BASC WORKING PAPER SERIES

A CENTRALIZED CYBERSECURITY STRATEGY FOR TAIWAN

Hsini Huang
Tien-Shen Li

Working Paper 2018-08

BERKELEY APEC STUDY CENTER
552 Barrows Hall
University of California
Berkeley, California 94720-1950
September 2018

This paper is part of a project "Comparative Industrial Policy in the Cyber Security Industry: Policies, Drivers, and International Implications," organized by Vinod K. Aggarwal and Andrew Reddie of the Berkeley APEC Study Center and funded by the Center for Long-Term Cybersecurity at the University of California, Berkeley. The authors acknowledge valuable comments from Professor Vinod K. Aggarwal, Professor Naiyi Hsiao, and Andrew Reddie who helped to shape and edit this paper and support from the Center for Long-Term Cybersecurity, Institute of East Asian Studies, and BASC at UC Berkeley for hosting the "Comparative Industrial Policy in Cybersecurity" workshop series.

A Centralized Cybersecurity Policy for Taiwan
Hsini Huang and Tien-Shen Li
BASC Working Paper No. 2018-08

Abstract

Viewing cyber security as a matter of national security, the Taiwanese government established the National Information and Communication Security Taskforce (the Taskforce) in 2001 to actively implement ICT security infrastructure policies and strengthen national capacity against threats to the country's increasing cyber security issues. A series of national strategy programs and action plans followed the founding of the Taskforce and were carried out over the last fifteen years. Authorities in Taiwan are deliberating over the draft of "Information and Communication Management Act (ICM Act)" in response to the increasing awareness of potential malicious cyberattacks targeting the public and private sector. Under this Act, both government and non-government bodies will have to comply with the new legislation with the hope that the coded regulations and new management scheme will have a positive impact on enhancing national security and increasing the domestic market.

This article aims to provide a thorough review of the proposed national information security policies in Taiwan between 2001 and 2017, as well as deliver a case for the comparative study of industrial policies employed to bolster domestic cyber security markets.[1] By summarizing the government's industrial policy in developing a cyber security market and identifying key stakeholders involved in the policy-making process, we describe the major rationale and drivers behind the government's plan of action and aim to push for a more comprehensive understanding of the proposed policy tools used by the authorities to boost the development of the cyber security industry in Taiwan.

Hsini Huang[2]
Department of Political Science and Graduate Institute of Public Affairs
National Taiwan University
Taipei, Taiwan
hsinihuang@ntu.edu.tw

Tien-Shen Li
Department of Social and Public Affairs
University of Taipei
Taipei, Taiwan
ltsn0625@gmail.com

[1] Aggarwal and Reddie 2018, Theory chapter.

[2] Hsini Huang is an assistant professor of Public Affairs and Political Science at National Taiwan University. She received her PhD in the School of Public Policy at Georgia Institute of Technology in 2012. She has published articles in the Cambridge Journal of Regions, Economy and Society, Science and Public Policy, and Research Policy.

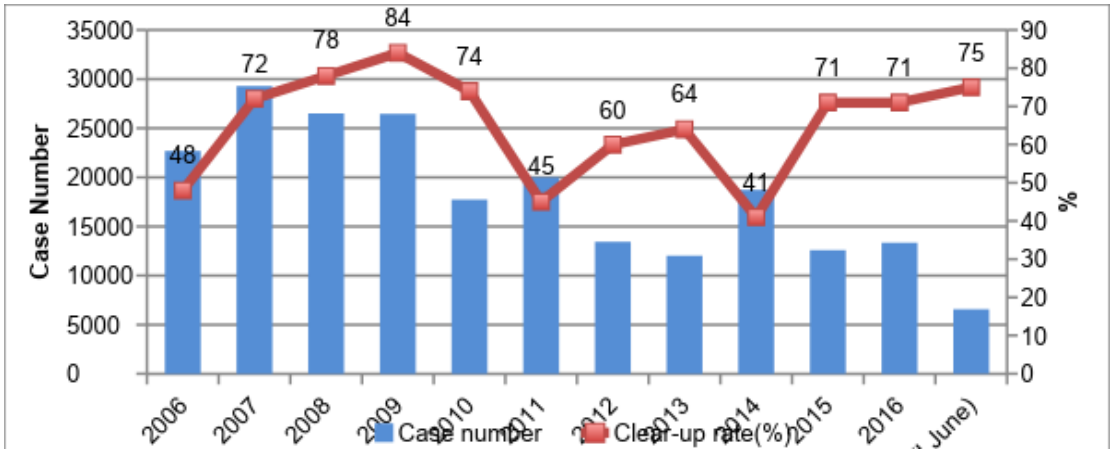
1. Background and the Cyber Security Industry in Taiwan

The rapid development of information and communication technology and the Internet of Things (IoTs) has dramatically increased cyber security challenges and their risks to everyday civilian life. For example, in July 2016, a multinational criminal ring conducted an ATM heist by implanting malware to withdraw about 2.6 million US dollars from dozens of machines belonging to the same computer networks of First Commercial Bank in Taiwan. Similar ATM malware heists occurred in Asian and European countries as well (ZDNet, November 22, 2016) . In order to strengthen Taiwan's cyber-security capacities, the Taiwanese government decided to create the Department of Cyber security (DCS) in August 2016 to serve as the strategic center for national information security.

Taiwan is among the most heavily attacked nations in East Asia when it comes to cyber attacks, behind China, Vietnam, and Japan due to its geographical location and its special political situation with China. According to the Taiwan News, there are on average more than 20 million cyber attacks targeting government websites in Taiwan everyday, mostly from China (Taiwan News, April 5, 2018). Cross-strait tension and lack of mutual cooperation has made it difficult to investigate transnational cyber-crimes (Chang 2012).

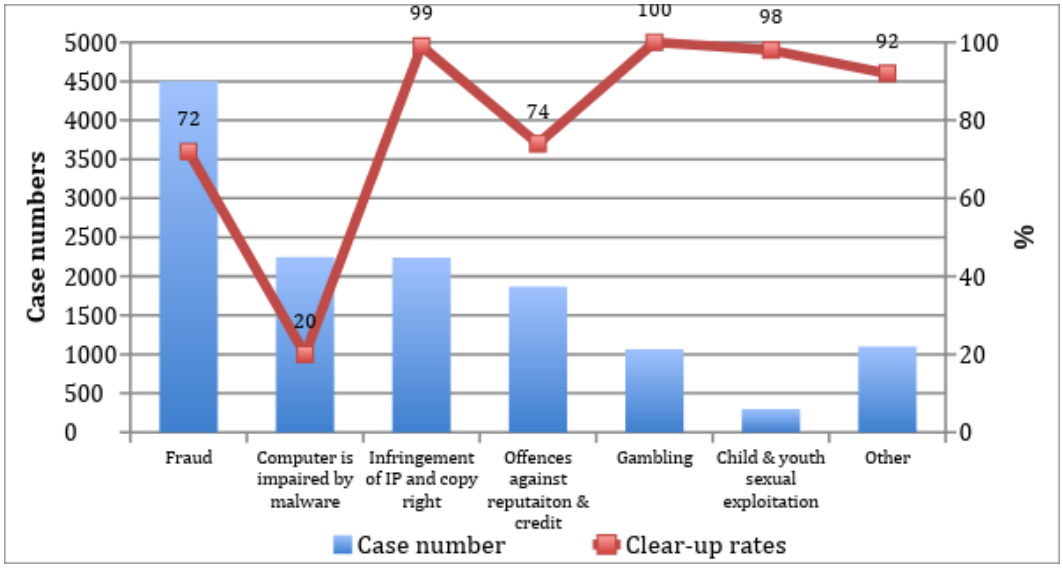
Information security, which is often used interchangeably with cyber security in Taiwan, has been a great concern since the use of Internet. Figure 1 shows that the case numbers of cybercrimes reported by National Police Agency have been fluctuating between 2006 and 2016. Although the number of cybercrime cases appears to have a downward trend, the National Policy Agency still reported over 13,000 cybercrime cases in 2016 alone. Breaking this figure down by types of cybercrime (Figure 2), the 2016 data showed that fraud (34%) is the most common type followed by malware attacks (17%), infringement of IP and copyright (17%), and attacks on reputation and credit (14%). Coming as no surprise, attacks using malware have the lowest clear-up rates (20%).

Figure 1 Cybercrime cases reported by the National Police Agency, 2006-2017 June



Source: NPA statistics (2006-2016) Available at: https://www.npa.gov.tw/NPAGip/wSite/lp?ctNode=12878&CtUnit=2646&BaseDSD=7&mp=1

Figure 2 Type of cybercrime and clear-up rates in 2016



Source: NPA statistics (2016)

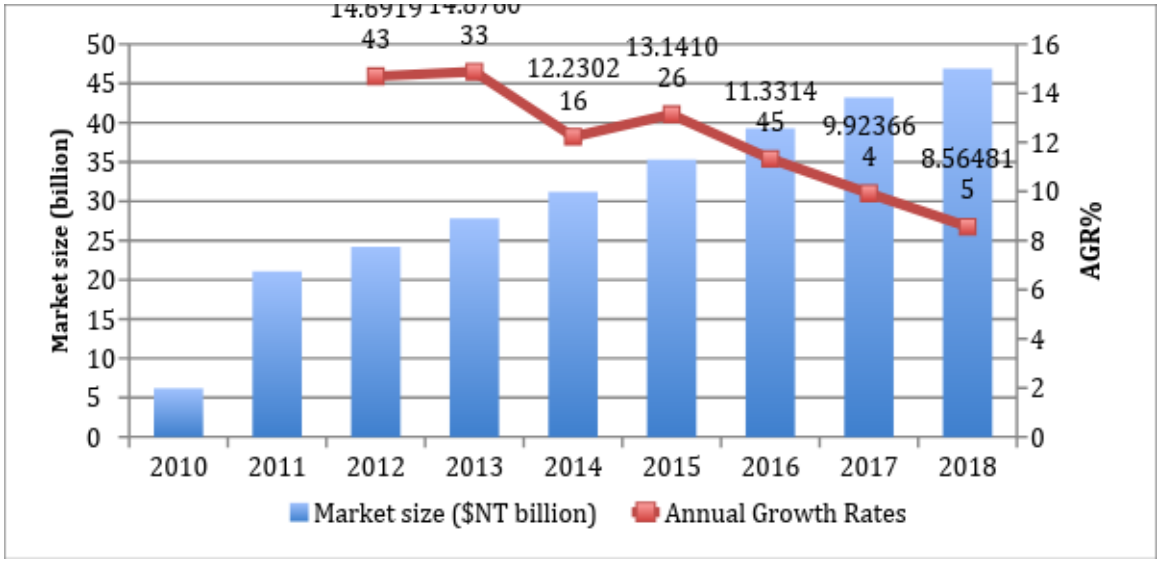
Regarding information and communication security as a matter of national security, President Tsai's government echoed in its defense policy that "cyber security is national security and the new Information Communication Electronic Force Command–ICEF–will help protect Taiwan's digital domain." Following President Tsai's inauguration in May 2016, the Ministry of National Defense (MND) announced that the administration would move forward with the establishment of a new military service command center for cyber security. Cyber security, along with aerospace and missiles, would be one of the three targeted fields in defense industrial policy working to meet national security and economic growth interests.

1.1 The Cyber Security Industry in Taiwan - Overview

With the rapid development of IoTs, the ICT-related security issues have become a big concern both in Taiwan and globally. The increasing threats of cybercrime and cyber-attacks make both private and public sectors aware of the risk and has resulted in them wanting to invest more in cyber security management. As a result, the information security market in Taiwan has expanded at an annual rate of 14% since 2011, increasing in scale from US$700 million to US$1.44 billion in 2017. The size of Taiwan's information security market is projected to continue to increase from 2015 to 2019 with an annual growth rate of 8.7% (As shown in Figure 3). However, domestic firms in the cybersecurity industry tend to be in small scale. According to a new release from the Department of Cyber Security, there are around 294 companies with a total of 8500

employees working in this sector in 2017. Eighty percent of the companies have less than 50 employees and focus on similar areas.

Figure 3 Size of information security market in Taiwan (2010-2018)



Source: National Strategy for Cybersecurity Development Program (2013) The market size and growth rates of year 2017 and 2018 are projected forecast numbers.

2. The State Policy and Stakeholder Analysis for the Cyber Security Industry

2.1 Overview

We begin this section by introducing the government's cybersecurity policies from the last fifteen years. In 2001, Taiwan's government, the Executive Yuan, approved the National Information and Communication Infrastructure Security (2001-2004) Mechanism Plan (the Phase 1 Mechanism Plan), a program to span over four years, from 2001 to 2004. Built upon the foundation of the phase 1 mechanism plan, the National Information and Communication Security Taskforce was established in 2001 and was in charge of implementing information security protection systems to all 3,713 major government agencies. Policy programs carried out from the phase 1 plan mostly emphasized the categorization of agencies by the cyber threat levels as well as the information security readiness across public sectors.

Between 2005 and 2008, the Executive Yuan continued to carry out a new National Information and Communication Infrastructure Security (2005-2008) Mechanism Plan (a so-called the Phase 2 Mechanism Plan). The primary policies were to 1) set up an accountability system by creating the Chief Information Security Officer (CISO) position

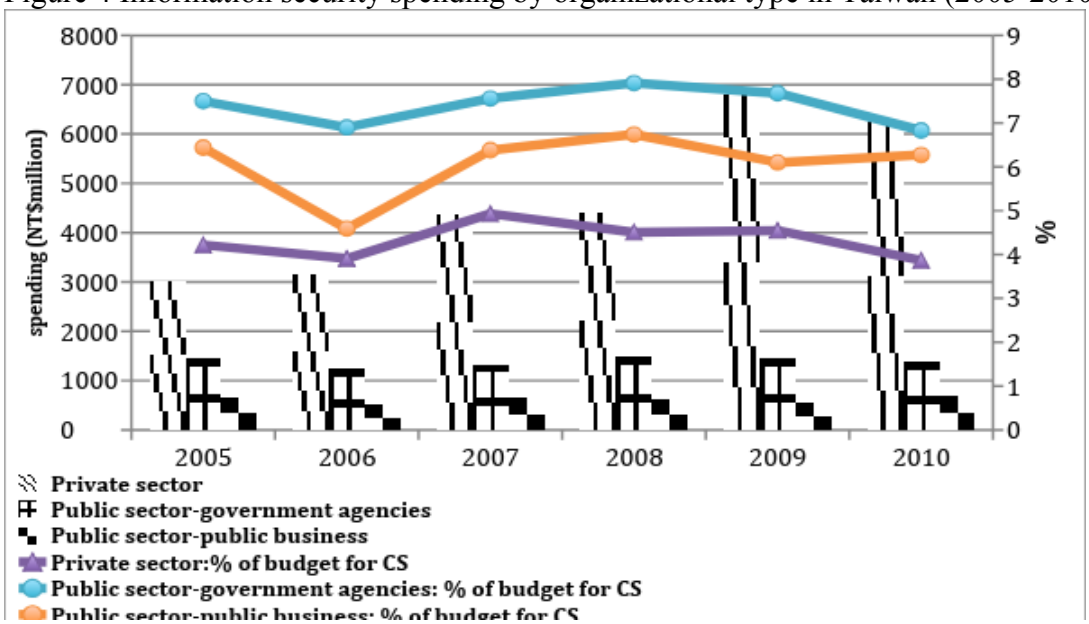
at each Ministry, and 2) establish the National-Security Operational Center (N-SOC) to actively improve information security surveillance, audits, and management.

To continue the development of cyber security protection and environment, the Executive Yuan, under the Ma Administration, approved the Phase 3 Development Program[3], which operated from 2009 to 2012. This phase of the policy program began to take "industrial development" into consideration. More than 20 action plans were implemented to assure the overall improvement of information security protection and investment not only for public agencies/business, but also for local enterprises. Another important milestone of legislation was the enforcement of the Personal Data Protection Act (PDPA) in 2012 and a modification of PDPA in 2015.

Interestingly, despite the efforts and actions taken by the government since 2001, the organization's spending on information security is unchanged. Figure 4, below, shows a level trend in terms of the total amount of information security spending for public sectors, including both government agencies and public business units between 2005 and 2010. For private organizations, while spending has increased, when it comes to the percentage of the budget for cyber security in comparison to total IT spending, there does not appear to be a rising trend either. Unfortunately, no further data is available beyond 2010 since the computer resource survey conducted by the Directorate-General of Budget, Accounting and Statistics was discontinued in 2011 due to a budget cut. Therefore, there is no evidence reflecting current security spending for the public sector and the percentage of budget for cyber security for all sectors following that point. However, by examining the data between 2005 and 2010, it is unlikely that the trend would go up immediately following 2011 during Phase 4 of the Develop Program (details of the phase 4 program will be introduced later). Future studies should further investigate the actual effects of those national policies and action plans.

[3] For the Phase 3 and Phase 4 national plan, the Executive Yuan changed the program name from National Information and Communication Infrastructure Security Mechanism Plan to the National Strategy for Cybersecurity Development Plan.

Figure 4 Information security spending by organizational type in Taiwan (2005-2010)



Source: Directorate-General of Budget, Accounting and Statistics, the Computer Resources Survey Report (2005-2010)[4]

Following the footprints of the previous three phases of the national plan, Phase 4 of the National Strategy for Cybersecurity Development Program (2013-2016) was carried out by the Executive Yuan which shifted the policy goals from intra-government security management towards inter-sectorial security management and some initial planning for cyber security industrial policies and development. This included 1) strengthening the technology capabilities of cyber security firms and research institutes and 2) expanding the human resources for cyber security by providing government-sponsored training and job-matching platform.

The National Information and Communication Security Office (NICSO[5]), Department of Cyber Security (DCS) and the National Communications Commission (NCC) are the three key agencies responsible for cyber security policies. Among them, DCS (formerly the Office of Information and Communication Security) is a newly established administrative department dedicated to lead and manage the cyber security governance in Taiwan and founded in August 2016 under the Executive Yuan. One of the major missions of DCS is to promote the enactment of the Information and Communication Management Act, the basic law for Taiwanese cyber security. Moreover, DCS announced the new Cyber Security Flagship Programs in 2017 that would run for the next four years from 2017 to 2020. Eight ministries are included and have been given different tasks for the construction of the Information Sharing and Analysis Centers (ISAC), the Security Operation Centers (SOC) and the Computer Emergency Response Teams

[4] The annual summary of survey statistics is available at https://www.dgbas.gov.tw/np.asp?ctNode=405

[5] NICSO is affiliated with the National Security Council in Taiwan

(CERT) (As shown in Table 1). For example, the Ministry of Economic Affairs (MOEA), the Ministry of Science and Technology (MOST), the Ministry of Health and Welfare (MOHW), and the Ministry of Transportation and Communications (MOTC) are respectively charged in establishing the ISACs for critical infrastructures of energy, water resources, high-tech parks, medical treatment, and transportation. In addition, the MOEA plans to support cyber security industry by means of talent cultivation, government procurement, tax deduction for R&D, counseling services, and establishment of mobile application safety check institutions.

Under the coordination of DCS, a special budget of approximately NT$1.4billion (~ US$46.7 million) annually (as indicated in the 2017 budget report) will support both central and local government departments/agencies to improve and develop Taiwan's cyber security environment from 2017 to 2020.

Table 1 A division of labor of cyber security tasks across government ministries

Ministry	Main Tasks of Cyber Security
Ministry of Economic Affairs (MOEA)	● Establish the Information Sharing and Analysis Center (ISAC) for critical infrastructure of water resources and energy supply. ● Support cyber security industry and cultivate senior talents.
Ministry of Science and Technology (MOST)	● Establish the ISAC for critical infrastructure of science-based industrial parks. ● Subsidize universities and colleges to cultivate talents and research on advanced cyber security technology.
Ministry of Health and Welfare (MOHW)	● Establish the ISAC for critical infrastructure of public health.
Ministry of Interior (MOI)	● Raise the capacities of digital forensics in high-tech crimes.
Ministry of Education (MOE)	● Improve the cyber security of Taiwan Academic Network.
Ministry of Transportation and Communications (MOTC)	● Establish the ISAC for critical infrastructure of transportation.
National Communications Commission (NCC)	● Strengthen the protection for national basic communication network and do researches on IoT information security.

Ministry of National Defense (MND)	● Build Information Communication Electronic Force (ICEF) to protect digital domain in Taiwan and reinforce cyber security industry. ● Establish multilateral cyber security agreement to increase multinational collaborations.

Source: summarized by the authors

2.2 Stakeholders in Policy-making

In Taiwan, the stakeholders of policy-making for the cyber security industry can be classified into three categories: government, market, and research institutes.

2.2.1 Government

As mentioned in the previous section, government actors include a broad range of governmental ministries. Based on national development plans, each ministry or agency is assigned with tasks in field of cyber security. The Department of Cyber Security is taking the advisory role with MOEA and MOST serving as the two primary ministries formulating industrial policies.

2.2.2 Market

Technology Providers

The Taiwanese cyber security industry is immature, lacking in large and world-renowned local service providers. Government-run Chunghwa Telecom (CHT), the largest telecommunication corporation in Taiwan, recently established a new cyber security subsidiary in 2018. The CHT subsidiary is expected to be the bellwether of the Taiwanese cyber security industry. In addition, some associations composed of ICT service providers, such as the Taipei Computer Association (TCA), and the Information Service Industry Association of R.O.C. (CISA) pay close attention to the development of cyber security industry. Moreover, The Hacks in Taiwan (HIT) Association is also an influential non-profit organization in Taiwan. The members of the HIT association are hackers, engineers, and business people in the cyber security industry. Since 2010, the HIT association annually hosts HITCON, which aims to bridge cyber security professionals and businesses.

Service Demanders

If the Information and Communication Management Act passes, the act will substantially increase potential clients in the industry. According to the act, service providers for critical infrastructures, such as high-tech parks, energy, water resources, ICT, transportation, finance, and medical treatment, are the potential clients that will be strictly regulated to strengthen cyber security protection.

2.2.3 Research Institutes

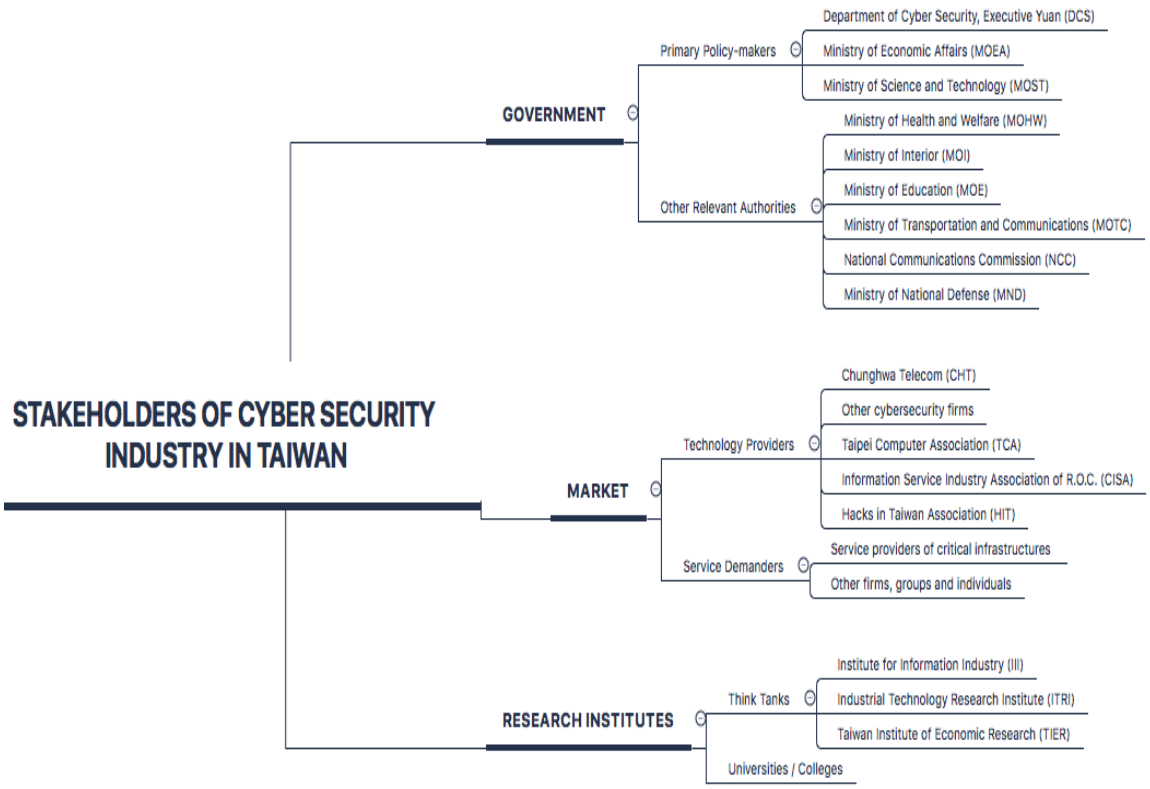
Think Tanks

Think tanks, such as the Institute for Information Industry (III), the Industrial Technology Research Institute (ITRI) and the Taiwan Institute for Economic Research (TIER), assist the Taiwanese government in promoting and researching the cyber security industry. The III and the ITRI are the two leading Government-Organized Non- Governmental Organizations (GONGOs) established in 1970s by the MOEA for promoting technological industries in Taiwan, including information and communication sectors. Moreover, the TIER is a private economic think tank founded in 1976. Nowadays, the above three institutes receive a great amount of government funding every year to carry out research and projects relevant to the cyber security industry.

University/College

For cultivating cyber security talents, universities and colleges in Taiwan are expected to lead to teaching resources, deliver more relevant courses, and conduct further research on advanced issues.

Figure 5 Stakeholders of cyber security industry in Taiwan



3. The Market Failure and Government Interventions for Cyber Security Industry

3.1 A Path Dependency Model in Developing the Industrial Policy

As an export-oriented country specializing in the electronics industry and precision machinery industry, Taiwan is an exemplary economy among developing countries in Asia. Since World War II, Taiwan has been known for allowing it's industrial policy making to be driven by a group of highly independent technocrats and political elites that emphasized centralized industrial policies (Wade 1990). Since 1970, the Taiwanese government has maintained a dominant role in investing in targeted fields and industries; for example, through its investment in the plastic and textile industry in the 1950s and the world-famous semiconductor industry in the 1980s. In almost all of these cases, the government always took the lead in new industries while maintaining a strong connection with private firms and potential entrepreneurs. The special relationship between the government and industry in Taiwan is shaped under a co-evolution ecosystem (Amsden and Chu 2003; Breznitz 2005, 2007). As Breznitz (2007) describes, a common pattern of this co-evolved relation consists of two stages. The first stage was that the state's research agencies (e.g., ITRI for hardware and III for software) absorbed and improved a new technology from abroad. After successfully testing the prototype internally, they transferred the improved technology to private companies to spur the industry. In the second stage, when the industry emerged, the state-sponsored research agencies shifted to be more of an assisting role that would collaborate with private firms to develop R&D capabilities.

The rationale behind the aforementioned industrial governance is to overcome market failure where private sector actors, especially start-ups and small and medium-sized firms, are reluctant to enter new, high-risk technological fields due to lack of capital and information uncertainties (Harris and Carman 1983). Similar to Aggarwal and Aggarwal's (2016) discussion concerning the rationales of state intervention for industrial policy, the Taiwanese government legitimizes their intervention policies based on perceived market failures. Government interventions to overcome market failure included monetary incentives such as R&D tax credit, subsidies to SBIR or targeted industries, loans, or financial assistance (Yang, Huang, and Hou 2012), and with government procurement being commonly used in Taiwan as well.

However, with the experience of the semiconductor industry in Taiwan in the 1980s, the concept of "governing the market" seemed to not work as well following 1990 due to globalization and the increasing pace of R&D in new emerging industries. Reasons could be multifold. In one of our informal interviews, one previous government officer said he believes the weakening role of those research agencies can be attributed to the rapid development of Internet which facilitates the flow of knowledge with low costs. Private companies nowadays can easily acquire top-notch technological knowledge using online resources, as well as from the increasing number of young talents studying or working abroad. The technological capability and absorptive capability of private firms might be as good as or even better than the state-sponsored research institutes. On the other hand,

Breznitz (2007) also argued that the latecomer advantages of the developmental nations might not suit the OEM/ODM-based industrial structure anymore. A great deal of literature also shows that the actual policy effect of whether providing fiscal incentives will increase innovative performance was still under-debating. Reviewing prior literature, the traditional view of public funding as remedy to mitigate the market failures may increase incentives for private sectors to invest on R&D (Arrow 1962). However recent studies argue that public funding is actually replacing private firms' R&D investments, especially in high-tech industries with intensive tacit knowledge (Aschhoff 2009; David, Hall, and Toole 2000; Lach 2002).

Looking specially at our cyber security case, the government is hoping that this field of technology will become the next generation of IT industry. Based on the new national program for cyber security (The Eight Flagships Program for Cyber Security) proposed by the Department of Cyber Security of Taiwan Government in 2017, it's obvious that the government has strong ambition to develop and strengthen Taiwan's cyber security industry. A formal research associate at the Taiwan Institute Economic Research, mentioned in our interview that most of Internet users in Taiwan currently adopting information security products from foreign companies. Domestic information security companies tend to be small in scale and concentrate in similar areas, such as Firewall/UTM, Email-security, and the PKI/Crypto areas. The only domestic cyber security company with more than 1000 employee is Trend Micro Corporation. There are many large foreign companies who have a majority of the market share in Taiwan. These companies include Symantec, Check Point, Cisco, Juniper, Fortinet, EMC, CA, McAfee, Websence, Kaspersky and so on (U.S. Commercial Service Report 2017).

Nevertheless, we observe from our interviews and archival government documents that there is a very strong intent of government interventions in shaping the cyber security industry policy. Following the Aggarwal and Aggarwal (2013) framework, the rationale for government intervention in Taiwan could be categorized into several types of market failure: (1) Excessive competition, (2) externality, and (3) dynamic scale economies. We explain the three different market failures below.

(1) Excessive competition

As mentioned earlier, most of the cyber security companies in Taiwan are very small in scale and cater to niche markets by providing specialized security solution packages which are often embedded in the mature security systems owned by larger foreign corporations. When foreign companies dominate most of the key technologies and the market in the cyber security field, the competition is tough for the domestic actors, as well as for the sustainability of the local industry network. In other words, excessive competition in the market is likely to lead to a weak domestic industrial chain.

(2) Externality

Another type of market failure is about externality. Our interviewees mentioned that the lack of incentives for companies to adopt new technologies is the key bottleneck. In order

to create a complete industry chain for the cyber security sector, there not only has to be producers of upstream and downstream chains, but also the demand chain in the market as well. While the risk of having weak security systems is high for enterprises in almost every sector nowadays, for those chartered business such as the critical infrastructure providers (CIPs, e.g., water, energy, telecommunication, etc.), the market competition is limited. For instance, the Taiwan Power Company is a state-owned electric power monopoly. The lack of competition in market is criticized for leading to market inefficiencies such as clumsiness and inertia to organizational learning. Additionally, back to the concerns about cyber security, customer satisfaction of data protection and potential risks might be external costs for those state-owned CIPs.

Technology externality is also an important point of concern for the government in cultivating a new knowledge-intensive industry. The consequence is the under-investment in early-stage R&D. The antidotes are public subsidies/grants, R&D tax-credit, or supporting university-industry collaboration.

(3) Dynamic scale economies

Another crucial reason that the growth of Taiwan's cyber security industries has been hampered are the institutions of the capital market itself. Criticism includes a) the strict initial public offering (IPO) rules against the software companies, and b) a national financial system that is reluctant to conduct long-term investment (or the so-called patient capital). For the first criticism, the listing requirements set out in the Taiwan Stock Exchange (TWSE) is stricter than Singapore, Hong Kong, and Japan. Requirements for listing include no accumulated deficits and at least 6% pre-tax net profit for the past two years. Given that the IPO rules did not favor software or Internet companies, as a result it limited the growth of software-based industry, including the cyber security field. For example, the largest cyber security company in Taiwan, Trend Micro, was rejected by the TWSE but got listing on the Tokyo Stock Exchange in 1998.

For the second criticism, Fuller et al. (2003) argued that as a late developer country, Taiwan intentionally constructed a financial system that, although managed to have a very low average debt-to-equity ratio, ultimately hampered the long-term investment for R&D and innovation. This risk-averse atmosphere in the capital market limited Taiwan's ability to innovate in the IT industry, especially when shifting from hardware manufacturing to the more value-added areas like the software sectors.

3.2 Government Interventions in the Cyber Security Industry

In order to enlarge the pie of the cyber security market in Taiwan, the government proposes two major action plans to be implemented between 2017 and 2020, including:

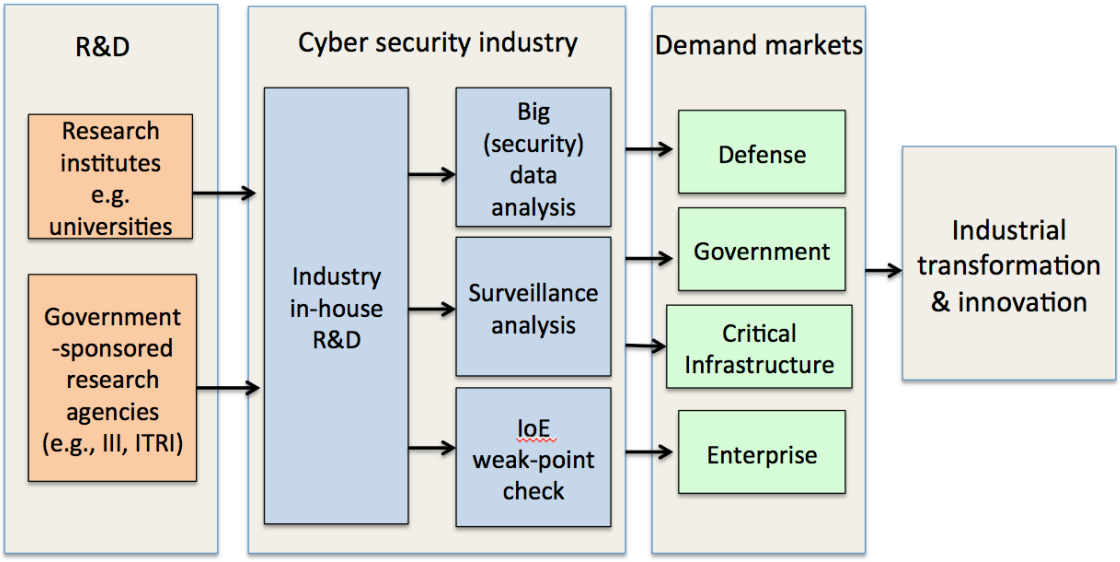
1) Increase market demand to stimulate private supplies, and 2) Enhance the overall cyber security workforce.

For the first action plan, the goal is to increase firms' technological capability and boost the market by identifying where the demand is. Similar to many previous industrial policies in Taiwan, the research agencies are once again playing the role of technology leader, with the hope that they will stimulate collaborations between the agencies and industry to further encourage more industrial in-house R&D investment. The second part of the action plan, aims to enhance the overall cyber security workforce in Taiwan. As mentioned by one of our interviewees, a senior government officer at the Department of Cyber Security:

"Cyber security talents are definitely crucial to the development of the industry, but we need state policy to pull the market demand to keep our labor force. For example, we have the Ministry of Education working on in-school training and the Ministry of Economic Affairs subsidizing on-the-job training or after school staff training." His excerpt reveals a hidden worry that the supply of qualified human resources is slower than the demand of the market. In this regard, it will be difficult to develop domestic industry in the field of cyber security.

We summarized the overall policy practices and government intention in Figure 6 according to the Report of the National Cyber Security Program of Taiwan which was announced in 2017. From the chart, it is clear that the state policy is hoping to identify the key players in the potential market, including R&D actors, the private sectors, and the targeting consumers.

Figure 6 The development of cyber security industry: government action plans



Source: National Cyber Security Development Program (2017)[6]
Summarized and graphed by the authors

[6] The complete report can be accessed via:
https://www.nicst.ey.gov.tw/en/News.aspx?n=833B775CE6C4F9F5&sms=0A29FF40DDCD03DD

Howard Jyan, Director of DCS, the advisory department of cyber security, announced in recent speeches that the DCS has identified five potential markets. Table 2 summarizes the proposed policies for the five targeted markets, including the government procurement market, the enterprise market, the critical infrastructure information protection (CIIP) market, the defense market, and the mobile application safety market. For each market, the perceived government rationales are in column 2, the proposed policy instruments are listed in column 3, and the government strategy and potential problems of those interventions are described in column 4 and 5.

It is obvious that this type of government intervention is similar to the information responses approach summarized by Harris and Carman in 1984, which emphasizes using a series of policies to influence the market. To summarize, state policy in Taiwan has two major approaches while pushing the new industry. One is to reshape the market through initiating a new cyber security management law. In Taiwan, supporters are advocating for the Information and Communication Management Act to become the basic law of Taiwanese cyber security. Through regulation, many existing private, public, and nonprofit entities will have to upgrade devices and conform to new market standard. On top of the legislative base, another thread of state policy is about market creating, for instance, expanding the scale of government procurement, creating new market demands by imposing a new security standard, and providing financial subsidy for SMEs.

Table 2 A regulation-driven cyber security industrial policy of the 2017 strategy plans proposed by DCS

Types of market	Government rationale	Proposed policy tools	Strategy	Problems with government intervention
Government market	1] National policy goal 2] Excessive market competition	1] New regulation mandate 2] Centralized contracts for government procurement of cyber security software and cloud services	Increase domestic demand	Inefficiency in finding the best solutions Too much protection for domestic companies

The enterprise market	1] Technology externality 2] Dynamic scale economies (lack of VCs and capital market)	1] Tax credit for R&D investment in cyber security, targeting existing IT companies and SMEs 2] Provide R&D grants or subsidies	Encourage R&D	-Government failure - Crowd-out effect - Provide no motives for local enterprise to be competitive
CIIP market	1] Externality	1] New regulation mandate 2] Assist critical infrastructure enterprise to upgrade its cyber security protection systems Provide fiscal incentive for R&D and technological upgrade	Create new market demand	Strategic behavior in obeying the regulation
Defense market	1] National security goals 2] Uncertainties in international relationships	1] Launch the Information, Communications and Electronic Warfare Command in 2017 2] Increase spin-off of military technologies and research discoveries	National Security	Unable to reach the economy of scale hole to government budget
Mobile application safety check market	1] Incomplete information	1] Establishing third party institutions for mobile application safety check	Niche Market	Strategic behavior in getting the safety check

Source: Summarized by the authors

4. Discussion: Challenges the Government is Facing

The following section will further discuss what problems the government might be facing while developing the cyber security industry. Three problems are listed below.

1. A lack of dedicated authority leading the whole cyber security policy

As mentioned in the policy and stakeholder section, the Department of Cyber Security (DCS) was created with an important mission: to push forward the enactment of the Information and Communication Security Management Act. The draft law of this Act was sent to legislature in October 2016. However, once the Act has passed, will the DCS remain the authority in charge of carrying out the policy implementation? The DCS is an internal department within the Executive Yuan Office with a scale of 21 government workers. The challenge for DCS will be in coordinating different ministries to come up with corresponding policies, as well as implementing those policies. The DCS might have some ideal blueprint in mind, but in practice, ministries often suffer from limited resources and rigid division of responsibility. For example, although the Ministry of National Defense just launched a new military command for information and communications warfare, the 2017 defense budget is still below 3% of GDP (approximately US$102 billion). With the creation of new command, the budget for 2017 is merely 1.5% higher than 2016 national defense budget. Thus, given the constraints, it is unlikely that the Ministry of National Defense can put in extra effort to foster the cyber security industry or the spin-off of new innovation from its research institutes. A thorough examination of this interagency approach adopted by Taiwan authorities is worth-noting for future studies.

2. Identifying the best policy interventions to solve market failure

Much of the current government intervention for cyber security industry is to overcome various market failures. Examining the action plans proposed by the Department of Cyber Security, we observe that a lot of efforts are put into overcoming problems of technology externality and fostering the market for the domestic cyber security industry. In the past, the government used many intervention tools repeatedly. For example, the use of tax policy protects key industries (e.g., biotechnology) for the conduct of R&D activities. Government procurement of IT systems or services was limited to domestic companies. Public funding for project subsidies or SBIR grants was also restricted to local applicants. However, many traditional policy tools are considered to be ineffective or indifference as more and more empirical research are revealing the policy effects using more quasi-experimental methodologies (Chai and Shih 2016).

Under traditional intervention, one immediate impact is the imposition of barriers to entry for foreign companies. This is likely to discourage knowledge flows and learning across foreign and domestic firms. Additionally, too much protection for domestic firms could lead to a lack of competition for local enterprises. Although some argue that public funding could alleviate the underinvestment of risky technology, especially for small and medium-sized firms (Meuleman and De Maeseneire 2012), critics contend that

government funding is likely to cause either a crowding-out effect or no effect at all, suggesting that companies tend to use government funding to substitute their own R&D investment. Even worse, for grant awards, government has the tendency of picking previous winners to assure program success (Wallsten 2000). Additionally, government failure could occur in the process of selecting the contractors or grant awardees where authorities have information asymmetry problems and end up being no better than private financial sector investments or venture capital.

We suggest that the government carefully evaluate current policy tools that aim to solve market failure. Alternative policy tools, for example, public venture capital with investment conditions might be able to alleviate market failure for high-risk industries and agent problems (Lerner 2002).

3. A collaborative or competing model between the government and the private sector

As a latecomer in the global economy, Taiwan used to have a very good model between government-sponsored research agencies and industry, in particular the role of Industrial Technology Research Institute (ITRI) and the semiconductor industry in HsinChu city (Breznitz 2007). However, in the case of cyber security, the focus is more towards software. Compared with the big hardware companies in Taiwan, software firms tend to be small and younger. One reason is that the leading research agency, Institute for Information Industry (III), from the beginning of its establishment, was competing with existing private software industry. If they could play more like a technology/knowledge transmitter, they might be able to provide more support to local enterprises. For example, the Cyber Security Technology Center within III is taking the business of assisting the cyber security safety check for government agencies. As a result, the particular role of III is likely to undermining the development of the software industry, as well as the cyber security industry.

The aforementioned discussion leads to our next question. Who should be the market leader? Our interviewees, a former TIER research associate and a university professor specializing in the cyber security field, both mentioned that Chunghwa Telecom, the biggest telecommunications company in Taiwan, could be the market leader. With Chunghwa's scale and capital resources, it could initiate an industrial alliance for the whole supply chain of cyber security firms. However, as a publicly-traded company, our interviewees also say, "Chunghwa is very risk-averse investing in the new IT areas." Thus, lowering barriers for market entry and inviting an anchor/incumbent firm to invest in Taiwan could be something for the government to consider.

Some directions for further development

This paper began by introducing the development of cyber security policy carried out by Taiwanese authorities since 2000. To closely investigate the industrial policy for cyber security, we then provided a thorough review of the current national information security policies in Taiwan and key stakeholders in the policy-making for the cyber security industry. Drawing from existing literature on government intervention, we analyzed

current policy tools used by the Taiwan government to foster a focal industry. To sum up, this paper also pointed out Taiwan's cyber security challenges and potential problems of intervention in the global competitive market.

Based on interviews and government archival documents, we summarized three different perceived market failures in the cyber security industry in Taiwan, including excessive competition, externality, and the dynamic scale economies. To achieve a complete industrial chain, the government seems to take those concerns seriously and is eager to shape a new market that will facilitate the growth of the industry. However, we also observe that the mindset of the state policy is pretty similar with the planning for the semiconductor industry in the 80s. It was centralized, top-down thinking, and adopted a regulatory-driven approach as well. In addition, the Industrial Technology Research Institute (ITRI), a government-owned research institute, was assigned to be the R&D and innovation leader and the knowledge transmitter for the industry. We observe very similar policy instruments are applied in today's cyber security industrial policies. There is a lack of bottom-up discussion from the private sector and local stakeholders about what the industry and innovators really need.

In summary, the cyber security industry in Taiwan is still in its infant-stage. On one hand, due to the design of the financial system, Taiwanese companies as a whole are reluctant to invest in large-scale long-term R&D projects and talent cultivation. They tend to prefer incremental innovation, which are less risky and low cost. On the other hand, the Taiwanese government anticipates improving the cyber security of government agencies and critical infrastructure with regulatory thinking. To develop the cyber security industry in Taiwan, this paper suggests the following:

First, at the administrative level, the government should empower a Minister without Portfolio in the Executive Yuan to conduct the development and the implement of relevant policies of the industry, as well as coordinate different ministries. Second, it is important to stimulate the domestic market by raising tax incentives for businesses to invest in R&D and talent cultivation and not just new equipment and hardware infrastructure, which tend to be one-time investments.

Additionally, a strong local industrial chain and inter-connected industrial ecosystem is crucial for the development of cyber security industry. Findings of our study show that the majority of the IT security market in Taiwan is dominated by many large foreign companies. The local industry will not grow if the legal environment, capital, the market, and the key talents are not in place (Huang 2017). Rather than imposing the traditional protectionism-approach policies by mandating strict rules against foreign entries, which is likely to hamper knowledge spillover and learning, we suggest the government adopt a more non-traditional policy to enhance the technological capacities of local companies. For instance, encouraging collaboration between government labs or government affiliated organizations and private sectors (as well as a more open investment environment). The legal environment could be more creative, open to allowing new cyber security products to have a trial phase, like a regulatory sandbox. Moreover, open to at

least discussing the possibility and applicability of alternative channels for collecting funds and capitals would be necessary.

Lastly, in order for a new industry to run and grow sustainably, human resources are crucial. For policy-makers, we suggest that the relevant policy tools are to collaborate with think tanks and universities for basic and advanced training courses in cyber security and related fields.

References

Aggarwal, Sonia, N., and Vinod K. Aggarwal. 2016. "The Political Economy of Industrial Policy." . Working paper. https://basc.berkeley.edu/wp-content/uploads/2017/09/BWP16-01.pdf.

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," BASC Working Paper Series, 2018-01.

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: The U.S. Case," BASC Working Paper Series, 2018-02.

Amsden, Alice, and Wan-Wen Chu. 2003. *Beyond Late Development: Taiwan's Upgrading Policies*. Cambridge, MA: The MIT Press. https://mitpress.mit.edu/books/beyond-late-development (October 16, 2017).

Arrow, Kenneth. 1962. "Economic Welfare and the Allocation of Resources for Invention." In NBER Chapters, National Bureau of Economic Research, Inc, 609–26. http://ideas.repec.org/h/nbr/nberch/2144.html (July 15, 2011).

Aschhoff, Birgit. 2009. *The Effect of Subsidies on R&D Investment and Success: Do Subsidy History and Size Matter?* ZEW - Zentrum für Europäische Wirtschaftsforschung / Center for European Economic Research. ZEW Discussion Paper. http://econpapers.repec.org/paper/zbwzewdip/09032.htm (February 1, 2016).

Breznitz, Dan. 2005. "Development, Flexibility and R & D Performance in the Taiwanese IT Industry: Capability Creation and the Effects of State–Industry Coevolution." *Industrial and Corporate Change* 14(1): 153–87.

Breznitz, Dan. 2007. *Innovation and the State: Political Choice and Strategies for Growth in Israel, Taiwan, and Ireland*. Yale University Press. http://www.jstor.org/stable/j.ctt1nppt9.

Chadwich, Jonathan. 2016. “ATM Hacks in ‘more than a Dozen’ European Countries in 2016: Group IB.” *ZDNet*. https://www.zdnet.com/article/atm-hacks-in-more-than-a-dozen-european-countries-in-2016-group-ib/.

Chai, Sen, and Willy Shih. 2016. “Bridging Science and Technology through Academic–Industry Partnerships.” *Research Policy* 45(1): 148–58.

Chang, Lennon. 2012. “Cyber Conflict between Taiwan and China.” *Strategic Insight* 10(1): 26–35.
Cyber Security: Overview, Regulatory Trends, and Opportunities in Taiwan. 2017. Taipei: U.S. COMMERCIAL SERVICE.

David, Paul A., Bronwyn H. Hall, and Andrew A. Toole. 2000. “Is Public R&D a Complement or Substitute for Private R&D? A Review of the Econometric Evidence.” *Research Policy* 29(4–5): 497–529.

Fuller, Douglas, Akintunde Akinwande, and Charles Sodini. 2003. “Leading, Following or Cooked Goose? Innovation Successes and Failures in Taiwan’s Electronics Industry.” *Industry and Innovation* 10(2): 179–96.

Harris, Robert G., and James M. Carman. 1983. “Public Regulation of Marketing Activity: Part I: Institutional Typologies of Market Failure.” *Journal of Macromarketing* 3(1): 49–58.

Huang, Hsini. 2017. “Invisible Constraints: The Relationship among Non-Competition Agreements, Inventor Mobility, and Patent Commercialization.” *Science and Public Policy* 44(3): 341–53.

Huang, Tzu-Ti. 2018. “Taiwan Government Websites Hit with over 20 Million Cyber Attacks a Month, Mostly from China.” *Taiwan News*. https://www.taiwannews.com.tw/en/news/3398654.

Lach, Saul. 2002. “Do R&D Subsidies Stimulate or Displace Private R&D? Evidence from Israel.” *The Journal of Industrial Economics* 50(4): 369–90.

Lerner, Josh. 2002. “When Bureaucrats Meet Entrepreneurs: The Design of Effective `public Venture Capital’ Programmes.” *The Economic Journal* 112(477): F73–84.

Meuleman, Miguel, and Wouter De Maeseneire. 2012. “Do R&D Subsidies Affect SMEs’ Access to External Financing?” *Research Policy* 41(3): 580–91.

Wade, Robert. 1990. *Governing the Market: Economic Theory and the Role of Government in East Asian Industrialization*. Princeton, NJ: Princeton University Press.

Wallsten, Scott J. 2000. “The Effects of Government-Industry R&D Programs on Private R&D: The Case of the Small Business Innovation Research Program.” *The RAND Journal of Economics* 31(1): 82–100.

Yang, Chih-Hai, Chia-Hui Huang, and Tony Chieh-Tse Hou. 2012. “Tax Incentives and R&D Activity: Firm-Level Evidence from Taiwan.” *Research Policy* 41(9): 1578–88.