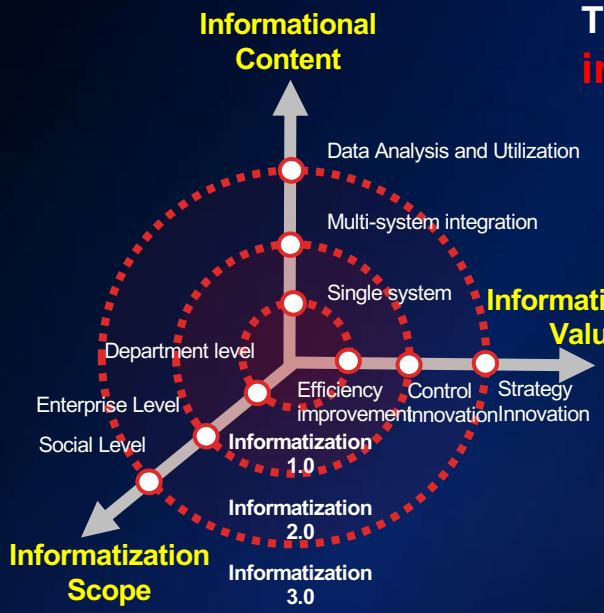
中国网络安全产业概况
Cybersecurity Industry of China

Dr. Paul XY. Chen

March 3, 2023

Drivers of Cybersecurity Industry Development



Three driving forces for the development of the cybersecurity industry: informatization, threat confrontation, and policy compliance

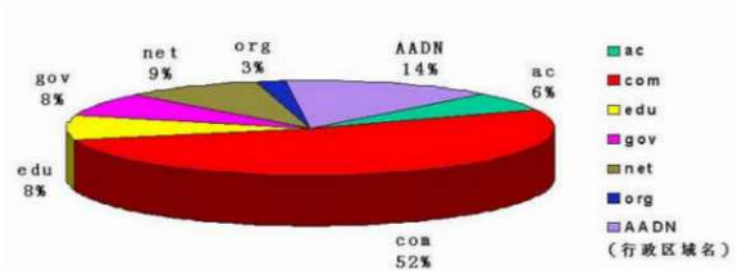
Single-point defensive security products → Defense-in-depth system → Normalized and practical security capabilities

The initial stage of China's cybersecurity industry: 1994-1997

▲On April 20, 1994, China realized the first TCP/IP full-function link with the Internet. Subsequently, a large number of networked information systems were gradually established and operated, playing an important role in scientific research and production.

	AC	COM	EDU	GOV	NET	ORG	行政区域名	合计
数量	259	2131	325	323	370	99	559	4066

各类域名所占的比例如下图所示：



97年10月域名分布情况

---from China Internet Network Information Centre, Statistical Report on the Development of Internet in China (1997/10)

The remote networks and remote access services poses the following security threats：

- Illegal access: illegal access resources that are not allowed to be accessed, thus causing security issues such as data leakage
- Network eavesdropping: during end-to-end data transmission, attackers listen to data transmitted in the network with the aim of stealing data, tampering with data, replaying data, etc.
- Network virus: Viruses use the network to spread and destroy

★On February 18, 1994, the Regulations of the People's Republic of China on the Security Protection of Computer Information Systems, Decree No. 147 of the State Council of the People's Republic of China, was officially issued.

The Growth Period of China's cybersecurity Industry: 1998-2012

Information security assurance system gradually formed

Changes in attack drivers

Prior to 2004

driven by Interest

CIH virus spreads globally

2004~2007

mainly driven by economy

TJX Credit Card Information Theft

2008~2012

simultaneously driven by economy and politics

Iranian nuclear plant hit by Stuxnet

Information security system flourishes

In 1998, the US proposed the IATF system

In 2005, the ISO 27000 standard system was officially published.

As of 2010, the US SP800 standard is approaching 499 documents

As of 2012, the cobit standard has been updated to version 5.

01 Core regulatory bodies established one after another to promote information security systems

1998 Public Information network security Supervision Bureau

2001 State Council Informatization Office

2003 China Information Security Product Evaluation and Certification Center

2005 State Encryption Administration

02 Gradual improvement of Classified Cyber Security System

1999 GB 17859-1999 "Guidelines for the Classification of Security Protection Levels of Computer Information Systems

2003 Opinions of the State Informatization Leading Group on Strengthening Information Security Assurance ([2003] No. 27)

2007 "Information Security Classified Protection Management Measures" ([2007] No. 43)

2008 GB/T 22239-2008 "Information Security Technology - Basic Requirements for Classified Protection of Information System Security" standard was issued, which together with other security standards constitute the core group of security standards.

2012 Several Opinions of the State Council on Vigorously Promoting the Development of Information Technology and Effectively Safeguarding Information Security ([2012] No. 23)

The Acceleration/Transition Period of China's Cybersecurity Industry: 2013-2019

Cybersecurity rises to national strategy

The "Snowden" incident changed the definition of cybersecurity

From the original Network Security and Information Security to Cyber Security, cyber security has been elevated to a national strategic level

Conflict rages in the Fifth Dimensional Cyberspace

Cyber attacks are driven by profit or political purposes, triggering major security incidents at home and abroad such as the Ukraine power grid intrusion and global ransomware virus, and security issues such as critical infrastructure and personal information continue to emerge, making the cyber security situation increasingly critical.

National cybersecurity policy follows the cybersecurity situation closely

Feb 2014

The Central Leading Group on cybersecurity and Informatization was established, with Xi Jinping, General Secretary of the Central Committee of the Communist Party of China (CPC) and President of the People's Republic of China (PRC), as its leader, stating that "without cybersecurity , there is no national security".

Apr 2016

General Secretary Xi delivered the "4.19 Speech" and the National Cyberspace Security Strategy was released in the same year.

June 2017

The Cybersecu rity Law came into force, bringing cybersecu rity into the era of the rule of law.

July 2017

he Central Internet Information Office (CIO) released the Regulations on the Security Protection of Critical Information Infrastructure (Draft for Comments).

June 2018

The Ministry of Public Security released the "Regulations on cybersecurity Level Protection (Draft for Comments)", and China's cybersecurity entered the era of equal protection 2.0.

May 2019

The national standards "Basic Requirements for Classified Protection", "Requirements for Classified Protection Evaluation" and "Technical Requirements for Classified Protection Security Design" were officially released and came into effect on 1 December of the same year

The deepening period of China's cybersecurity industry: 2020-

The digital security wave is on its way

Post-epidemic era

1 Jan 2020

The COVID–19 epidemic is a major public health emergency with the fastest spread, the widest range of infections, and the most difficult prevention and control since the founding of New China.

The Law of the People's Republic of China on Codes was adopted by the Fourteenth Session of the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China and shall come into force on 1 January 2020

April 9, 2020

In the post-epidemic era, the accelerated application of 5G, the accelerated development of video conferencing and collaborative working, and the dramatically accelerated wave of digital transformation have brought new opportunities for economic development while also bringing many new challenges to the field of cybersecurity

The Opinions of the State Council of the Central Committee of the Communist Party of China on Building a More Perfect Institutional Mechanism for Market-Based Allocation of Factors proposes that data becomes a new type of production factor.

July 3, 2020

Key Security Threats

- Data leakage
- Employee misuse
- Illegal operations

The (Draft) Data Security Law of the People's Republic of China is published on the website of the Chinese National People's Congress for public consultation, with a deadline of 16 August 2020 for comments

October 13, 2020

Data security and the crisis of trust are now the key security issues.

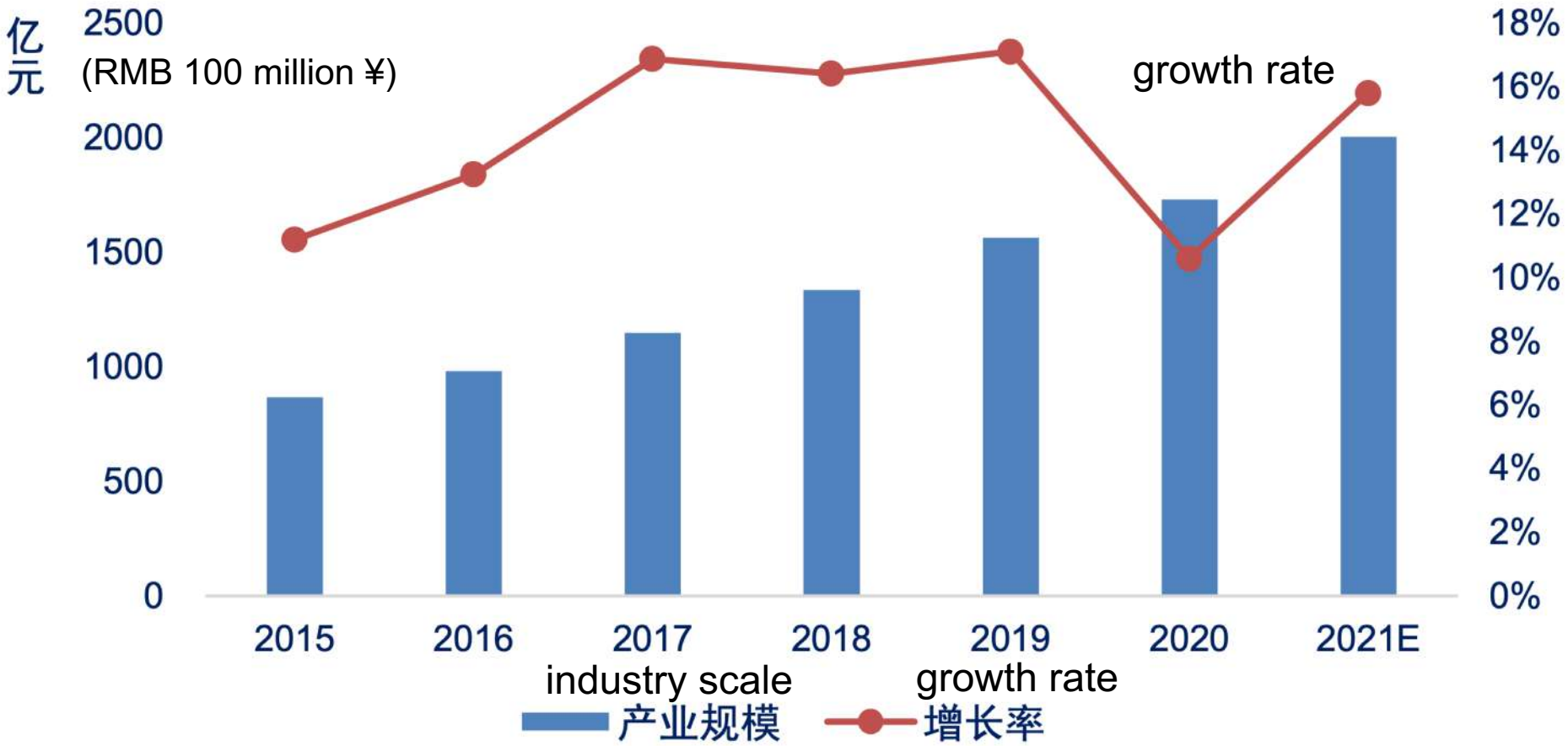
The meeting of the chairmen of the Standing Committee of the 13th National People's Congress has proposed a motion on the draft law on the protection of personal information for consideration

New Planning New Opportunities New Era

New infrastructure: In March 2020, the Standing Committee of the Political Bureau of the Central Committee of the Communist Party of China held a meeting and proposed to accelerate the progress of the construction of new infrastructure.

The 14th Five-Year Plan: On 29 October 2020, the Proposal of the Central Committee of the Communist Party of China on the Formulation of the 14th Five-Year Plan for National Economic and Social Development and the 2035 Visionary Goals, which states that the 14th Five-Year Plan will certainly be five years of intelligent development, and all industries will be upgraded with new information technology

The Scale of China's cybersecurity industry



Source： CAICT

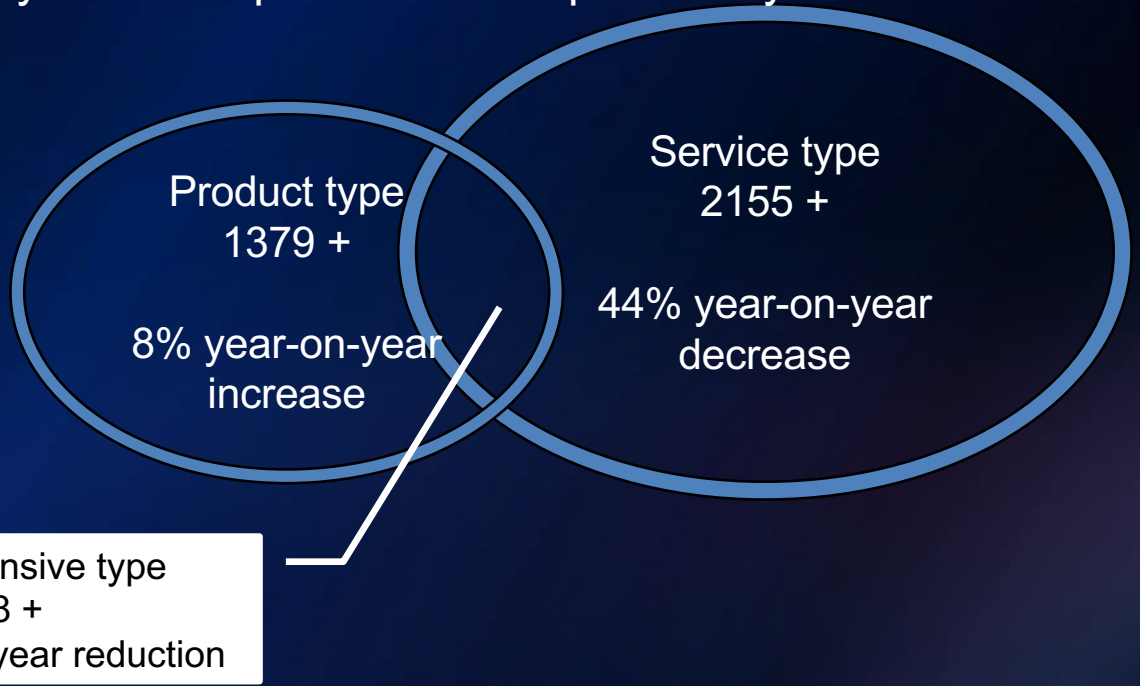
Major players in China's cybersecurity industry in 2021

Companies	**Security Revenue** (100 million ¥)	**Revenue Growth Rate**
Qianxin	58.1	39.5%
Venustech	43.9	20.3%
Sangfor	36.9	10.2%
Topsec	33.5	18.2%
Westonecloud	27.9	17.0%
Nsfocus	26.1	29.8%
DAS-security	18.2	37.6%
Asiainfo	16.7	30.8%
360	13.8	70.9%
Zhongfu	12.7	27.9%
Dptech	10.3	15.6%

By the end of 2022, there will be 29 companies in China's A-share market with cybersecurity as their main business, and 18 companies with non-main business in cybersecurity but separately listing their income.

Distribution of Cybersecurity Enterprises in China

As of June 2022, the number of cyber security companies in China is about 3,256, mainly due to the impact of the COVID epidemic, which has decreased by 31% compared with the previous year.



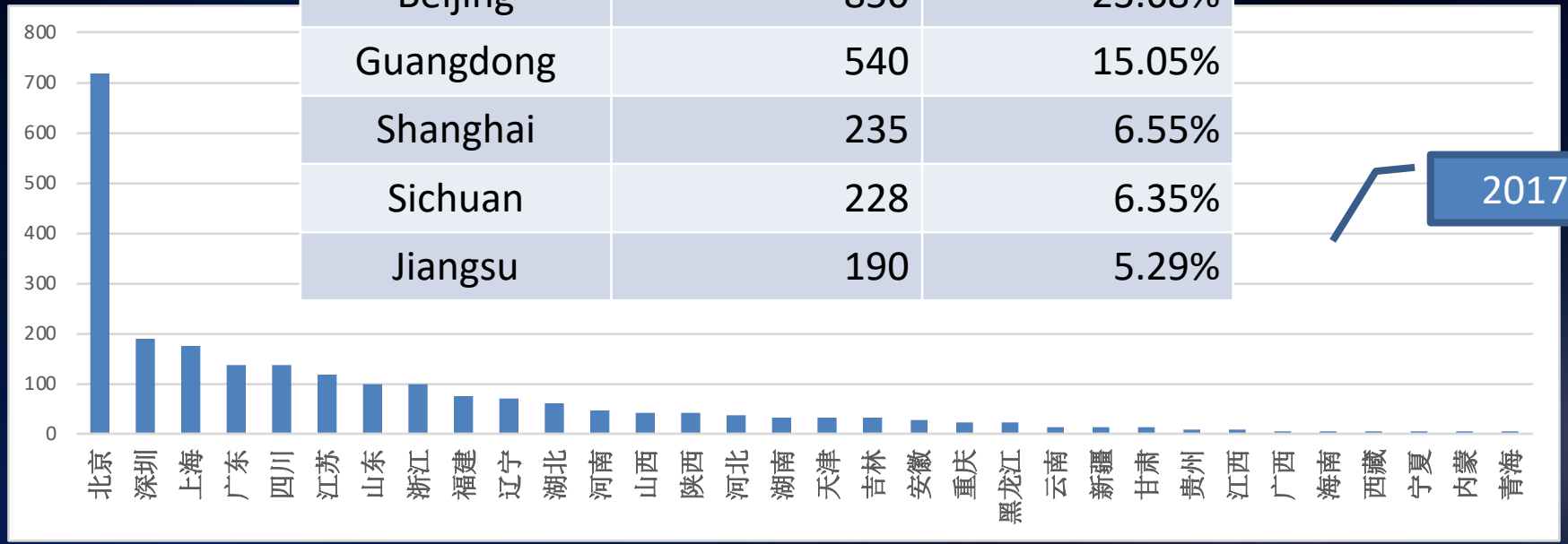
Source: CCIA

Geographical Distribution of Chinese Cybersecurity Enterprises

2020

Location	Enterprises No.	Proportion
Beijing	850	23.68%
Guangdong	540	15.05%
Shanghai	235	6.55%
Sichuan	228	6.35%
Jiangsu	190	5.29%

2017



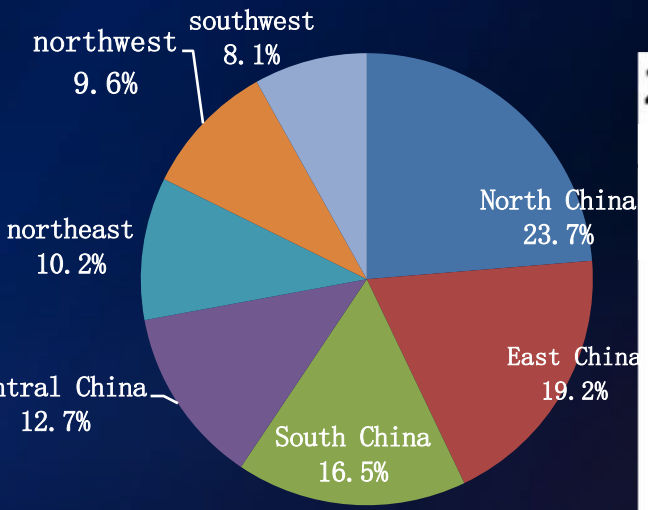
Source: CCIA

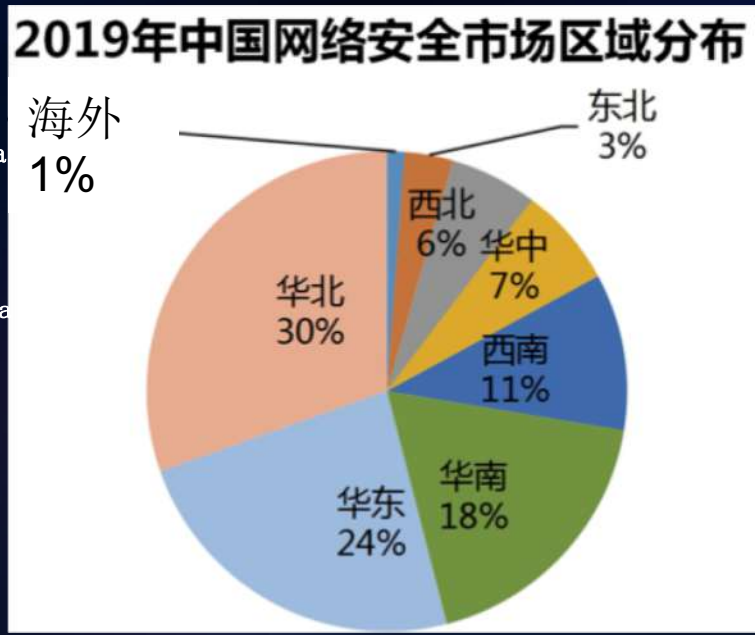
Regional distribution of China's cybersecurity industry market

China's cybersecurity product sales market is mainly concentrated in the three major regions of North China, East China, and South China. The sales of cybersecurity products in these three regions account for about 60% of the overall market.

In addition, affected by national policies such as the development of the west and the revitalization of the Northeast in recent years, the development of informatization in the Northwest, Southwest, and Northeast regions has also accelerated, and the demand for cybersecurity products has increased.

Regional Distribution of China's Cyber Security Market in 2017

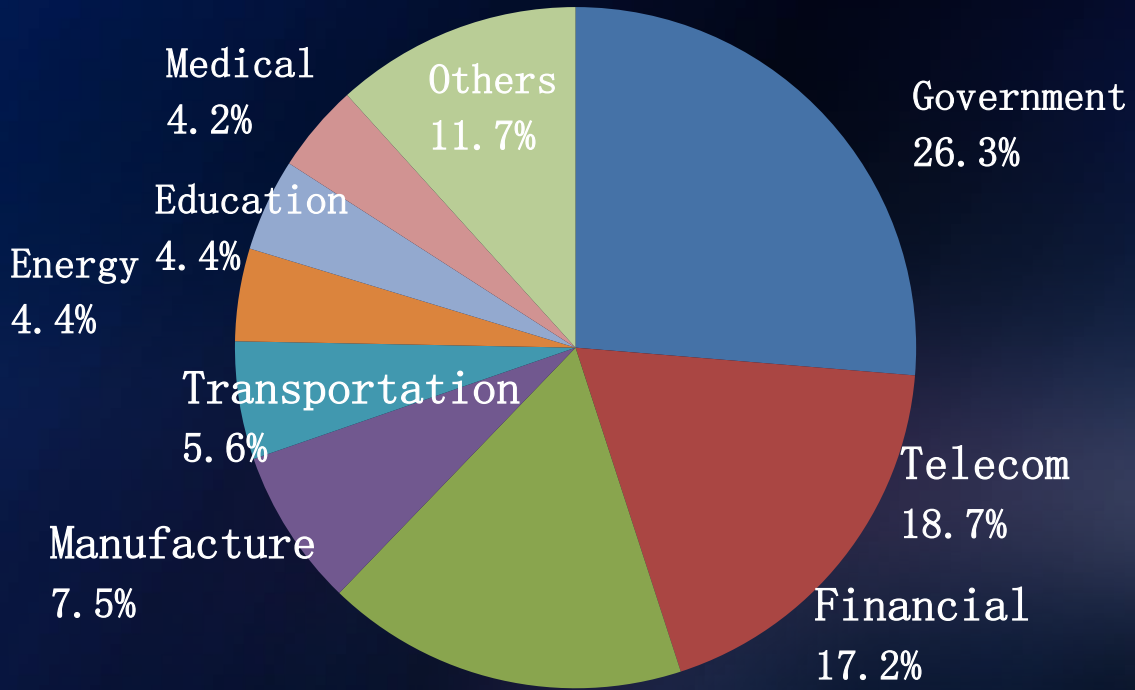




Source: CCIA

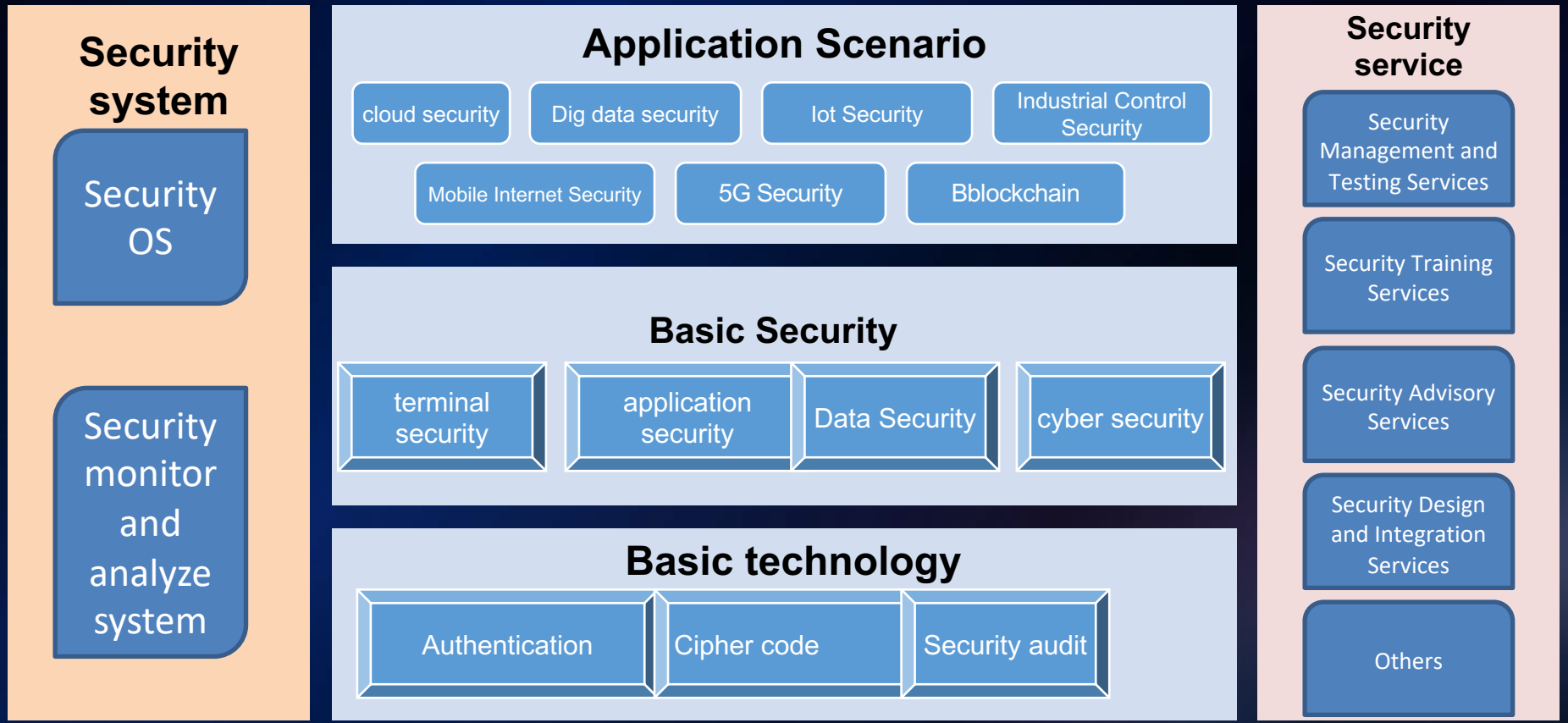
Industry distribution of China's cybersecurity market

The government sector still holds the largest share of the cyber security products market at 26.3 per cent, followed by the telecoms sector with 18.7 per cent, followed by finance with 17.2 per cent, manufacturing with 7.5 per cent, transportation with 5.6 per cent and energy and education both with 4.4 per cent



Source: CCIA

Cybersecurity product and service map



Source: CCIA

China Cybersecurity Market Panorama 2022

Source: Cybersecurity Reviews

Overview of China's cybersecurity industry financing in 2021

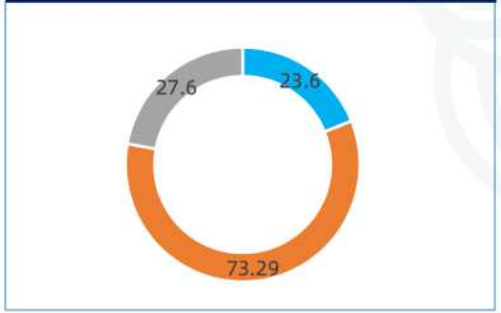
125.16亿元 2021年融资额	175次 2021年融资交易数	41.8亿元 2021年并购额	4 2021年并购交易数

（2012-2022H1）网络安全行业融资额

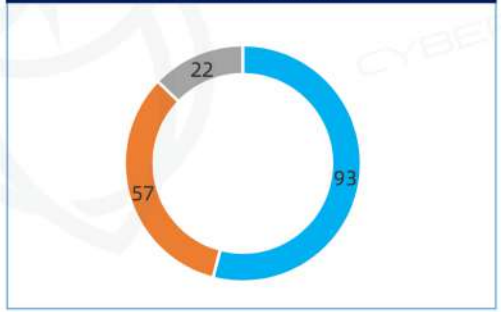
2021年并购事件

并购标的	并购方	交易金额
北京万里红	北京东方中科	29.79亿
沈阳通用软件	360	4.64亿
北京数字观星	360	2.56亿
东巽科技	360	2.34亿

2021各轮次融资金额分布（单位：亿元）



2021各轮次融资次数分布



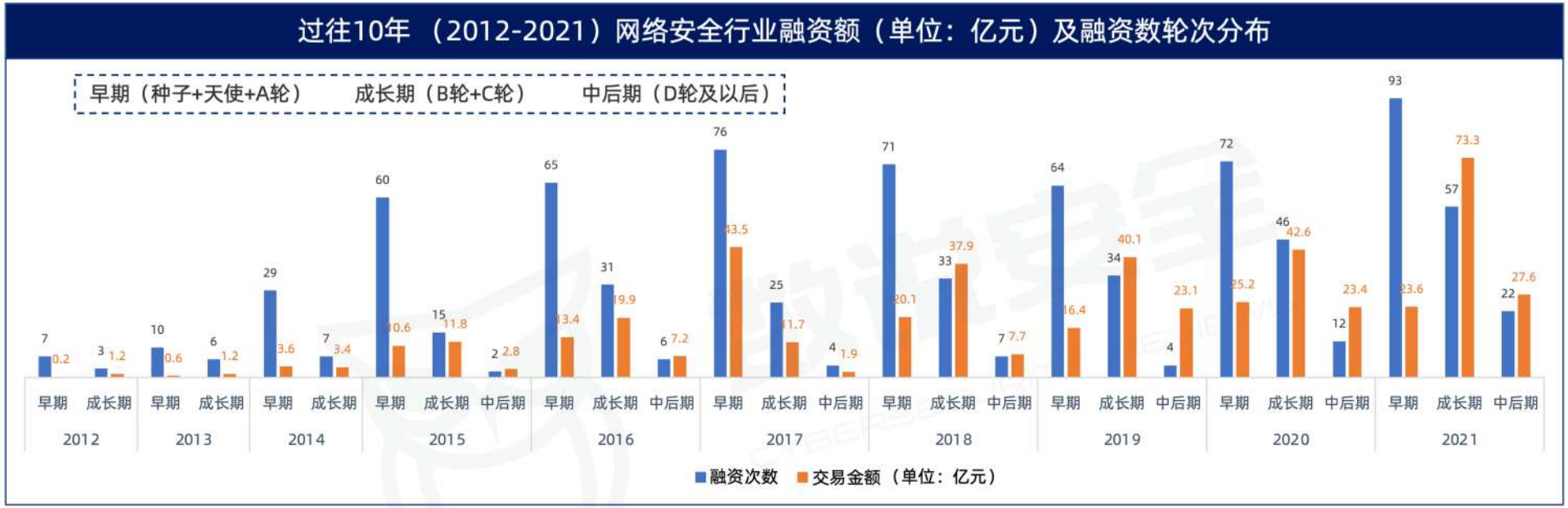
早期（种子+天使+A轮）　成长期（B轮+C轮）　中后期（D轮及以后）

2021各赛道融资额分布

Source：Annual reports of listed companies, prospectuses of proposed listed companies and other public information, Cybersecurity Reviews

China Cybersecurity Industry Financing Overview 2012-2021

Source: Cybersecurity Reviews



① The cybersecurity industry continues to be bullish, with both the amount and number of funding rounds hitting new highs in 2021.

② The number of funding rounds in FY21 increased year-on-year - 29.1% for early-stage projects, 23.9% for long-term projects and 83% for mid- to late-stage projects; except for early-stage projects, the growth rates of funding for long-term and mid- to late-stage projects were 72% and 17.9% respectively.

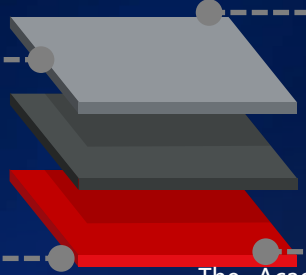
③ The number of early-stage projects raising funds increased, the total amount raised fell by 6.34% and the average single funding amount fell by 28.57% compared to 20 years. In addition to some star-studded start-up teams being sought after by investors, more start-up projects chose to lower their expectations for quick financing in order to survive and gain growth.

④ The financing amount of late-stage projects has increased to build up strength for industry consolidation; at the same time, the single financing amount has decreased due to the problems faced in matching the primary and secondary markets, down 35.89% year-on-year in 2021.

Cybersecurity Professionals is the foundation of industry development

The Current Training Situation of cybersecurity Professionals

China's cyber security education is at an initial stage



2019
42 universities set up cyberspace security academies or cyberspace security research institutes

2021
215 universities set up 287 cyber security majors, including 140 in information security and 81 in cyberspace security

2017
Issuing the "Model Project Management Approach for the Construction of a First-class Cybersecurity Academy

2015
The Academic Degrees Committee of the State Council and the Ministry of Education have established a first-level discipline of cyberspace security under the discipline of engineering

The CISP personnel qualification business of China Information Security Assessment Centre has been growing at a rate of more than 50% per year in recent years and has trained tens of thousands of information security professionals.

Huge shortage of cyber security professionals

Only 30,667 information security graduates have been trained in the last 3 years from 2017-2019

The current total shortage of cyber security manpower exceeds 1 million, with an annual incremental increase of 15,000, and the supply and demand is very unbalanced

In 2016, university academic education trained only about 8,000 graduates in cyber security-related majors (undergraduate and doctoral), with rapid growth to about 24,000 of vocational colleges in 2021

Four trends of the cybersecurity industry

Domesticizing

Under the international background, localization is the basic guarantee of cybersecurity and a reliable support for digital transformation

Segmentation

cybersecurity is deeply integrated with industry business needs, and scenario-based security solutions serve industry segmentation and digital development

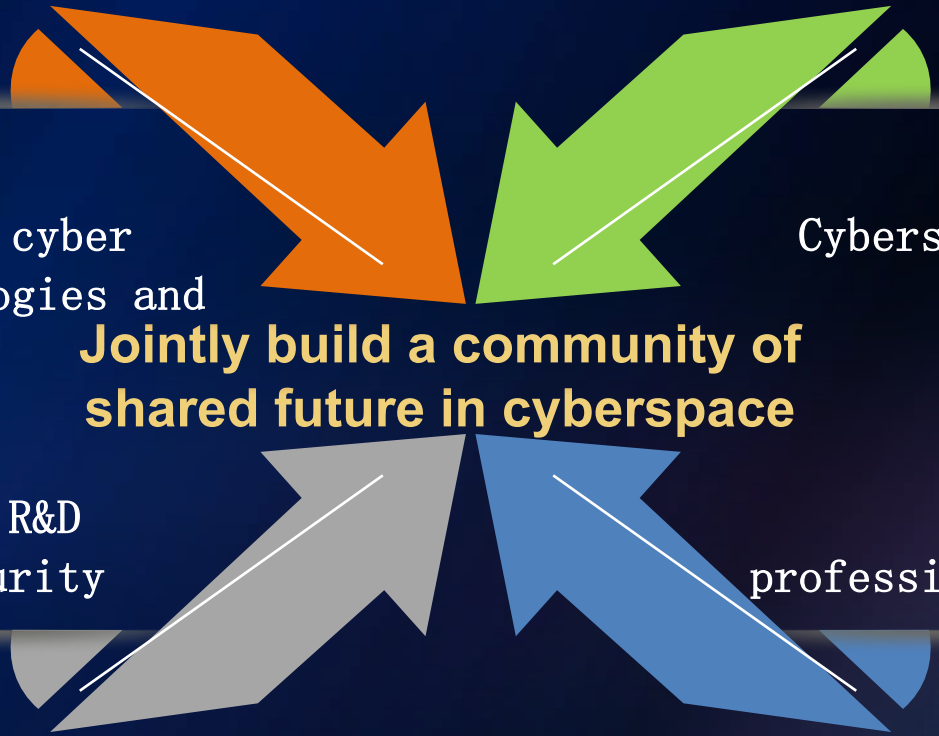
Intelligentizing

The development of technology makes it possible to intelligentize cybersecurity , and the security efficiency will be further improved

Service-based

The essence of cybersecurity is the confrontation between people, and product toolization and delivery services are conducive to improving cybersecurity benefits

Win-Win Cooperation



01

Collaboration on cyber security technologies and products

02

Cybersecurity market cooperation

Jointly build a community of shared future in cyberspace

03

Collaboration on R&D of new cyber security technologies

04

Cybersecurity professionals training cooperation

Thanks!