Australian Standfirst

# Sino Spycraft & Sophisticated Cybersecurity:

## Cuba, Vanuatu, UAE – Financial Risk Management Concernment Confronting The D10

Risk Management

**05 July 2023 | HFI#851**

**Stirling Larkin, CIO**

Across the Developed Ten Democracies, or D10, listed and private conglomerates are deploying their extensive computing infrastructures – especially in cloud and to a lesser extent edge servers – to the commercialisation of Artificial Intelligence, or AI, on a large scale, enabled by Taiwanese makers of the semiconductors and related equipment needed to amass such AI über-technology.

Cite:- Taiwan's Looming Crisis Is A Much Bigger Threat Than Markets Realise, 20 June 2018

Cite:- Taiwanese War & Markets Fallout, 30 January 2019

Cite:- Australia's Impossible Choice: Taiwan, 13 December 2020

Cite:- All Eyes On Taiwan: Microprocessors, Hypersonics & The Opportunity Set Across The Defence Complex, 20 May 2022

Beyond these *Mega-Caps* & multi-generational family groups, there exists a rich ecosystem of investable assets exposed to the AI megatrend within the Sino, pan-European and North American technological universe.

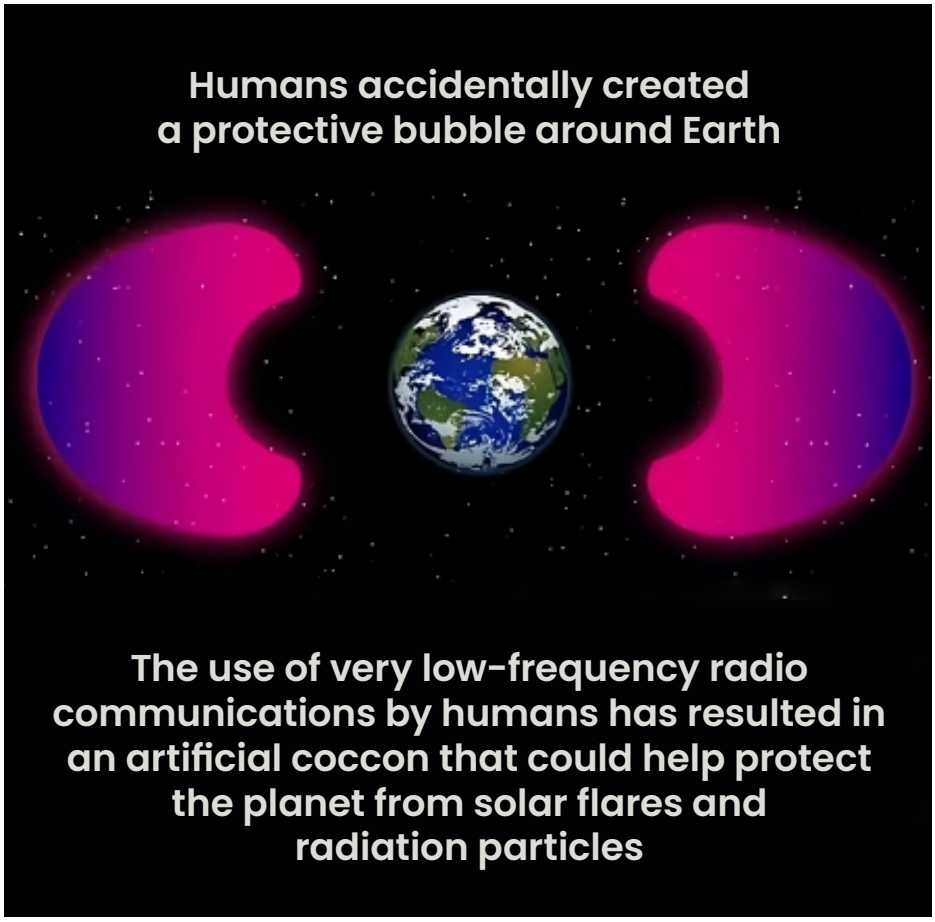
Protecting these rich ecosystems and the global investors whom seed them, the question of sophisticated cybersecurity plus risk management protocols in the eventuality of a ***Great Pacific War*** {now but a question of when, not if} becomes paramount, especially considering new AI-driven variables across the back-end of datasets cybersecurity, the front-end privacy of now known Sino-Cuban + Sino-Ni-Vanuatu listening posts and whatever really went on in the UAE bloc during the early 2010's and again, now.

Cite:- Relative Magnetism Of Rare Earths For Real-Money Investors: Green Capex, The Great Pacific War & Digital Revolution, 14 October 2021

Cite:- The Levant And Law of Unintended Consequences: Emerging Markets Northwest Of The Arabian Plate, 25 May 2020

Cite:- The Return of Great Power War, 2022

Complicated technologies have always defined *Realpolitik*, hegemony & wealth but the recent conflation of the quantum supremacy race, commercialised Generative AI and the *Formosan question* ratchet portfolio risk management and at-large cybersecurity to a new level of concernment for the individual global investor and monopolistic conglomerate alike.



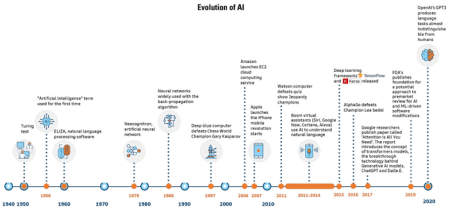

Cite:- Military Conflict With China, 6 November 2019

Cite:- Hong Kong Affects Backend Of Australian Wealth Management, 4 December 2019

Cite:- Goodbye Hong Kong, 19 April 2020

Cite:- Wolf Warrior Statecraft, 5 May 2020

Cite:- What Some Blanket As "Inflation" Is In Fact China Closing Its Factories To The West: Inflation In A US Election Year, Markets Impact & The *Sinosphere*, 6 January 2022




Even when what was thought to be a dependable family office cybersecurity practice of air-gapping came into question last month when a pair of NASA probes detected that within our *Magnetosphere* an artificial bubble around Earth had formed since the 1960's when radio communications from the ground interacted with high-energy radiation particles in space, allowing Sino, Russian and Indian spy satellites to differentiate Very Low Frequency, or VLF, noise from that of encrypted digitally transmitted datasets (within or outside of an Airgap, et cetera).

Cite:- Why Cybersecurity Will Be Key Issue In 2020s, 15 January 2020

Cite:- Cybersecurity for Family Offices: Edge Servers, Airgaps & Common Sense, 9 March 2022

Paradoxically, NASA now believes that the outer edge of the artificial bubble lines up almost exactly with the inner edge of the *Van Allen belts*, which suggests VLF waves can push radiation particles away and that the inner edge of the belts are much further from Earth now than it was in the 1960's, when humans sent fewer VLF transmissions (and when financial records, transactions or particulars were not broadcasted across the airwaves).

Commercially, cloud computing created new investment opportunities by enabling the delivery of software as a utility, Generative AI today further unlocks value as it extends this utility and provides new tools for enhancing end-user productivity.

Cite:- How 'Algo'/DMA Traders

Backstop Major American, Asian & European Markets: The Past, Present & Future Of Investing Without Surrendering Your Human Edge, 8 September 2021

Cite:- Scientific and Technological Flows Between the United States and China, 2023

While traditional AI has been helpful in making predictions of outcomes, Generative AI is about generating content such as text, video, images or computer code, which was previously not possible and in unison with Large Language Models, or LLM's, which will produce profound levels of proficiency and intelligence, literally and metaphorically.

Within the reach of *Pax Americana*, Microsoft [MSFT:US] has clearly taken the technology industry by storm by being first out of the gate with Co-pilot variations of *Microsoft 365*, *GitHub* and *Dynamics*; Adobe [ADBE:US] stands to revitalise its growth prospects with the launch of *Firefly*, while *CRM* should benefit from a front-office productivity boost, both within the listed and private sectors.

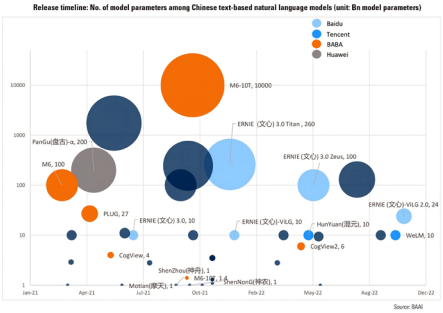
Additionally, Intuit Inc. [INTU:US], Alphabet Inc. [GOOGL:US], Amazon [AMZN:US], NVIDIA Corp [NVDA:US], and Meta Platforms Inc. [META:US] are *Mega-caps* best positioned to succeed in this new AI-driven paradigm.

Just as the cloud *hyperscalers* – such as Amazon Web Services, Microsoft Azure & Google Cloud – commercialised cloud infrastructure and platforms, which in turn accelerated the growth of Software-as-a-Service, or SaaS businesses, OpenAI's ChatGPT will and has driven adoption of Generative AI across software enterprises, integrating into the technology stacks of both qualitative datum and also layering quantitative datasites with AI analytics (a.k.a. Dynamic Big Data, or DBD).

Alternatively, within the *Sinosphere*, Bǎidù [9888:HK] debuted their generative AI Chatbot, *ERNIE-Bot*, in March followed by AliCloud's launch of Model-as-a-Service, or MaaS and "*Tongyi Qianwen*" in April, with upcoming smart assistant full integration into Alibaba's [BABA:US] work productivity and all key applications.

Cite:- The Lucrative Investment Question Of Our Time: Chinese Technology – Sino Semiconductors, Digital 元 & Cyber-Sovereignty, 26 April 2021

China pundits are optimistic about China developing its own unique foundation models with Chinese language understanding advantages, leveraging its competitive advantages holding an abundant and idiosyncratic data-pool in Chinese, better understanding of the language compared to foreign peers and a deep bench of research and engineering talent.




Cite:- The Investment Theme We Like, For A Technology We Hate: Facial Recognition Technology (FRT) and Dual-Use Applications, 13 July 2020

On 11th of April, the Cyberspace Administration of China, or CAC, released a new draft regulation for comments on Generative AI, highlighting twenty one potential articles and serendipitously, on the same day the US Government also announced that it will weigh possible rules for AI tools such as ChatGPT.

According to the released Plan on Reforming Party and State Institutions on 16th March, a new agency named 'National Data Bureau' (国家数据局) will be established under China's top economic and social development authority, the National Development and Reform Commission, or NDRC.

China also has a Regulations on the Administration of Deep Learning of Internet Information Services which imposes obligations on Generative AI service providers alongside existing Measures for Data Export Security Assessment guidelines (more than just a 'guideline'... firing squad..).

Clearly, Generative AI has very significant implications for the world of cybersecurity and can be leveraged to detect fraud, malicious actors, spam incidents and importantly for global investors, more advanced AI + Machine Learning in cybersecurity to buttress both offensive and defensive applications: (a.) aggressors leverage Generative AI capabilities to increase the speed and variation of attacks, and (b.) security vendors apply AI to reduce the time to detect and respond to zero-day attacks at scale.

Unlike consumer AI where generative solutions can drive creative capabilities, enterprise-focused security AI requires far more exacting applications and have historically been constrained by access to comprehensive data sets.

This remains the biggest hurdle for AI in cybersecurity today, along with the challenges of preventing unintentional shutdowns of mission critical workloads.

However, across the D10, we are starting to see the benefits of AI & Machine Learning in threat detection and believe platforms with extensive internal data logs across both Endpoint and Network are best positioned to benefit long term.

CrowdStrike [CRWD:US] is leveraging its extensive data and telemetry history to equip new modules on its Falcon Platform with AI capabilities and the company has a history of effective marketing to both decision makers and consumers, which positions them as a strong brand as consumer awareness of AI application grows.

Another 2023 example, Palo Alto Networks [PANW:US] is leveraging its extensive threat detection logs in building out major product releases including its AI-based security operations (SOC) platform *XSIAM* and updates in Prisma Cloud. Similar to CrowdStrike, Palo Alto's marketing is effective across both decision makers and end users in enterprise technology.

Cite:- Military & Security Developments Involving China, 2022

Observability across data centres, neural networks, containers & serverless computing back-end platforms, hybrid clouds and edge computing are all material concepts that best be speedily understood by savvy global investors whom wish to protect their financial corpora whilst also proactively participating in the rich ecosystem of investable assets exposed to the incumbent AI megatrend set upon us. ■