashed, hydraulic and electrically operated systems have frozen up, cash points are malfunctioning.

Something has gone badly wrong

And information is almost impossible to come by. The main news networks are operating – or so it seems. But they're supplying information that is false or gives no details about what's happening.

You're miles from home, the city has come to a standstill, no one knows what's happening and people are starting to panic. You're caught in the middle of the most sophisticated cyber attack the world has ever seen.

Actually, no, you're not. You're sat at home reading this issue of *Frontier Tech Investor*. And maybe you're starting to think: that could never happen, not here.

But it could. In fact almost every "hack" I just described to you has happened somewhere in the world, one way or another.

Take traffic lights, for instance. It is possible to hack into their operating system and lock them onto red. Security researchers at the University of Michigan have hacked 100 wirelessly networked lights – and were able to control them from afar (they did it has an experiment rather than a malicious attack). As IOActive Lab's Cesar Cerrudo put it at the Def Con 22 conference: "Anyone will be able to hack these devices and mess with traffic control systems since there is no patch available."

Or how about critical operating systems for things like doors, electricity, lighting systems, heating and video surveillance? According to a *Wired Magazine* story, there's a vulnerability that would allow hackers to control these systems remotely. According to the story, "The vulnerability in the Tridium Niagara AX Framework allows an attacker to remotely access the system's config.bog file, which holds all of the system's configuration data, including usernames and passwords to log in to operator work stations and control the systems that are managed by them."

It's the same story all over the world. In 2014 ComputerWorld carried a story containing an interview with cybersecurity expert Dan Clements. He described the situation in blunt terms: "We found thousands and thousands of these systems with what are essentially their digital front doors left wide open. Someone needs to be aware that there are vulnerabilities here that could affect critical infrastructure, including utilities and financial systems."

And London has previous when it comes to cyber attacks. Not on the scale I just described, of course. But during 2012 Olympics, there was a major attack on the power systems in the Olympic Park. As the Games' security chief put it: "At 5pm that evening, that's when we had probably our most serious attack in terms of a denial of service attack. That lasted for 40 minutes, 10 million requests coming from 90 IP addresses across North America and Europe," said Pennell.

Fortunately, the attack didn't cause any real damage. But the point remains: hackers have the ability, and in some cases the organisation, to launch large scale cyberattacks. The increasing interconnectedness of technological systems amplifies this risk.

This is a fairly new idea. As Eoin pointed out earlier, the Internet of Things means that cybercrime now has a new dimension. Where once it was a digital threat to digital property – data and personal information – it is now a digital threat to physical infrastructure. Take Stuxnet – the cyberweapon reportedly used to attack Iran's nuclear power systems. Stuxnet itself has no physical form – it's virtual. But its effects were decidedly non-virtual – they were real. That's a big change, and one that's going to become increasingly important as the threat grows.

The rise of political populism

Eoin Treacy
Investment Director

Populist nationalism is a theme which is gaining adherents all over the world. Xi Jinping's appeal to nationalism in order to inspire support for economic reform and to sustain the Communist Party's monopoly on power is an example in China. While I personally support the UK's decision to leave the EU, because of the democratic deficit evident within the political union, there is no doubt that there was a populist tone to the rhetoric that presaged the decision. The growth of similar movements in the Netherlands, Finland, Denmark, France, Italy and Spain suggests this is not simply a UK phenomenon. The surprisingly large support base both Donald Trump and Bernie Sanders appealed to in their respective campaigns for Presidential nominations are also evidence of populist nationalism in the USA.

Another way of thinking about the evolution of this kind of political perspective is that the trend towards greater cooperation appears to have changed. National self-interest is increasingly seen as a more important priority and not least in geopolitics. The Syrian refugee crisis could have been forestalled if NATO has been willing to set up safe zones for displaced people within Syria but no country was willing to do it. Russia's adventurism in Eastern Ukraine is only possible because it has judged, correctly, that no other country has the appetite to stop them. The rise of ISIS and the deplorable acts they commit so publicly could be stopped but no country with the means to eradicate the threat has the will to act. China's increasingly muscular actions in the South China Sea are only now being met with some form of resistance from the USA and then in a very soft way.

The failure of extraordinary monetary policy to stoke growth while simultaneously inflating asset prices, which has conspired to deflate living standards, has contributed to the economic malaise that has helped fuel the rise of populist solutions. For the USA two expensive wars in Afghanistan and Iraq with little success to show for a massive expenditure of human life and money has also contributed to a more insular mind set.

So far this has not translated into protectionist policies, a rolling back of globalisation or widespread antitrust cases against major corporations. However the risk is that these could become targets for populist policies if they are seen as threats to domestic living standards. That suggests the risk premium attached to markets is higher now than it was last week and could well intensify. It brings politics further into consideration of the markets which in itself is not a positive development.

The risk premium attached to markets is higher now than before Brexit

Risk warning

Your capital is at risk when you invest in shares – you can lose some or all of your money, so never risk more than you can afford to lose. Bid/ offer spreads, commissions, fees and other charges can reduce returns from investments.

The *Frontier Tech Investor* portfolio is not intended to represent the exact price at which you could buy or sell a share. Our reference price is the closing price on the day the recommendation was published. Sometimes readers will achieve better entry/exit prices; sometimes worse. All gains are gross, and returns will be affected by dealing costs and taxes.

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.

The information and opinions expressed do not necessarily reflect the views of other editors/contributors of MoneyWeek Research Limited. Full details of our complaints procedure and terms & conditions can be found on our website moneyweek.com.

Investment Director: Eoin Treacy. *Frontier Tech Investor* is issued by MoneyWeek Research Ltd. Registered in England and Wales No 9539630. VAT No GB629 7287 94. Registered Office: 8th Floor Friars Bridge Court, 41-45 Blackfriars Road, London SE1 8NZ.

MoneyWeek Research Limited is authorised and regulated by the Financial Conduct Authority. FCA No 706697. **https://register.fca.org.uk/**.

© 2016 MoneyWeek Research Ltd.

Energy

Company	Ticker	Rec Date	Price Then	Price Now	Gain/ loss %
Orocobre Ltd	ORE. AX	07/04/16	A$ 2.92	A$ 4.96	69.86

Technology

Company	Ticker	Rec Date	Price Then	Price Now	Gain/ loss %
Cyberdyne	7779	30/05/16	JPY 2,353	JPY 2,309	-1.87
IBM	IBM LN	07/06/16	152.98	152.35	-0.64
SAIC	SAIC US	05/07/16	58.17	58.17	0

Medical

Company	Ticker	Rec Date	Price Then	Price Now	Gain/ loss %
Acorda Therapeutics	ACOR	07/04/16	$ 27.98	$ 25.99	-7.11
Intuitive Surgical	ISRG	07/04/16	$ 626.12	$ 666.31	6.42

Moonshot

Company	Ticker	Rec Date	Price Then	Price Now	Gain/ loss %
SolarWindow	WNDW	07/04/16	$3.96	$4.04	2.02

For the full portfolio including live prices, please visit the *Frontier Tech Investor* subscriber area. **You can view that by following this link.**