Hutchinson Lilley Investments LLP
robert.hutchinson@hlinv.com

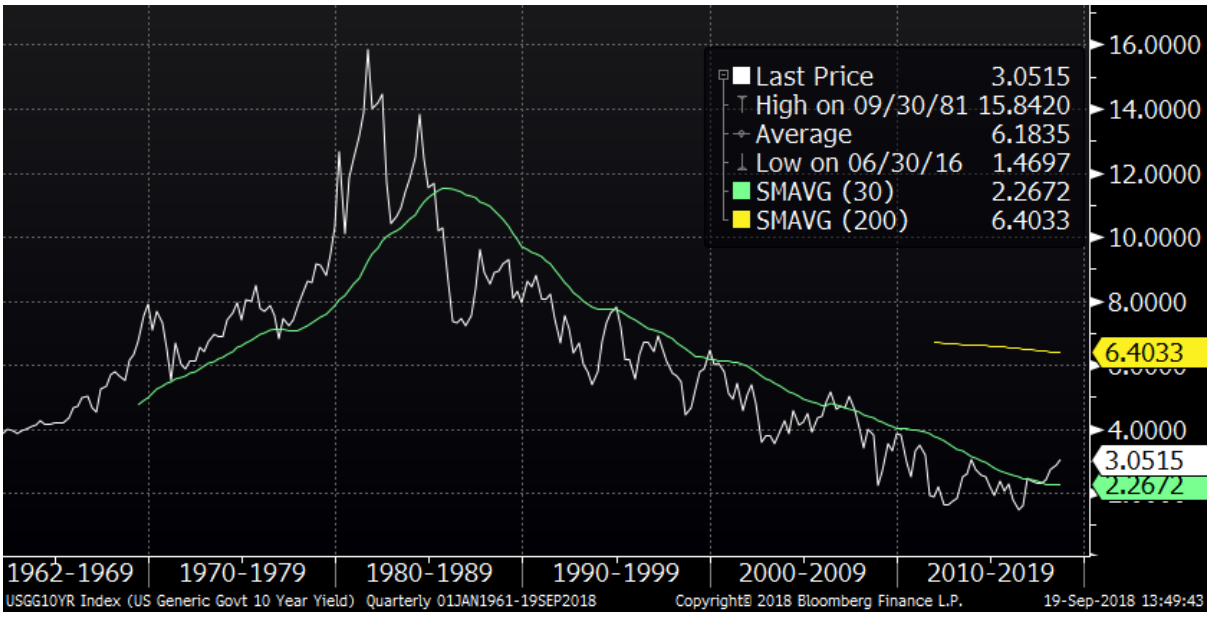
Cyber Danger (September 2018)

For the 9 months to end September, the world equity index is negative. The US continues to be the stand out on the positive side and emerging markets on the negative. Emerging markets are always hit disproportionately when Dollar liquidity is reduced and when US interest rates rise (see below). Europe and the UK are down so far in 2018 – the UK because of Brexit related political instability (I think) and Europe because of a creeping crisis in the Italian bond market, which I covered in the May report – An Italian Story - and which has deteriorated since.

S&P Index shown v Rest of World Shares

US Interest Rates moved up further during September, both at the short and the long end. The Federal Reserve raised the short interest rate and the bond market raised the long one (by investors dis-investing). In November 2016 our report was titled "The End of the Bull Market in Bonds" which was written after the Federal Reserve had implemented its first interest rate hike since the 2008 financial crisis. At that time the yield on the US 10yr bond was 2.4% and the US Consumer Price inflation rate was 1.6%. Since then there have been a further 7 hikes in the US interest rate, the latest coming in September 2018. Now the 10 year yield is 3.05% (and CPI 2.7%) which represents a near 30% increase in funding costs for long term borrowers – the largest of which is the US government.

34 Year down trend in US interest rates is broken

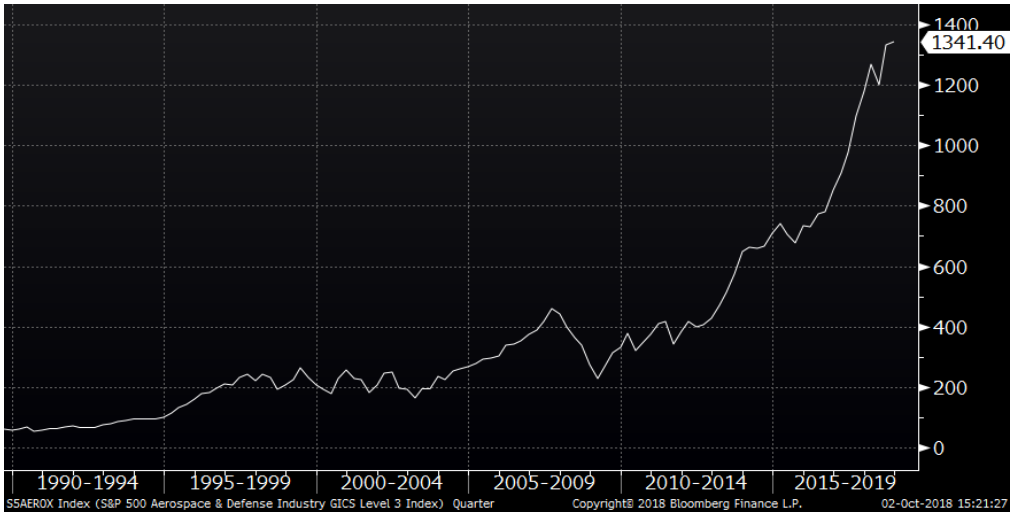


In the first 11 months of 2018 the US budget deficit (spending less taxes) rose by approximately one third to $898bn. Federal spending rose by 7% to $3.88trn while revenues rose only by 1% to $2.99trn. In fiscal 2017 the deficit was $666bn. Each year's deficit is added to the national debt which now stands at $21.5trn against $10.0trn 10 years ago. As shown above, the interest rate that borrowers must pay has risen and the US Government is the world's largest borrower. Its spending on interest is currently 6.6% of its total budget but is about to more than double both in money terms and as a percent of the budget. It will soon exceed spending on defence which stands at 11%.

Defence

One of our long term investment themes has been the defence sector, not because we approve of the wars (the contrary, of course) but because the US's permanent commitment to war makes this sector the nearest thing to an investment certainty there is. Whichever party is in power, there is no shortage of conflicts that the US government is willing to get involved in, together with its allies such as the UK. There are usually many voices speaking out to fight and only few calling for refrain. And once you have the weapons, you just need to use them. Can you imagine the feeling of unfulfillment for any General or Admiral in reaching the end of his service without ever having fired his weapons somewhere in anger, if only just once? This poor reflection of the human condition is of course excellent news for the suppliers of aircraft, ships, radar, ordnance and technology which is reflected in their share prices.

Chart of US Defence Sector



I have been reading the newsletter of Richard Maybury since 2002. Maybury is an unusual analyst. His grasp of economics is excellent as is his knowledge of military history having served in the 1960's in the airforce. His monthly subscription Early Warning Report is the first I saw which spelled out the case for owning defence stocks. (It is one of the best newsletters you can buy). My regret is not having been more fully committed to this theme. There were moments in the past when I believed that it might have run its course, only for it to become firmly established once again. So we have made money out of it over the years but nowhere near as much as we should have done and as would be suggested by the above chart.

Cybercrime

Since about a year ago, Maybury has developed a second long term theme which sits elegantly alongside the first. This theme is cybercrime which he says is still in its infancy and which is set to panic the world – a world which since 1995 has made itself totally dependent upon the internet. Most businesses simply could not function without being online.

Independently of the Maybury reports on the subject of cybercrime, I came across an article from Wired magazine which describes a devastating and widespread attack in 2017 by a dastardly piece of malware called notpetya. The article focuses on the impact of the attack on one company in particular, the Maersk shipping group. Maersk is headquartered in Denmark but its operations are worldwide. They control 76 ports and have over 800 ships. It is a real ripping yarn – here, an excerpt:

> *"I saw a wave of screens turning black. Black, black, black. Black black black black black," The PCs, Jensen and his neighbours quickly discovered, were irreversibly locked. Restarting only returned them to the same black screen.*
>
> *All across Maersk headquarters, the full scale of the crisis was starting to become clear. Within half an hour, Maersk employees were running down hallways, yelling to their colleagues to turn off computers or disconnect them from Maersk's network before the malicious software could infect them, as it dawned on them that every minute could mean dozens or hundreds more corrupted PCs. Tech workers ran into conference rooms and unplugged machines in the middle of meetings. Soon staffers were hurdling over locked key-card gates, which had been paralyzed by the still-mysterious malware, to spread the warning to other sections of the building."*

This article is certainly worth reading if only to get a sense of the worldwide disruption caused to just one target company as a result of the attack. The malware shut down ports across the world causing billions of losses, from rotting food to "just in time" factories closing through lack of component deliveries. The way the problem was fixed is also fascinating – like the very best crime thriller.

There is little information about the scale of cyberattacks because much of it takes place in secret. But by one estimate the global cost of ransomware has gone up by 15 times in the last 3 years. (This is where a victim's systems are locked down and only reopened against payment of a sum of money as ransom). The hackers are so smart that even the CIA, FBI and Pentagon have been caught. The key point though is that one cannot know who is responsible.

This is not conventional warfare where you can identify your enemy, mobilise against him or even negotiate with him. You are dealing with individuals or small groups who are excellent at disguise.

If and when cyber attacks are reported in mainstream media the article almost always attribute blame to the Russians or the Chinese. It may well be that attacks are by people in Russia or in China but this does not mean that the attacks are being carried out by those governments. It is more likely that those governments don't know who the attackers are either. Now this is being increasingly acknowledged: "Sophisticated cyber foes are adept at concealing their identities, making it hard to know exactly where an attack originates" according to Defense News, a US publication.

For anyone who has read Robert Heinlein's, The Moon is a Harsh Mistress, the small cell hierarchical structure will be familiar. This is an extremely efficient revolutionary strategy (versions of which were used by the Viet Cong, the IRA and during the Russian Revolution) in which subversion is carried out by small groups where no 1 person knows any more than 4 other people – the person who recruited him together with 3 people he recruits. It is nearly impossible to break down. Cybercrime seems to be organised on this basis.

For a little under a year, and as a result of the Maybury newsletter, we have held an exchange traded fund (ETF) which itself holds stocks of companies involved in the malware protection industry. These firms specialise in trying to protect buisinesses in the first place and carrying out the fixes once the problem strikes. We do not usually buy ETFs but we made an exception. In addition to these specialist cyberattack companies, we understand that the traditional defence companies (which we already hold) have been offered contracts worth billions by the Pentagon to develop their own cyberprotection abilities. This reinforces the original investments too.

This is set to be just as enduring a theme as the traditional defence sector described above and we anticipate retaining an exposure here even if the US market goes through a difficult patch.

Market price of HACK US Equity ETF

Summary

World equities have been in a bear market in 2018. Rising US interest rates have so far not halted the US stock market although they have wreaked damage to emerging markets and their currencies. Rising rates have also put pressure on the gold price (and obviously the US bond market).

There are numerous signs that the US share market is in a late stage of its cycle. However, there are some attractive robust long term themes which should offer resilience. Among these, defence and cybercrime fighters are preferred choices.