Analysis on the Competitiveness of 360 Government-enterprise Security Business

Haochen Liu*

Department of Management and Economics, Tianjin University, China

*Corresponding author: liuhaochen_@tju.edu.cn

Keywords: Qihoo 360, Government and Enterprise Security, Competitiveness Analysis.

Abstract: The rapid development of the Internet in China has brought substantial economic benefits and brought many problems in network security. Especially in recent years, China has attached great importance to national security, which has raised network security to the level of national strategy. This paper uses SWOT analysis, Porter's five forces model, and PEST analysis. It mainly analyzes the business competitiveness of the newly established Government-enterprise Security Group after separating the former 360 enterprise security group from the parent company Qihoo 360. The data come from academic papers on network security companies, company annual reports, securities financial reports, etc. At the same time, combined with the relevant knowledge of network security, the research is not confined to the macro level. Through analysis, the market competitiveness of the Government-enterprise Security Group belongs to the first echelon in China and has made significant contributions to the cause of China's national network security. However, efforts are still needed in the international market. This is mainly because the technical level is relatively backward or even controlled by others, and the structure of domestic security products is quite different from that of the international ones. This study also provides references and some suggestions for developing domestic security enterprises in the future.

1. Introduction

1.1 Research background

With the adjustment of national policy and the frequent occurrence of network attacks today, network security and information security have become a hot spot in recent years. As early as more than ten years ago, with the rapid development of China's Internet and the explosive growth of the number of Internet users, the personal network security business has become a hot spot at that time. Qihoo 360 Company seized these opportunities. With the subversive business model, the profit model of free personal security services and charging for value-added Internet services has defeated many traditional companies that buy security softwares [3]. Nevertheless, at this time, most large enterprises are still importing foreign security products such as Symantec and McAfee. The Ministry of Information Industry saw the drawbacks and ordered domestic security products to replace imported products. At this time, the former 360 Enterprise Security Group was established. Today, the personal security business market is saturated. However, government agencies and large enterprises have been repeatedly attacked. Therefore, the Government-enterprise security business has become a new outlet and has also become the direction of transformation of many security enterprises. The former 360 enterprise security group also separated from Qihoo 360 and became Qi Anxin independently. Zhou Hongyi, president of Qihoo 360, was determined to rebuild the Government-enterprise security business team and established Government-enterprise Security Group. He said he wanted to "be a 360 beyond 360."

1.2 Research significance

This paper focuses on the competitiveness of the government and enterprise security business of Qihoo 360, which started with the TOC business in the era of TOB and TOG business. As one of the

leading enterprises in the security business, Qihoo 360 has maintained its competitive advantage by cooperating with foreign companies or acquiring more advanced technology since its establishment in 2005. However, with the development of society, the company's problems such as too single revenue model, weak revenue growth of Internet advertising business caused by the disappearance of demographic dividend, and lack of core technology have been exposed. These problems need to be improved urgently, so Qihoo 360 is determined to independently develop security technology and transform it into the direction of government and enterprise security at the same time. At the same time, network security is in line with the country's needs, and other enterprises can better develop their own security business by understanding the advantages of Qihoo 360 to serve society and the country better.

2. Use PEST to analyze the external environment of the company

2.1 Political

In 2015, China put forward the concept of "sovereignty over cyber security." In 2016, the Cyber Security Law was promulgated, which clarified the principle of sovereignty over cyber security, required the establishment of a security protection system for critical information infrastructure, and successively promulgated a series of supporting documents such as the Regulations on Hierarchical Protection and the Regulations on Hierarchical Protection 2.0 [12]. This virtually makes government departments and enterprises pay more attention to network security; otherwise, if the personal information of an enterprise's users is leaked or even sold publicly, the enterprise should also bear the corresponding legal responsibility.

In the 14th Five-Year Plan for Network Security issued in 2021 and the forthcoming Action Plan for Network Security Industry, it is further clarified that the proportion of government and public enterprises and institutions investing in network security should not be less than 10% [22]. In the past, few enterprises invested in the security industry because of its high investment and low return. Therefore, the rigid policy regulations help security companies get more customers and promote the company's product development and updating to meet the needs of the government and enterprise market.

2.2 Economical

2.2.1 China's domestic cyber security market is on an upward trend

In 2020, the scale of China's network security industry reached 172.93 billion yuan, an increase of 10.6% compared with 2019. In 2021, the market recovers rapidly, and the industry scale is expected to be about 200.25 billion yuan, with a growth rate of about 15.8%. In the next three years after 2021, the annual compound growth rate is expected to reach 20%, more than twice the global growth rate [12]. Continued expansion of the market size can attract investment, increase the development space of security companies, and bring them more significant revenue and opportunities. It can also enable Tencent, Baidu, and Qihoo 360, an Internet company with multiple core businesses, to shift its focus or transformation to the network security business.

2.2.2 There are many segments in the security market, and any enterprise cannot monopolize the whole industry

The whole security industry is subdivided into 13 industries and up to 106 secondary industries. There are more than 300 manufacturers, and each has its own leading products [17]. For example, Anheng Information Company is far less competitive than Qi Anxin in terms of volume and overall market competitiveness. 360 Government and Enterprise Security Group is deeply convinced of this industry giant, but it is the leading company in database auditing and data desensitization in the field of subdivision and has been well received by customers. On the contrary, although the overall strengths of Qihoo 360's Government-enterprise Security Group is powerful. However, the competitiveness of

products under the category of security detection is not strong, such as network security audit and traffic analysis.

2.2.3 Lack of international market for domestic security companies

Fortinet, a giant international network security company, has nearly 60% of its revenue coming from the international market. On the contrary, the proportion of Chinese enterprises in the international market is relatively low, such as less than 3%, and the customers are basically relatively backward countries and regions [7]. The lack of international market leads enterprises to compete only in the domestic market, which is not conducive to the formation of a benign competitive environment in the long run. From a technical point of view, the lack of international market for domestic security companies reflects that the technology of domestic security companies has no advantages, and the product characteristics and advantages are not obvious. Therefore, only by opening up the international market and competing with the giants of international network security companies can the technical level and business ability of domestic companies be improved.

2.2.4 The structure of the domestic security market is different from that of the international security market

In 2020, the international security market accounted for nearly 45% of security services, 38% of software and 17% of hardware [7]. China, on the contrary, security hardware accounted for 47%, services for 32% and software for 21% in 2020. [7] However, compared with previous years, it has been greatly improved. One of the reasons for the low proportion of security services in the Chinese market is that the level of technical personnel in security services is uneven, and the demand of customers is becoming higher and higher. For example, for penetration testing of enterprise websites, many companies' services only stop at scanning websites with vulnerability tools. Detect whether there are common vulnerabilities. Customers want to know whether the existing vulnerabilities have the opportunities to be exploited by hackers or even penetrate into the enterprise's intranet. It is further hoped that the service personnel will give detailed vulnerability information and specific solutions. Another reason is that security services do not have a rigid pricing standard like security hardware. Such as the capacity and performance of the firewall, the detection capability and detection strategy of the intrusion detection system. The reason for the lowest proportion of security software is likely to be the prevalence of pirated software in the Chinese market.

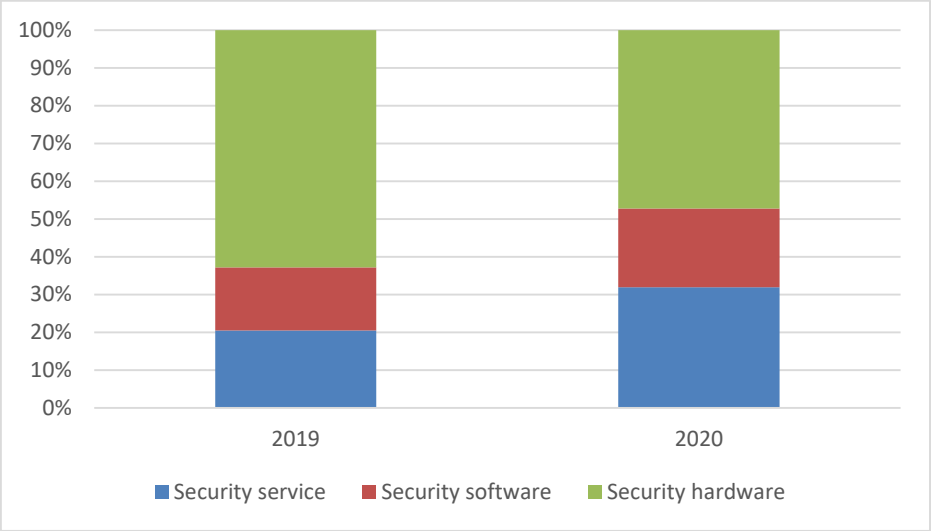

Figure 1. The structure of Chinese network security market [7]

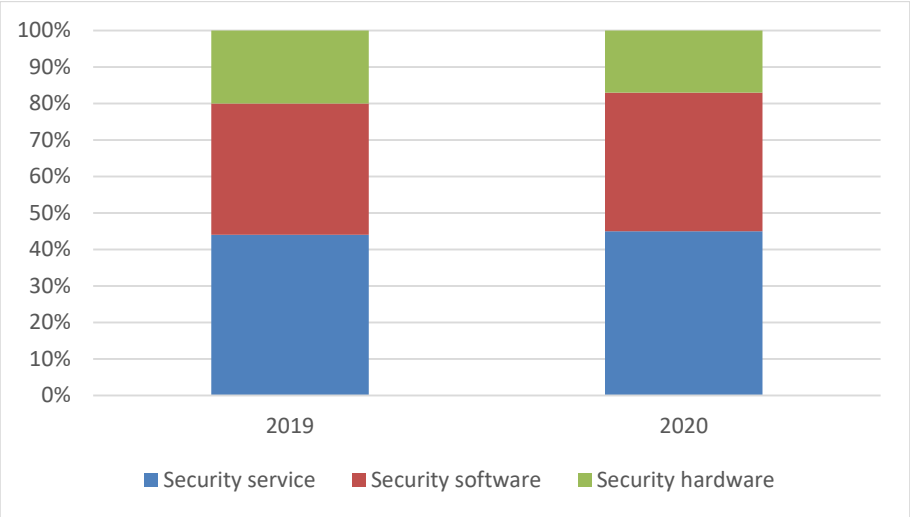

Figure 2. The structure of worldwide network security market [7]

2.3 Social

2.3.1 Small and medium-sized enterprises are the main customers

According to the data given by the vice minister of the Ministry of Industry and Information Technology, the number of Chinese enterprises has reached 46 million in 2021, of which more than 99% are small and medium-sized enterprises [22]. The size of medium-sized enterprises is generally 300-1000 people, and 47.44% of medium-sized enterprises have deployed network security products, an increase of 130.40% over 2019 [17]. Small and medium-sized enterprises generally purchase security services because of their small size and weak financial capacity. Such as training its employees in cyber security and purchasing cyber security managed services (MSS). Or buy unified threat management appliances that include firewalls, intrusion prevention, and intrusion detection systems.

2.3.2 Increasing Digitalization of Chinese Society

The scale of digital economy has reached 31.3 trillion-yuan, accounting for 34.8% of Chinese GDP. At the same time, the growth rate was 9.4%, twice that of the United States. [22] Online shopping alone has a transaction volume of 10 trillion yuan, such a huge amount of data and transaction records will naturally lead to data security issues. At present, most commercial platforms will record the preferences of customers to achieve personalized services, so these data with potential commercial value will become the target of attack and theft. Further, the amount of these data is large and often interrelated, which can obtain a large amount of practical information with a small number of attacks. Therefore, it will naturally become the target of many hackers.

E-government is also on the rise. As of March 2020, the number of online government users in China has reached 694 million [22]. By doing so, the government has facilitated the lives of the public, but it has also increased the risk of citizens' personal information being leaked. Some malicious software has certain data upload and monitoring functions, which can track the user's location and steal sensitive information. For example, the citizen's name, contact information, home address and even ID number. How to store and protect these massive data is a challenge.

2.3.3 The situation facing China's national network security is still grim

The number of tampered government websites in China was 515, 138.4% over 2018. The number of government websites implanted with backdoors reached 177, an increase of 6.4% over the end of 2018[22]. Targeted threat attacks (APT) around the military industry are increasingly frequent and highly targeted, while the aviation and shipbuilding industry is a crucial area of attack, and more than 30 APT spy organizations have been found abroad to attack China for a long time [16]. It is not difficult to see that China's cyber security threats are still severe. On the one hand, government websites are

implanted with backdoors so that attackers can access and modify them as administrators at any time to achieve their goals.

On the other hand, most of the targets attacked by APT are essential industries related to the country's fundamentals. From the "orientation," we can see that the attacker's purpose is powerful. Usually, the attacker is a top-notch organization with a clear division of labor and a clear purpose. He keeps an eye on critical departments for a long time, collects intelligence, obtains essential secrets, and lurks for a long time. The attack lasts for several years or even more. More importantly, attackers usually do not attack the target directly but use a third party as a springboard to attack the target. This makes it challenging to find the attack source, which is why APTs are challenging to defend against. In the fight against APT organizations, since 2011, Qihoo 360 has been assisting the government, military industry, scientific research, finance, and other vital units to defend against cyber-espionage attacks explicitly targeting the mainland of China. The number of APT reports issued by 360 Government and Enterprise Security Group is the first in the world, and the number of APT attacks launched is the third in the world. A total of 46 overseas APT organizations attacking China have been monitored.

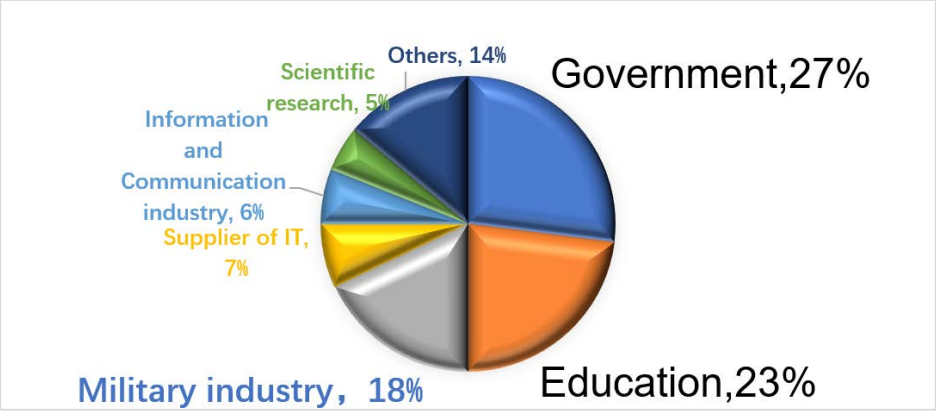

Figure 3. The aim of APT attackers, 2019 [16]

2.4 Technological

2.4.1 Network security products and their trends

In terms of how to deploy products, security products can be divided into six basic security areas: endpoint security, network and infrastructure security, application security, data security, identity and access management, and security management. The network security market can be divided into three sub-markets: security hardware, security software and security services [12]. With the innovation of technology, the demand for overall security products shows a trend of evolution from hardware installation of a single device to software system platform of multiple devices, and then to a set of security solutions. That is to say, the company can not only consider how to do one or several security products well. Instead, they should have the ability to give customers a complete set of solutions under different backgrounds and needs.

2.4.2 Changes in Internet communication protocols

With the rapid development of the Internet this year, more and more devices are connected. The fourth-generation communication protocol (IPV4), which has been released since 1981, can no longer meet the actual needs due to the limited number of addresses [18]. So, the sixth generation Internet (IPV6) has come into people's vision. Its address length is 128 bits, theoretically available—IP addresses. Because the number of addresses is almost unlimited, making it possible for everything to be connected to the Internet. Every object can be assigned to an address and connected to the network. At the same time, it is almost impossible to find potential and attackable objects by simply traversing and scanning within a network segment. Scanning and occupying a certain number of hosts with loose defense is the basis of launching DDOS attacks, and the application of IPV6 protocol undoubtedly increases the cost of DDOS attacks.

However, the risks in the other four layers, except for the IPv4 network, still exist in the IPv6 network [19]. That is to say, although security threats based on scanning to find flaws are improved, attacks against the transport layer, such as sniffing, are not significantly improved because packets are still unencrypted by default. Alternatively, forge its physical address (MAC address) in the data link layer to realize the access of unauthorized terminals. Based on the above analysis, the traditional DDOS attack may be weakened by the increase of its attack cost, but once the hacker uses some means to escape the interception of the target firewall or the detection of the intrusion detection system to control a certain number of hosts, it can still be achieved. Therefore, network security companies can allocate part of their investment in the anti-DDOS business to firewalls or intrusion detection systems.

2.4.3 Application of new technology

Big data technology, Internet of things technology, and artificial intelligence have been widely used. These technologies bring new security problems and help the development of network security technology. In the big data scenario and the application of artificial intelligence, the processing and collection of user data become ubiquitous [24]. If not correctly applied and managed, the risk of personal information leakage can be further increased. In April 2020s, Osan American cloud backup provider exposed the records of more than 135 million online customers. In September of the same year, the Microsoft Bing application database was leaked, and more than 100 million search records were intercepted. Similarly, the Internet of Things technology can improve automation, thus facilitating people's lives. However, all kinds of terminal access are also likely to be used by hackers, such as the home router infection cannot usually access the Internet, camera intrusion leads to private life exposure, etc.

The application of new technology also promotes the further development of network security. Artificial intelligence is playing an increasingly important role in the configuration of active security protection policies and has also made many attempts and achieved good results in intrusion detection, detection, and blocking of malware and viruses [14]. Big data analysis and detection technology can also improve the detection and discovery ability of threats and attacks and establish security models so that machines can learn and improve themselves to deal with new threats intelligently.

3. SWOT Analysis of Qihoo 360

3.1 Strengths

3.1.1 Qihoo 360 has many safeties technicians

The company has the largest team of security experts in the Eastern Hemisphere. Through 15 years of continuous recruitment, training, precipitation, and accumulation, the team has rich experience in actual combat attack on defense and can quickly respond to and analyze advanced threats. 360 has more than ten security expert teams representing the world's top technical level, with more than 3,800 security expert teams. The security elite team has more than 200 people, and in 2020, a total of 13 experts from 360 were honored on the "MSRC Global Most Valuable Security Elite List"[10]. Excellent technicians are the core of the security company, which ensures the high-cost performance and reliability of the company's business. At the same time, it can also contribute to the company's technological innovation.

3.1.2 The network security industry has strong sustainability and Qihoo 360 is developing rapidly

There is a consensus in the field of network security that there is no permanent and absolute security. Due to the vulnerabilities of operating systems, databases, network protocols, etc., and the increasing number of their functions, the corresponding security vulnerabilities will also increase. The famous 0-day vulnerability is to exploit known vulnerabilities that have not yet been solved or patched. Therefore, it can only be prevented by various means. Therefore, the income of security companies can also be guaranteed, and Government-enterprise Security Group has developed rapidly since their

establishment. In 2021, the company's government and enterprise security business revenue increased by 322% year-on-year, and the half-year revenue scale has exceeded the whole year of 2020[20].

3.1.3 Qihoo 360 has rich business experience

The company has been involved in network security for a long time. In 2005, founder Zhou Hongyi founded Qihoo 360. Today, Government-enterprise Security Group has announced that Government-enterprise security has entered the "3.0 era". As early as the emergence of national-level security products such as 360 Security Guard, 360 Group has set foot in the Government-enterprise market and developed the security software 360 Security Guard Enterprise Edition for Government-enterprise units, known as "1. Since then, the company has begun to provide professional security products and services to government and enterprise users, known as the "2.0 era"[11]. At present, the company has cooperated with 78% of ministries, 80% of central enterprises, and 82% of large banks. As well millions of small and medium-sized enterprises have carried out cooperation in network security [21]. At the same time, Qihoo 360 can further enhance the team's practical experience and business ability through cooperation with government and enterprise units. It can also win more development opportunities and rising space for enterprises.

Table 1. Qihoo 360's occupational history

(Sources from: Official website of Qihoo360)

Service object	Service items	Transaction amount	Time	The stage in which
Microsoft Corporation	Help find and fix vulnerabilities in a range of Microsoft products	Microsoft Official Six Global Public Acknowledgements, an unknown amount of RMB	2008-2012	Government and enterprise security "1.0 era"
enterprise users	Release 360 Security Guard Enterprise Edition	Security services are free for users, 0 RMB	2011	Government and enterprise security "1.0 era"
enterprise users	360 Enterprise Security Group officially announced its establishment to provide enterprises with security solutions and services based on "data-driven security"	0 RMB	May 2015	The "2.0" Era of Government and Enterprise Security
National government departments	Capture the advanced attack group Blue Treasure Mushroom.	An unknown amount of RMB	April 2018	The "2.0" Era of Government and Enterprise Security
Chongqing Hechuan District Government	Phase I Project of 360Network Security Collaborative Innovation Industrial Park in Hechuan District, Chongqing	240 million RMB	June 2019	The "2.0" Era of Government and Enterprise Security
government and enterprise users	360 Releases Government and Enterprise Security Strategy 3.0	0 RMB	September 2019	The "3.0" Era of Government and Enterprise Security
Tianjin Municipal Government	Emergency Management Informatization (Phase I) Project of Tianjin Emergency Management Bureau	120 million RMB	October 2019	The "3.0" Era of Government and Enterprise Security
Changsha Judicial Department	Changsha "Digital Rule of Law, Intelligent Justice" Informatization Project	42.81 million RMB	October 2020	The "3.0" Era of Government and Enterprise Security

3.1.4 The high reputation of the company

In the Internet era, users are the most valuable resources. The biggest capital of Internet enterprises is not the size and tangible assets of the company, but the customer resources, which are the core capital [4]. Qihoo 360, the parent company of 360 Government and Enterprise Security Group, has a high reputation in the hearts of the public, which improves the social prestige of 360 Government and Enterprise Security and helps senior managers of government and enterprise to recognize it. At the same time, a large part of the funds needed for the development of Government-enterprise Security Group come from Qihoo 360, which attracts users through free personal security products and then turns traffic into cash. According to the annual report of Qihoo 360 in 2020, the revenue of Internet advertising and Internet value-added services amounted to more than 860-million-yuan, accounting for nearly 75% of the company's total revenue [10].

3.2 Weaknesses

3.2.1 Fierce competition in the security market

Homogeneous competition in the security market is serious, including traditional software companies such as Qi Anxin, Deeply Convinced and Qixing Chen, as well as Internet companies such as Tencent, which started with social software. The competition also mainly revolves around the three aspects of security hardware, security software and security services. Although the market seems not small, there are many very competitive competitors. Take the firewall that major companies will basically deploy as an example, Huawei has done a good job in this respect, and Qi Anxin is deeply convinced [17].

3.2.2 The government and enterprise security business require a high level of the company

Unlike the main personal market before 360, the market demand of government and enterprises is fragmented, and the demand of each enterprise cannot be the same. For example, the State Grid only needs to solve its terminal security problems, while Wuzhong District of Suzhou needs to build a complete security defense system for its e-government network [10]. This requires companies to design products and solutions according to the characteristics of customers, which are customized rather than a single model like TOC products. Therefore, it is a challenge in terms of technical level and service capability.

3.3 Opportunities

3.3.1 Introduction of state-owned capital

In January 2021, 360 announced the implementation of the non-public A-share issuance plan, which issued 381,308,030 shares for 12.93 yuan per share, targeting 17 companies and raising a total of 4.93 billion yuan. Part of the shareholders introduced by 360 is state-owned background, among which China Life and Zhongfa No.1 are large state-owned institutions [13]. On the one hand, the introduction of state-owned capital can prevent the breakdown of the capital chain caused by the blind investment of enterprise managers, on the other hand, it can also increase the confidence of other private investors and enterprises in the company [23]. Because of the company's nature and income structure, Qihoo 360 is an Internet company, and its main business is not just security. It also invests in Internet advertising services, smart hardware, games and automotive markets. In 2020, the safety industry accounted for only 7% of the company's total revenue. Therefore, the income of other businesses will greatly affect the investment of the security industry. Poor performance in one of them is likely to strain the company's finances, causing banks to refuse loans and investors to withdraw their capital. To sum up, the investment of state-owned capital is undoubtedly to help Qihoo 360 develop its security business steadily on the premise of ensuring sufficient funds while deepening the cooperation between the company and local governments.

3.3.2 The company is closely linked with the state organs and will receive policy support

360 has made great contributions to national network security. Many of China's infrastructure, some state units, including the military and public security systems, have played a huge role in ensuring their network security. Qihoo 360 has also responded positively to the call of the state to delist from the US stock market and return to the domestic market [9]. Since then, the company has participated in major security activities such as the two sessions, the 19th National Congress, the 93 military parades, the "The Belt and Road Initiative" Summit, the G20, the BRICS Conference, APEC and the 70th-anniversary celebration, and continued to play an important role in national security and national defense security-related work.

3.4 Threatens

3.4.1 The company lacks partners

In 2010, it clashed with several Internet companies, including Tencent and Baidu, which was called the "3Q War". Several Internet companies announced that their products were incompatible with those of Qihoo 360 Technology Co., Ltd. and were eventually mediated by the Ministry of Industry and Information Technology. However, rising, Kingsoft and other veteran anti-virus software manufacturers have been Qihoo 360 market and legal acts of litigation [2]. The "3Q" war has pitted Qihoo 360 against two giant companies on China's Internet, and Qihoo 360 has naturally lost the support of many people. It has even been labeled as "China's largest rogue software manufacturing company". At the same time, it also makes the company lack partners, such as Qihoo 360, which once proposed to buy Rising, but was flatly rejected by Rising. Among the strategic partners of Government-enterprise Security Group, there are few competitive domestic Internet companies and anti-virus software companies.

3.4.2 Impact of Separation of Subsidiaries

Due to the separation of 360 Enterprise Security Company from its parent company, Qi Anxin was established, resulting in a large brain drain, and the profits of shareholders were also reduced. The stock price of Qihoo 360, the parent company, continued to fall, from about 17 yuan per share in 2019 to about 12 yuan per share at the end of 2021[10]. It has a negative impact on the company's financing. At the same time, Qi Anxin has reached a strategic partnership with Tencent and Huawei, which may lead to the disclosure of trade secrets. In addition, the two sides are also competing in the network security market, and the Government-enterprise Security Group has an advantage in application security and terminal management products. Qi Anxin is better in data management and safety monitoring.

3.4.3 There is a gap between the technical level and that of the top international security companies

360 Government-enterprise security group lacks core technology, and there is still a gap with the international top level. Fundamentally speaking, the basic theory of network security and computer hardware infrastructure are almost all original creations of Europe and the United States, and European and American countries have the advantage of technological first mover [7]. For example, there is a foreign company named Cloudflare, which mainly does firewall and anti-DDOS business, which is also the strengths of 360 Government and Enterprise Security Group. But Cloudflare's technology is advanced because it can make websites faster, resist most network attacks, intelligently filter suspicious traffic and hide real website IP addresses. In this respect, there is a gap between the Government-enterprise Security Group and it. In addition, on May 23, 2020, Qihoo 360 was officially added to the "entity list" by the U.S. Department of Commerce to restrict its acquisition of technology and products involving U.S. technology. This makes it more urgent and important for the company to independently develop core technologies.

Table 2. SWOT Analysis of Qihoo 360

Internal environment analysis / External Environment analysis	Strengths Qihoo 360 has many safety technicians. The network security industry has strong sustainability and Qihoo 360 is developing rapidly. Qihoo 360 has rich business experience. The high reputation of the company	Weaknesses Fierce competition in the security market. The company is closely linked with the state organs and will receive policy support.
Opportunities Introduction of state-owned capital The company is closely linked with the state organs and will receive policy support.	Strength's opportunities strategy (S.O) Through its influence and technical advantages in China, it can lead the implementation of several safety projects and further enhance the experience and prestige of its team.	Strengths threats strategy (S. T) To provide support for the construction of national network security, on the one hand, to enhance the company's image and market share. On the other hand, it can also be recognized by the state.
Threatens The company lacks partners Impact of Separation of Subsidiaries There is a gap between the technical level and that of the top international security companies	Strengths threatens strategy (S.T) Analyze the gap with foreign security companies, and then increase R & D investment by virtue of their strong financial advantages, and reward technicians and R & D personnel who have made outstanding contributions.	Weaknesses threatens strategy (W.T) Qihoo 360 should actively seek partners, such as joining hands with tinder, which equally has an advantage in terminal security. At the same time, we should adapt to the market demand, take customers as the center, and not seize the market through viral marketing as in the PC era.

4. Market competitiveness of the company's products

4.1 Bargaining Power of the Buyer

Security business is one of the main revenue sources of Qihoo 360, with a turnover of 612 million yuan in 2020. At the same time, it is also the transformation direction of the company, that is, from the individual user market to the enterprise user market. [1]Therefore, buyers will have more say in bargaining. At the same time, government and enterprise customers can buy the products of many companies by virtue of their economic strengths, which makes the product competitiveness of 360 companies decline. At the same time, government and enterprise customers obviously have greater bargaining rights because of their special attributes.

4.2 Threat of alternatives

Qihoo 360 has a formidable dynamic innovation capability, and the products developed have the characteristics of micro-innovation [15]. The essence of network security is the confrontation between the offensive and defensive sides. Confrontation requires continuous operation and accumulation of capabilities. So, 360 has built a systematic centralized system to accumulate these offensive and defensive experiences, which is the security brain proposed by 360. The security brain not only contains multiple sets of analysis and diagnosis systems linked to various intelligence networks throughout the country, behind it is the 24-hour online support of the world's largest security database and the world's top security expert team. This product is used with other products of 360 company, and the security products of other companies are difficult to replace. The higher the value of resources, the higher the degree of scarcity, the more difficult it is for competitors to imitate, and the more

sustainable competitive advantage enterprises will gain [6]. Security brain is also an important tool for Government-enterprise Security Group to have a long-term competitive advantage.

4.3 Degree of competition among industry players

Table 3. The comparison of three leading enterprises of network security [22]

Company name	Number of R & D personnel	Proportion of R & D personnel to total employees	Total R & D investment	Operating income	Leading products
360 Government and Enterprise Security Group	4146	62.45%	2.871 billion RMB	808 million RMB	Almost all
Chi Anxin	2938	35.89%	1.228 billion RMB	4.16 billion RMB	Infrastructure protection, security operation management and terminal management
Convinced	Above 1600	40%	1.08 billion RMB	3.34 billion RMB	Infrastructure protection, application security testing services under application security, and bad information detection and filtering services under security detection and business security.

The above table selects the leading enterprises in network security, which are almost the same in terms of enterprise size and technology level, and are all enterprises invested by state-owned capital, belonging to the "national team" of China's network security. The data in the table are for 2020. The strong products are all from the 2021 China Network Security Product User Survey Report released by Ann in the new list.It is not difficult to find that Government-enterprise Security Group is more than the other two companies in terms of the number of R & D personnel, the proportion of total employees and the total R & D investment. However, the company's revenue situation in 2020 is not as optimistic as the other two companies. Maybe this is just the establishment of Government-enterprise Security Group. Even some products of the newly independent Qi Anxin still have the word "360" on their trademarks. As a result, the company's popularity is not high. However, with all kinds of efforts, 360 Government-enterprise security products have gained a dominant position in almost all segments of the network security market in 2021, which shows that 360 has a solid technical foundation. It has puissant R & D capability and sufficient funds to support it.

In contrast, Qi Anxin has a slight advantage in security hardware and security software, especially in security detection products. Deep conviction is more prominent in security services. Compared with Government-enterprise Security Groups, they only have certain advantages in partial subdivision of products.

5. Conclusions

5.1 key findings

By analyzing the external environment of 360 Government and Enterprise Security Group, the company's situation, and the market competitiveness of the company's products, this paper finds that the competitiveness of Qihoo 360's government and enterprise security business occupies a significant advantage in the domestic market due to its years of accumulated technical experience and recruited talents, including the income support of other leading business of the company and the good support

of national policies. However, there are still many potential competitors, and Qihoo 360 has some shortcomings, such as lack of partners, technology has not yet reached the top international level. At the same time, due to the late development of computer technology in China, As a result, Qihoo 360 has almost no international market because of its technological disadvantage, the different structure of the domestic network security market, and some political reasons. In the long run, this is not conducive to the healthy development of enterprises.

5.2 Research significance

The significance of this paper is to analyze the Government-enterprise security market, which is relatively blank in the research field. Most of the previous articles focused on analyzing how Qihoo 360 became more prominent and more substantial in the TOC market or the case of Qihoo 360's backdoor return to the A-share market. At the same time, it also gives other security companies or Internet companies with security businesses a reference for developers to develop the company's security business better and contribute to China's network security cause. The deficiency of this paper is that some specific data are not given, but only qualitative analysis is done. At the same time, it only focuses on the security business of Qihoo 360, an Internet company, but does not analyze the security business of Internet companies such as Tencent and Huawei.

References

[1] Wang Shiqi. Research on Profit Model of 360 Company [D]. Hebei University. 2021.

[2] Li Xiaomin. Research on Competitive Strategy of Qihoo 360 Technology Co., Ltd. [D]. Shandong University of Finance and Economics. 2016.

[3] Li Chongsen. Why does Qihoo 360 become one of the top four Internet companies? [J]. Manager, 2014, 02: 28 - 34.

[4] Guo Xinyu. Strategic Management of Internet Enterprises. China's high-tech enterprises. 2014 (16).

[5] Guo Chen Xiazi. Research on Competitive Strategy of Convinced Company [D]. Xinjiang University. 2019.

[6] Liu Jingya. Research on the Path of Internet Enterprises to Gain Sustainable Competitive Advantage-Taking Qihoo 360 as an Example [J]. Management Case Study and Review. 2016, 9 (01).

[7] Computer industry: Network security industry continues to boom [R]. Wuxi: Guolian Securities, 2021.

[8] Shi Lin. Qihoo 360's Competitive Strategy and Industry Impact Analysis [J]. Modern telecommunications technology. 2014, 44 (Z1).

[9] Yu Miao. Motivation Analysis of Qihoo 360 Delisting in the United States [D]. Shenyang University of Technology. 2018.

[10] 360 Company 2020 Annual Report [R]. Tianjin: Qihoo 360 Technology Co Ltd, 2020.

[11] Zhao Zhiyuan. 360 Government and Enterprise Security 3.0 Strategy [N]. Network Security and Informatization, 2019.10 (8).

[12] Computer Industry 2022 Annual Strategy: Where the Inflection Point Comes, the Golden Stone Opens [R]. Beijing: Cinda Securities, 2021.

[13] 360 (601360) Company In-depth Report [R]. Beijing: Capital Securities, 2021.

[14] Lei Xin. Future development trend of network information security. [J] CATV Technology. 2018 (08).

[15] Wenke Wang, Qilin Cao, Li Qin, Yan Zhang, Tianli Feng, Linyun Feng. Uncertain environment, dynamic innovation capabilities and innovation strategies: A case study on Qihoo 360 [J]. Computers in Human Behavior. (95) 2019.6: 284 - 294.

[16] 2020 Global Advanced Persistent Threat APT Research Report [R]. Tianjin: Qihoo 360 Technology Co Ltd, 2020.

[17] 2021 China Network Security Product User Survey Report [R]. Shanghai: Shanghai Anhe Information Technology Co., Ltd., 2021.

[18] Li Xinxu, Li Baochun. IPv6, Analysis of Internet Protocol [J]. Railway Computer Applications 2003, (06).

[19] Zhang Tao, Wang Huan, Zhou Zhongmou, Xiong Wei. Security Analysis of Internet Protocol Version 6 (IPv6). [J]. Jiangxi Electric Power. 2020, 44 (08).

[20] Revenue in the first three quarters of 360 was 8.539 billion yuan, an increase of 7.09 [N]. Economic Observer, 2021.11.01.

[21] He Jun. The revenue of 360 security business increased by 322 compared with the same period last year, and the revenue in the first half of this year exceeded the total of last year [N]. Securities Daily, 2021.9.1 (B03).

[22] The 45th Statistical Report on Internet Development in China [R]. Beijing: China Internet Network Information Center (CNNIC), 2020.

[23] Dong Xiaohong, Sun Wenxiang, Li Zhe. Can private enterprises alleviate financing constraints by introducing state-owned capital? [J]. Journal of Management, 2021, 34 (04).

[24] He L. Network security risks brought by the application of new technologies such. as big data, cloud computing and artificial intelligence [J]. China new communications, 2020, 22 (16): 155 - 156.1.