WHAT I LEARNED THIS WEEK

Excerpt from November 2, 2017

5 China is racing ahead to lead the world in the deployment of AI for cybersecurity. *Huge new winners and losers will follow.*

Pushed by the revelations of the NSA/Snowden scandal, China decided to take control over its technology destiny. China is already ahead of the U.S. on cyber defense—able to detect attacks faster and plug vulnerabilities more quickly. Presently, there is an average 20-day gap between when China's cybersecurity database publishes information on newly-discovered bugs versus the U.S. equivalent, calculates consultant Recorded Future. Details of the critical software flaw responsible for the Equifax hack that compromised sensitive information on 145 million Americans was published on China's National Vulnerability Database **within a day.** In contrast, it did not appear on the U.S. database for **three days.**

The U.S. National Vulnerability Database—run by the U.S. Department of Commerce—depends on voluntary submissions, primarily from producers of the buggy software. However, China uses a wider variety of sources and methods, including technical testing to compile its database. As a result, **Recorded Future found 1,746 "common vulnerabilities and exposures" in the Chinese database that are missing from the U.S. database.** The U.S. system is also providing inadequate coverage of industrial control systems and medical devices.

Baidu—China's AI leader—has established **the largest deep neural network in the world,** with 20 billion parameters, highlights a research paper entitled *"Who Will Win Practical Artificial Intelligence? AI Engineerings in China."* Baidu is now using its deep neural network to help drive the company's security software. Baidu is also building a platform for 372 police agencies to use sophisticated AI tools to help patrol cyberspace.

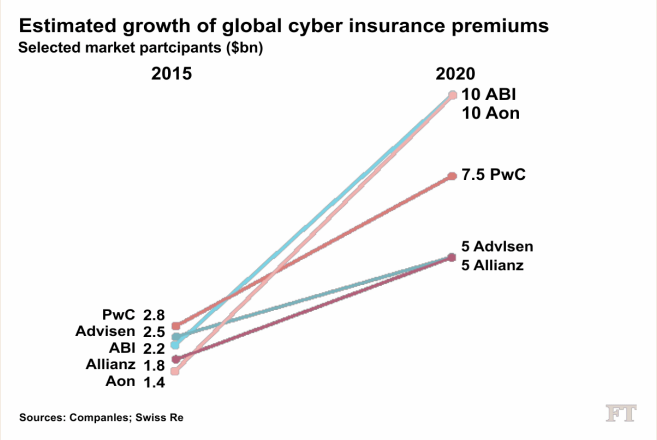
To expand its talent bench, China is building four to six "influential" cybersecurity schools over the next decade—**aiming to recruit "gifted youth" or "maverick geniuses."** These factors combined with China's lead in deploying AI systems and creating an un-hackable quantum communications network—conducting the first ever quantum video call this month—will provide a **competitive edge.**

What are the implications? First, the security industry is on-track to be one of the first large-scale adopters of AI—creating new self-learning networks and products, concludes a recent *Bloomberg Intelligence* analysis. AI promises to shorten the time for detecting intrusions from an average of 39 days, calculates Nemertes Research, to just hours or minutes. AI will become proactive by using behavioral analytics to stem cybersecurity risks from inside an organization. Within the next year, AI systems will be able to continuously re-write encryption keys—helping to prevent them from being unlocked from hackers outside an organization.

Second, artificial intelligence is a double-edged sword for cybersecurity. A new Cylance study concludes that AI will be weaponized for cyberattacks within the next 12-months—providing a clear asymmetric advantage to terrorists and criminals. **AI will make complex attacks faster and more effective—enabling attackers to react more quickly when encountering resistance.**

Third, current cyber defense systems may be unable to keep up with the speed of incoming attacks. This will drive a programming and technological arms race, notes an analysis in *The Conversation*, with defenders potentially using AI with retaliatory capabilities.

Fourth, the **cyber insurance industry is set to boom**—potentially tripling to $10 billion in three years. Allianz believes the cyber insurance market could reach $20 billion by 2025, up from $3 billion to $4 billion presently. A new EU rule in 2018—the General Data Protection Regulation (GDPR)—will accelerate demand for cyber insurance by **imposing penalties on companies that have a data breach.**



Source: The Financial Times

Consider the following:

- **AI will revolutionize cybersecurity.** Most breaches today are due to "cyber blindness," as it is impossible to manually read and analyze the huge volumes of data needed to be processed every day. Large companies can sift through 200,000 "security events" daily to identify a real threat, notes Caleb Barlow of IBM Security. However, on average, a cybersecurity analyst can review only 10 to 20 high-risk security incidents in a day.

  Machine learning algorithms enable the identification of data patterns, vulnerable user behaviors and predictive security trends at unprecedented speed and scale. IBM has combined its cybersecurity QRadar Advisor software with Watson to perform 60 times faster than a human investigator—reducing the time spent on complex analysis of an incident from an hour to under a minute. As a result, AI will help alleviate the shortage of human cybersecurity experts—with one million cybersecurity jobs expected to go unfilled globally this year.

- **China's new cyber law could threaten U.S. dominance in AI/ cybersecurity.** China's cyber strategy centers around the new law that took effect June 1, which includes its AI development plan. The law covers everything from strengthening resistance to vulnerabilities to media control, economic growth, and reduced dependence on foreign technology, notes Paul Triolo of the Eurasia Group.

The goal is to make China a cyber-superpower and increase its influence in setting global standards. "Without cybersecurity there is no national security," recently underscored President Xi Jinping.

The law will increase costs for foreign companies and may give Chinese companies an advantage. Companies must introduce data protection measures, and data relating to China's citizens or national security must be held on Chinese servers. **The measure also allows Beijing to request computer software source code.** Multinationals will be hard hit, because data localization will prevent them from combining client data in cloud storage spread across the world.

The global view of China's approach to security may begin to shift. Steven Lee Myers and Sui-Lee Wee recently noted in *The New York Times*:

> *For years, the United States and others saw this sort of heavy-handed censorship as a sign of political vulnerability and a barrier to China's economic development.* ***But as countries in the West discuss potential internet restrictions and wring their hands over fake news, hacking and foreign meddling, some in China see a powerful affirmation of the country's vision for the internet.***

- **"The AI itself is now becoming a target,"** warns Roman Yampolskiy, an AI/security professor at the University of Louisville. Hackers could exploit machine learning by gradually teaching a security system that unusual behavior is normal. Hackers could also use their AI to fake human voices and create video images granting criminals network access. "If you get a call from someone whose voice you recognize and they say, 'I don't have time to talk, give me your password', you will give it to them," underscores Yampolskiy.

  AI may prove to be the ultimate asymmetric hacking tool—reducing workloads for thieves and leading to an exponential increase in the number of attacks.

- **The rise of China's cybersecurity sector could accelerate sector consolidation.** The industry remains fragmented, as customers demand

fewer products and unified platforms that can provide a holistic security solution. Given the size of their balance sheets, *Bloomberg Intelligence* argues that IBM, Cisco, Check Point Software and Symantec are well positioned to lead an M&A roll-up of the sector in the West.

Chinese cyber-AI leaders are showing relative strength. Attractive candidates are:

√ **Baidu** (BIDU, $245.43), a leader in AI security-related systems—trading at 20.4x EV/EBITDA.

√ **Westone Information Industry Inc.** (002268 CH, 24.87 CNY), a provider of security information systems and security integration services in China—trading at 5.2x book value.

√ **Venustech Group** (002439 CH, 23.17 CNY), a provider of network security products and security services, including security gateway, security monitoring and data security and platforms—trading at 26.6x EV/EBITDA.