Institute of
Chinese Studies
ICS
中国研究所DELHI

OCCASIONAL
PAPER

No. 94 August

China as a Factor in Taiwan’s National Cyber Security Strategy

Kaushal Kishore Chandel

Institute of Chinese Studies,
B-371 (3rd floor), Chittaranjan Park,
Kalkaji, New Delhi - 110 019
Landline Telephone: +91-11-4056 4823 Fax: +91-11-23830728
Email: info@icsin.org
Website: www.icsin.org

ABOUT THE AUTHOR

Kaushal Kishore Chandel works as an Assistant Professor at Centre for Chinese and South East Asian Studies (CCSEAS), Jawaharlal Nehru University (JNU), New Delhi. His areas of interest are China’s cyber security, cyber warfare, international cyber governance, learning and teaching Mandarin. He has also served as an Assistant Professor in Centre for Far East Language (Chinese), Central University of Jharkhand, Ranchi, Jharkhand (2013-2014). His recent work “China's Perception of Cyber Security: Conflict and Cooperation with BRICS Nations” (retitled as "China's Cyber Issues"), has been published as a book chapter in the book titled "China and the BRICS, Setting Up a Different Kitchen" published in 2016 by Pentagon Press, New Delhi.

Contact: kaykayjnu@gmail.com

China as a Factor in Taiwan's National Cyber Security Strategy

Abstract

In today's information age, cyberspace is closely linked with economic prosperity, security and integrity of a nation. Therefore, cyber security has been elevated to the level of national security by many countries, and Taiwan has also done the same. Ever since cyberspace was declared as the fifth war-fighting domain by the US, many nations have invested in the new domain so as to build both offensive as well as defensive capabilities. In recent past many nations have published some form of National Cyber Security Strategy (NCSS). Taiwan has also released its own version of NCSS. NCCS is considered as the official document through which most of the nation states elaborate their national visions, guiding principles, perceptions of the threat and strategic objectives. In a post COVID-19 and post Russia-Ukraine conflict world, it is imperative to analyse Taiwan's NCSS, in order to understand Taiwan's priorities, concerns and strategic objectives in cyberspace. It is also crucial to study how China, being the most dominant players in 5G and artificial intelligence technologies, is perceived in Taiwan's NCSS.

By using qualitative and quantitative methods, and by using both Chinese and English language primary and secondary sources, this paper attempts to study: Taiwan's strategic objectives and priorities in cyberspace; how is China perceived in Taiwan's cyber strategy; what kind of role Chinese capabilities play in shaping Taiwan's NCSS; and how Taiwan plans to develop its cyber capabilities in order to counter China in case of a crisis or conflict.

Keywords: Taiwan's Cyber Security, China factor in Taiwan's Cyber Security, National Cyber Security Strategy (NCSS), Taiwan's National Cyber Security Program (NCSP), Taiwan and China in Cyberspace

Introduction

In June, 2017 while formally establishing the Information Communication Electronic Force Command (ICEF), an independent military cyber command, the President of Republic of China (ROC hereafter Taiwan) Tsai Ing-wen (蔡英文) declared, ‘cyber security is national security’ (Robyn 2018). In November, 2019 at a meeting with a team of ‘white hat’ hackers at the Presidential Office, she reiterated Taiwanese government position, ‘Cyber security is directly linked to national security and is a top priority for the government’ (Su and William 2019). Ever since cyberspace was declared as the fifth war-fighting domain by the US, many nations have invested in the new domain so as to build both offensive as well as defensive capabilities. Consequently, many incidents of cyber attack have been reported across the world, for e.g. Estonia in 2007, Georgia in 2008, the Stuxnet incident, breach of Sony Corporation, the American F-35 fighter jet blueprint being stolen, the incident of Office of Personnel Management (OPM) in 2015, Russia’s alleged role in meddling with 2016 US Presidential election, etc. According to Taiwan’s national defense report 2017, ‘Of all non-conventional security threats, complex disasters and cyberattacks represent the biggest threats to Taiwan.’

These cyber attacks have obvious political implications and result in huge economic loss. One report (McAfee 2018) estimated, ‘Cybercrime now costs the world almost $600 billion, or 0.8 percent of global GDP’. The report also claimed, ‘When you look at the cost of cybercrime in relation to the worldwide internet economy’ it is ‘$4.2 trillion in 2016’. Thus, cyberspace is closely linked with the development, economic prosperity, security and integrity of a nation. Moreover, cyber security has been elevated to the level of national security by many nations, which is visible in their official documents. In recent past many nations and nation groups have published National Cyber Security Strategy (NCSS) or National Information Security Strategy. Taiwan has also released its own version of NCSS. Taiwan’s National Security Bureau (NSB) 2013 report, described People’s Republic of China (hereafter China) as being armed with a cyber army of more than 100,000 people. It also added that the China has allocated more than $80 million to its cyber war workforce in 2013 and the NSB director described the Chinese cyber threat as ‘very severe.’ One of the Taiwan’s officials recently claimed that Taiwan’s government network faces ‘five million attacks and scans a day’, he also emphasized that out of millions of cyber-attacks every month, half of them are believed to originate from China. In such a backdrop it is imperative to analyse Taiwan's NCSS, in order to understand Taiwan's priorities, concerns and strategic objectives in cyberspace. It is also crucial to study how China, being a dominant player in 5G and artificial intelligence technologies, is perceived in Taiwan's NCSS.

Existing literature do talk about Taiwan's cyber security and cyber security posture, however very few have attempted delving into Taiwan's perception of China by analysing Taiwan's policy papers related to cyberspace. Qualitative analysis of the primary sources (both in Chinese and English) in order to understand: what kind of role Chinese capabilities play in shaping Taiwan's NCSS; and how Taiwan plans to develop its cyber capabilities in order to counter China in case of a crisis or conflict, has also not been done. This paper is an attempt in this direction.

This paper attempts to study: Taiwan's strategic objectives and priorities in cyberspace; what kind of role Chinese capabilities play in shaping Taiwan's NCSS; and how Taiwan plans to develop its cyber capabilities in order to counter China in case of a crisis or conflict. By using both qualitative as well as quantitative methods, this study will make use of both Chinese and English language primary and secondary sources.

Relevance of NCSS

National Cyber Security Strategy (NCSS) is considered as the official document through which most of the nation states elaborate their national visions, guiding principles, perceptions of the threat and strategic objectives (Eric 2013). In NSCS the visions are translated into strategic objectives which are broken down further into a wide variety of priorities (Klimburg 2012). 'A national strategy may have different objectives: (1) to align the Whole of Government, (2) to coherently focus and coordinate public and private planning, and to convey the envisioned roles, responsibilities and relationships between all stakeholders, and (3) to convey one's national intent to other nations and stakeholders' (Eric 2013). A well-formulated National Security Strategy (NSS) should do at least three things:

Firstly, it should enable government departments and ministries to translate a government's national security vision into coherent and implementable policies. Secondly, a NSS should clarify how the state might act in international affairs – enabling a more proactive rather than reactive foreign policy. To illustrate, a NSS could be helpful in determining what elements of national power (e.g., diplomatic, information, military, economic) are most likely to be employed to reach specific international objectives. Besides informing international policy making, a NSS should serve to communicate strategic thinking to other states and the international community at large. Thirdly, a NSS should not exist in a strategic vacuum. On the contrary, it should be linked to existing national and international strategies to the extent that it is feasible to encourage a harmonised set of policies that are shared with likeminded partners (Klimburg 2012).

In this way, NCSS do not only include domestic policies and priorities rather they also talk about foreign policies and postures. NCSS aims to provide guidance to policy-makers regarding cyber policy priorities and potential resource allocations. However, these NCSS can also have other roles as well: they can play an active role in shaping the international image of a nation, and indicate where it thinks future collaboration would be possible. A NCSS can also form an important part of a nation's declaratory policy – indicating to potential adversaries where red lines may be drawn before retaliation can be expected, and what capabilities exist, or are being developed, to execute this type of policy (Klimburg 2012). For instance, the United States has repeatedly warned that it would consider cyber attack on its critical information infrastructures (CIIs) an 'act of war'. It is obvious that NCSS is also used as a deterrent by declaring a threshold and retaliation measures to be adopted when threshold is crossed.

Similar kind of argument is put forward by Tallinn Manual, which talks about effect based evaluation. If the consequences produced by cyber attacks on a nation are equivalent to that of war on a nation, the cyber attack should be considered as an act of war and retaliation should be used accordingly. This declaratory component is increasingly becoming a crucial part of NCSS. Similarly, NCSS document often includes 'political, internal security, foreign policy, defence structures and economic dimensions, stakeholders' participation framework etc at national level' (Klimburg 2012). Also the national vision of securing cyberspace reflected in NCSS give way to cooperate and collaborate with international stakeholders, other nations and groups of nations at bilateral as well as multilateral levels. Without this, addressing cyber threats does not seem to be feasible as Ilina argues, ‘The ability of the government to react to cyber space threats is limited and likely to be doomed to failure if not cooperating with the rest of the involved in the process. The continuous dialogue, based on coordination, cooperation and collaboration among stakeholders is a key factor for the success of the NCSS’ (Ilina 2015).

Ilina also points out that NCSS aims to guarantee that states are able to face the cyber security challenges and are aware of the consequences, as well as capable of undertaking adequate measures against violations and crime committed in information systems. There are so many reasons why one document can have so much of national as well as international importance. Yet another reason, though not necessarily the last one, is: ‘establishing a NCSS has substantial appeal because it encourages policy-makers to identify strategic objectives (ends), to pinpoint the resources available to reach those objectives (means), and to provide a guide on how such resources are to be applied to reach stated objectives (ways)’ (Klimburg 2012).

The Cyber Security Debate

Ever since the term ‘cyber security’ was widely used during the year 2000 with the ‘clean-up’ of the millennium software bug, no universally accepted definition has emerged till date (Klimburg 2012). While discussing about cyber related terms, it has been observed that definition of the problem is the actual problem (Kruger 2014). It has been conceived and defined differently by different nations. In their published NCSS by 19 nations, one third of the nations, discuss cyber security without even defining the term, however only less than half of the nations explicitly define terms such as ‘cyber security’ (Eric 2013). Even the United States, which has published maximum number of documents in comparison to any other nation, yet there is no clear definition of what the US government considers to be cyber security (Klimburg 2012). In the field of cyber security, ill-defined concepts and inconsistently applied terminology are further complicating an already complex issue. This causes difficulties for policy-makers, strategists and academics (Dewar 2014).

That’s why continuous efforts are being put in towards defining and building consensus. One of the examples at bilateral level is: Russia-US bilateral working group (the East West Institute

(EWI) and Moscow University) in their international cyber terminology framework, defined cyber security as ‘a property of cyberspace that is an ability to resist intentional and unintentional threats and respond and recover’. Another definition asserts, ‘Cybersecurity encompasses the defence against all types of cyber attacks, and includes a number of related issues not normally associated with cyberwarfare or even foreign policy, including critical infrastructure protection, Internet governance, cybercrime, data protection, and others’ (Klimburg and Tirmaa 2011). From national cyber security perspective,

> Cyber defence is a ‘collective effort’. The concept of ‘collective cyber defence’ can be interpreted as ‘operative cooperation of various (international) participants to defend from specific cyber attacks against one or more of the participants.’ Cyber defense uses the methods of physical obstruction or manipulation of the Internet traffic to limit the cyber attacks; sharing and combining intelligence capabilities, human resources and, even, communication infrastructure. In fact, collective defense can not only deal with ‘detecting’ and ‘responding to’, but it can also undertake active defense operations (Ilina 2015).

Another definition comes from International Telecommunication Union (hereafter ITU), which defines cyber security as:

> The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality (Klimburg 2012).

In spite of these different existing definitions, nation states either have their own definitions or do not define the term ‘cyber security’ at all. On the other hand as far as the term ‘cyber defence’ is concerned, according to some of the experts when the term ‘defence’ is paired with ‘cyber’ it usually is within a military context, but also may take into account criminal or espionage considerations. For instance the US Department of Defense (DoD) used the term ‘Computer Network Defense’ and defined it as: ‘actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the DoD information systems and computer networks’ (DoD JP 1-02 2010). This term has now been replaced by the use of ‘cyberspace defense’ defined as: “Cyberspace defense actions are taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach the cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration” (DoD JP 3-12 2018). At times when definitions start getting complex, Kruger considers cyber security as radically simplified and emphasises, ‘If we move primary information security into the information itself. With today’s processors, storage density and the right engineering, it is possible to make every piece of information a ‘hard target’ that protects itself and is still easy to use. The focus of cyber security can shift from the utterly impossible (defending the undefendable perimeter and persuading the unpersuadable user) to the merely difficult (moving information out of the clear)’ (Kruger 2014).

One more simple way of understanding the concept has been put forward by ITU, which in its report while differentiating between information security and cyber security asserts that information security focuses on confidentiality, while cyber security focuses more on integrity and availability (ITU 2011). Thus, according to the report cyber security is information security with jurisdictional uncertainty and attribution issues. Another simple outlook emerges from the Dutch definition of cyber security, which contemplates the ‘freedom from danger or damage due to the disruption, breakdown, or misuse of ICT’ (Klimburg 2012). Yet another interesting insight comes from Germany’s cyber security strategy, which distinguishes between two concepts – the internet as a public good and the internet as a public space – leading to different lines of action. The internet as a public good requires cyberspace security, meaning resilience of IT infrastructure, integrity, and availability of systems and data; whereas the internet as a public space requires security in cyberspace, which includes secure action in the cyber realm, authenticity, integrity, confidentiality of data and networks, legal security and legal obligation, security against crime and malicious activities. In spite of all these different definitions, Klimburg sums them up as:

The common theme from all of these varying definitions, is that cyber security is fundamental to both protecting government secrets and enabling national defence, in addition to protecting the critical infrastructures that permeate and drive the 21st century global economy. The slight differentiation in definition between governments and inter-government organisations is irrelevant, as their shared focus on the issues illustrates the first step in the long journey to actually providing for cyber security – no matter what the definition. (Klimburg 2012)

However, absence of cyber security and other related terms can lead to a significant level of confusion within one's own country. Moreover, as the cyber threat is global, proper definitions assist in understanding the cyber security approach of other nations, alliances, and international organisations and vice versa. Taiwan had also not defined it until its Cyber Security Management Act (CSMA) was passed in 2018. The Act states cyber security 'refers to such effort to prevent information and communication system or information from being unauthorized access, use, control, disclosure, damage, alteration, destruction or other infringement to assure the confidentiality, integrity and availability of information and system' (CSMA 2018).

National Cyber Security Debate

The term 'National Cyber Security (NSC)' is increasingly being used in official documents and policy discussions. It is also used by government spokespersons, but has hardly been well defined leading to improper understanding of the concept. Comparing it with cyber security Klimburg argues, 'It is very similar to the wider subject of cyber security itself – where common interpretations and implied meanings are much more frequent than universally accepted and legally-binding definitions.' Experts like Ilina, Klimburg etc. agree with the fact that there is no universally agreed definition of 'National Cyber Security (NCS)', however Klimburg argues, 'NCS has two obvious roots: the term 'Cyber Security' and the term 'National Security' – both of which are often differently defined in official national documents. Even if the term 'national cyber security' is seldom explicitly defined, it is possible to derive a working definition based on the respective use of the other two terms.'

Even Ilina also asserts, ‘A universal, agreed definition of NCS does not exist. Some that are a symbiosis of ‘Cyber Security’, ‘National Security’, etc. can be found in the strategic state documents. That means each country defines these concepts depending on their own vision.’ The US asserts that the term ‘National Cyber Security’ implies the protection of the .mil and .gov domain, and the ability of the systems within these domains to operate normally at home and abroad (DoD 2011). NATO National Cyber Security Framework Manual (Klimburg 2012) , which is an extensive study of NCS, describes NCS in terms of: Three Dimensions (the Governmental, the National or Societal and the International); Five Mandates (Military Cyber, Counter Cyber Crime, Intelligence and Counter-intelligence, Critical Infrastructure Protection and National Crisis Management, Cyber Diplomacy and Internet Governance); and Five Dilemmas (Stimulate Economy Vs Improve National Security, Infrastructure Modernisation Vs Critical Infrastructure Protection, Private Sector Vs Public Sector, Data Protection Vs Information Sharing, Freedom of Expression Vs Political Stability). It means NCS need to accommodate and address at least these many factors.

This study defines ‘National Cyber Security’ as: ‘The focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security.’ However, the study also recognises that National cyber security is a tool to reach a desired state of affairs, not an end in itself. While talking in terms of means and ends, Ilina emphasises, ‘It must be made clear that the National Cyber Security (NCS) is not an end itself. It is a tool to reaching the desired wellbeing of the individual, group of people, organizations, nations and world population. Most of the countries find defining a NCSS as a goal that will provide a secure virtual environment which guarantees economic growth, stable development and protection of people from various risks’ (Ilina 2015).

Taiwan’s NCSS Trajectory and Current Posture

The most recent official cyber security strategy document published by Taiwan came in 2021, titled ‘National Cyber Security Program of Taiwan (hereafter NCSP) 2021-24’, which is the sixth phase of Taiwan’s long term program that was initiated long back in 2001 (for plan/program since 2001 refer to Fig. 1) by the Executive Yuan, the highest administrative organ of Taiwan.

In the first phase (2001-2004), national information and communication security organizations and emergency centres were established, and government bodies were encouraged to set up ‘Information and Communication Security Teams’, defining ‘Ensure a secured and reliable information and communication environment’ as the goal of this period. In the second phase (2005-2008), the Government planned four policy goals: ‘Shorten the timing of notification’, ‘Enhance the protection ability for information security’, ‘Reinforce understanding and education in information security’, and ‘Promote international cooperation’. The third phase (2009-12) included: Critical Information Infrastructure Protection; Developing Emergency Response and Recovery Capabilities; Information System Classification and Categorisation; Strengthening e-commerce as the key focus.

Taiwan government, through its second and third phase ‘Plan and Program’, claims, ‘With the collaborative efforts of agencies from central government, special municipalities and local government, the interim objective of ‘establishing an overall information security protection system and improving information security protection capabilities’ has been achieved in the prescribed order’ (NCSP 2005-08 and 2009-12). Taipei also claimed, ‘Three implementation phases of the Mechanism Plan or Development Program have been completed, and information security management system has become increasingly robust. Personal information security awareness has also been raised.’ Yet another claim by Taiwan states:

> By implementing the 30 action plans, the following benefits were achieved in late 2012: increased investment in information security resources, improved readiness in information security regulations, enhanced national information security awareness, strengthened overall information security protection capability, increased frequency of information security drills, and reduced severity in information security incidents. Measures implemented in government agencies have been gradually made available to the private sector and enterprises (NCSP 2009-12).

Keeping these claims as the base, Taiwan unfolded the 4th Phase (2013-16), whose vision was: ‘Building a secure information security environment and becoming a high quality e-society’. This vision aims to gradually promote and implement a high-quality network community under the guidance of forward-looking policies and with joint efforts from both the public and private sectors, as well as with the support of Taiwan's combined resources and strengths. This vision is further translated into strategic objectives and in order to achieve these objectives a series of implementation strategies and action plans have been included in the 4th Phase.

The next two NCSPs of Taiwan (NCSP 2017-20 and 2021-24) follow a similar outline. Before talking about their visions, objectives, promotional strategies and tactical approaches, both discuss in detail: the Global Cyber Security Threats and International Policy Trends; Current State of Promotion of Cyber Security in Taiwan. The objective of 5th Phase was to 'promote the Cyber Security Management Act' (enacted in 2018) and 'complete National Cyber Security United Defense System'. Visions of both the phases also sounded slightly similar, which was to 'build Taiwan as a safe and reliable digital country' and to 'build Taiwan as a safe and resilient smart country' respectively. However, the current phase (2021-24 Fig. 2) emphasises on making Taiwan a cyber R&D hub, bolstering Taiwan's proactive defence, public-private partnership, and enhancing the resilience of critical infrastructure.

In later part, the document does a SWOT (Strength, Weakness, Opportunity and Threat) analysis of advantages and disadvantages of its internal environment and the opportunities and threats from the internal environment. It also 'adapt TOWS matrix to conduct strategic analysis on the aforementioned SWOT, using strengths, weaknesses and opportunities to formulate offensive strategies and transition strategies; then based on strengths, weaknesses and threats to formulate avoidance strategies and hedging strategies.'

It is worth paying attention here that Taiwan, after establishing first of its kind independent military cyber command (ICEF) in 2017, is now adopting proactive defence strategy and is also carefully weighing its option of choosing avoidance and hedging strategies. With its two decades long cyber strategy, Taiwan now seems to be more confident and articulate. President Tsai's 'cyber security is national security' strategy is predominantly visible in the fifth Phase, as it highlights 'building a National Cyber Security United Defense System', in which defending Taiwan's eight critical infrastructure sectors is at the core. This has been seen as Taiwan's attempt towards attaining 'Cyber Autonomy' (Hsu 2018), which is also clearly reflected in Taiwan's 'National Defense Report' of 2017 and 2021 (NDR 2017, 2021).

China Factor in Taiwan's Cyber Security

The first documented 'Taiwan-China Hacker War' took place in 1999 (Pryor 2019). In March 2015, the former Vice Premier of Taiwan, Simon Chang (張善政), left no doubt as to what was the principal threat Taiwan facing today. He said, 'Taiwan has no enemy in the international community except you-know-who (Gold and Wu 2015). Who in the world would try to hack Taiwan?' Earlier Chang has also served as a Minister of Science and Technology and also as a director of Asia hardware operations for internet giant Google Inc. Chang also said the percentage of cyber attacks on government systems originating from mainland China was 'very high'. In 2014 Chang in an interview revealed, 'Chinese cyberwar units have been engaging with Taiwan units almost every day, with some severe attacks every few months' (Tiezzi 2014). According to statements given by Tsai Teh-sheng, the director of Taiwan National Security Bureau, in one year, the bureau encountered more than three million hacking attempts from China (Gold 2013). Jens Damm claims, 'Despite improved cross-strait economic and cooperative relations in past several years, Taiwan considers mainland China a major threat to its security. Taiwan has been recipient of mainland launched cyber attacks for more than a decade' (Damm 2015). A Reuters report also claims that the island nation has endured at least a decade of highly-targeted data-theft attacks from China of the kind that are now clearly being directed towards larger countries (Gold 2013).

Major General Tschai Huichen, Taiwan's first female combat-status General, talks about three risks emanating from China: First, 'General Information Security Threats' like malwares, fake websites etc.; Second, 'Strategic Information Warfare' like media stories shaping the perception of Taiwan's population; Third, 'Information Warfare' through China's 'Cyber Army' and the use of paid individuals who pose as ordinary citizens making comments on the internet. Colonel Hsieh You-lin, characterises the threats from China in terms of the '3 Non-Operations': 'Non-Contact' (over the horizon); 'Non-Linear' (No fixed frontline); and 'Asymmetric Operations' (Bolt and Shearn 2015). Jim Liu, a Taiwanese security researcher, of California-based application security company Lucent Sky, says two types of viruses come from mainland China. 'There is sophisticated malware that is likely developed by the state or state-sponsored organisations, which are almost always targeted,' he said, 'There is also a large amount of simpler malware that targets everyone (including people and organisations within

China) (Zappone 2014)' According to National Security Bureau (NSB) report of April 2013, described China as being armed with a cyber army of more than 100,000 people. The report outlined the counter-measures taken by other countries against increasing state-sponsored cyber attacks. It also added that the PRC has allocated more than $80 million to its cyber war workforce in 2013. The NSB director described the Chinese cyber threat as 'very severe.'

Apart from these opinions, incidents of cyber attacks, in which China was involved, speak for themselves. In 2013, Taiwan's Coast Guard Administration computers were compromised, resulting in loss of 3,000 classified documents (Bolt and Shearn 2015). The NSB 2013 report revealed that the agency's external websites were hit by hackers 3.34 million times in 2012. In 2011, hacking attacks on Democratic Progressive Party (DPP) and Tsai Ing-wen presidential campaigns were traced to IP address to Xinhua, the official Chinese news service, although there were doubts about the true source of the attack. Perhaps 2005 breach may have given China access to all the data from Han Kuang 21 military exercise (Hsiao 2013). The first widely reported 'hackers war' in the world occurred between China and Taiwan in 1999, when then Taiwan's president Lee Teng-hui infuriated Beijing by suggesting the two countries accept state-to-state relations, rather than the status quo in which Taiwan eschews independence from Beijing despite having its own government (Zappone 2014). Chinese hackers responded by sabotaging government, university and commercial sites. These attacks reportedly involved more than 160 infiltrations of Taiwan's national computer networks (Hsiao 2013). The hackers also attacked the American Institute in Taiwan's website. Another incident happened in 2003, when a Taiwanese police agency realised hackers had stolen personal data, including household registration information, from its computer system (Gold 2013). Again in 2003, Chinese hackers were able to penetrate the computer networks of the governmental agencies of Taiwan, notably the Ministry of Defence, Election Commission and the National Police Administration (Sharma 2016). According to a Taipei Times report, China's 'Internet army' initiated more than 7.22 million cyber attacks on the NSB's websites in the past year, including 230,000 hostile attacks (Lo and Chen 2015). Due to so many cyber attacks, government employees of Taiwan are issued with two computers - one connected to the internet, and a second that remains offline for security reasons (Zappone 2014).

There are many such known as well as many unknown cyber intrusions, some of them are discovered many years after they actually take place. China's involvement in cyber attacks against Taiwan is also visible from their work pattern. For example, a Reuter report claims that people expect hackers to be night owls, but these guys (Chinese hackers) work very normal hours - on Chinese national holidays, for example, Taiwan does not see any hacking activity at all (Gold 2013). Another report asserts that while the traditional focus of Chinese cyber attacks has been on an adversary's government networks, however they have shifted their focus to civilian think tanks, telecommunications service providers, internet node facilities and traffic signal control systems. This trend appears consistent with the modus operandi of some Chinese hacker group activities against U.S. targets.

Involvement of China and PLA in cyber attacks against Taiwan keeps on appearing in Taiwan's official documents and also in many other academic reports. For instance, Taiwan's National Defence Report of 2013 claimed, 'Starting in 2010, the PRC began developing new spy software to steal classified information on the internet. The software was developed with automated functions capable of changing data encryption, concealing transfer channels, and countering tracing attempts by network security personnel.' Talking about the PLA's cyber capabilities, the 2015 Defence Report claims:

> The PLA has established basic offensive and defensive cyberwarfare capabilities at various military departments that include its military commands, 7 military regions, defense research agencies, defense mobilization information systems, and militia forces. In addition to using hackers to plant backdoors for stealing and transferring data, the PLA is also capable of using programs to acquire control privileges over the target server. PLA cyberwarfare units have also managed to infiltrate a target and remain undetected for 1,700 days. These cyberwarfare units are large and highly specialized organizations capable of dealing with information defence technologies employed around the world (NDR 2015).

Another important document, which talks elaborately about PLA affiliations, the Project 2049 Institute's 2011 report elaborated:

There are at least two bureau-level People's Liberation Army (PLA) units conducting cyber-espionage on Taiwan: they are the PLA Third Department's Sixth Bureau having a military unit cover designator of 61726, headquartered in Wuhan's Wuchang district; and the Nanjing Military Region's Technical Reconnaissance Bureau. The Nanjing MR Headquarters

Department, led by former General Staff Department (GSD) Second Department (military intelligence) Director Major General Yang Hui, oversees two TRBs that are likely focused on Taiwanese military and other communications and computer networks, as well as U.S. activity in the Western Pacific area of operations (Stokes, Lin and Hsiao 2011)

In terms of military capabilities mainland China's military strength is superior to that of Taiwan as PLA has roughly 10 times the number of troops as Taiwan's military (Demms 2015). Although, after recent military reform by Xi Jinping, PLA has decided a huge reduction of 300,000 PLA personnel by 2017, bringing the size of the active duty PLA down to two million, however the capabilities still seems to be in the favour of China (Allen, Blasko 2016). In response to the shifting Balance of Power, Taiwan has adopted a new defence posture. Over past two decades, it has significantly boosted its combat and asymmetric warfare capabilities on several fronts. In response to increased attacks from mainland, Taiwan engages some 3200 military personnel in cyber security (Demms 2015). However, Taiwan's own military cyber units were outnumbered (Tiezzi 2014) by their Chinese counterparts, which according to Taiwan's estimates: China has 100,000 people at work in a national cyber army (Zappone 2014). It seems the newly created Strategic Support Force (SSF战略支援部队), which was introduced on 31 December 2015, looks after the key responsibilities of information warfare and cyber warfare. According to official sources SSF will form the core of China's information warfare force, which is central to China's 'active defence' strategic concept (Costello 2016).

Song Zhongping (宋忠平), a former PLASAF (Second Artillery Force) officer and a professor at the PLA Rocket Force's Equipment Research Academy revealed that SSF will be composed of three separate forces or force-types: space troops (天军), cyber troops (网军), and electronic warfare forces (电子战部队). The cyber force would be composed of 'hackers focusing on attack and defense,' the space forces would 'focus on reconnaissance and navigation satellites,' and the electronic warfare force would focus on 'jamming and disrupting enemy radar and communications.' On January 14 2016, the SSF's commander, Gao Jin (高津) asserted that the SSF will raise an information umbrella (信息伞) for the military and will act as an important factor in integrating military services and systems, noting that it will provide the entire military with accurate, effective, and reliable information support and strategic support assurance (Costello 2016).

As far as objectives and intentions behind Chinese indulgence in cyber attacks against Taiwan are concerned, Taiwan seems to be worried for a variety of reasons. Chang specifically noted that ‘many of the attacks were aimed at stealing relevant information for use in negotiations with Taiwan,’ raising concerns that China is seeking leverage over what it considers a breakaway province. Chang also said the attacks, which occur almost daily, often target confidential information on Taipei’s bottom line for cross-strait negotiations (Tiezzi 2014). Apart from getting relevant and confidential information another Chinese intention, as suggested by Jens, is use of cyber network operations (CNO) as a tool to collect strategic intelligence. Moreover, Chang pointed out one more objective: China often uses Taiwan as an experimental target for new hacking techniques. This claim was also backed by Reuter’s report which asserts that Taiwan has become a rehearsal area for the Chinese cyber attacks. In this regard, Jens also pointed out, ‘It appears that mainland China uses Taiwan as a testing ground before it attacks the US.’ Chang further warned about Chinese intentions behind attacking Taiwan’s networks: there was potential for hackers to use Taiwan as a back door into the US systems.

Yet another motive of Chinese hackers, according to one report is Taiwanese trade secrets, as Taiwan is the producer of high technology products including 90 per cent of world’s laptops. Apart from all these, Taiwanese experts are also concerned that China could use cyber attacks to cripple the island’s infrastructure (Zappone 2014). The director general of Taiwan’s National Security Bureau emphasised that China’s cyber attacks are ‘not just stealing information, but possibly gradually focused on destroying our infrastructure.’ There are threats of disrupting and destroying military infrastructure as Taiwan’s NDR 2015 also mentions,

> The aim of cyber attacks is to disrupt the ROC Armed Forces command and control information system operations and delay its ability to respond in a timely manner to various incidents. The PLA may launch attacks against specified targets in the ROC through internet in the future with the aim of crippling national infrastructure system operations. Such attacks will pose severe threats to ROC military operational capabilities and national security.

However according to China’s position it follows the policy of ‘No First Use of Cyber Weapon’ and will not target civilian infrastructure(s) (Li 2012). This policy leads to the last yet most significant intention that is building up of cyber weapons for a full-fledged cyber war or using cyber war as a pre-emptive option just before actual outbreak of war against Taiwan.

Capabilities and Global Ranking

Although, Taiwan’s NCSPs are primarily focused on civilian sector and overall national cyber security, however some sections do have implications for military domain. Taiwan’s NDRs, on the other hand are more focused on military cyberspace. It is also worth noting that China has not been mentioned in any NCSPs, however NDRs have explicitly mentioned China many times and have drafted Taiwan’s cyber strategies vis-à-vis China’s cyber capabilities. NDR 2021 emphasises:

> Through organizational reform and realignment over the years, the PRC has been vigorously enhancing its cyber warfare capabilities. In peacetime, its cyber activities are centered on gathering or stealing intelligence, getting hold of key nodes of subject systems, and compiling a targeting list for cyber-attacks during the precision strike phase of future operations. In wartime, these activities are transitioned to sabotaging and destroying subject’s national critical infrastructures and C2 systems to cause turbulence and chaos in its society and decimate the internal security kept by the military and law enforcement organs of the nation and its government functions.

NDR 2021 also identifies ‘Threat of Cognitive Warfare from PRC’:

> Cognitive warfare is used to sway the subject’s will and change its mindset, and is not confined by time and space. Concerning its conventional applications, cognitive warfare is originated from the rationales of intelligence warfare, psychological warfare, and public opinion warfare. From the perspective of innovation, it can make use of highly efficient modern computing systems, the internet, and social media, to twist the subject’s social ideologies, mentality, and the sense of law-and-order through cyber infiltrations and manipulation of mentality and public opinions. The PRC is exploiting the tactics of cognitive warfare, mixing with ‘Three Warfares,’ which are

psychological warfare, public opinion warfare, and legal warfare, to disseminate indiscernible disinformation, and carrying out means of verbal attacks and saber-rattling in an attempt to create postures to its own favor.

The consequence of cognitive warfare can be seen in form of meddling of the US Presidential election 2016, which can have huge repercussions for any democracy including Taiwan (Abrams 2019).

In order to counter China, NDRs suggest building up Taiwan’s cyber capabilities. NDR 2017 talks about building Taiwan’s asymmetric/innovative capabilities in order to tackle China: ‘The ROC will not engage in an arms race with the PRC in the face of its huge military threat, but will apply asymmetric capability to achieve relative advantage for our Armed Forces and ensure that the “resolute defence, multi-domain deterrence” military strategy is implemented.’ NDR 2021 reiterates, ‘Facing a rapid military growth and intensifying threats from the PRC, the Armed Forces have to employ an innovative and asymmetric thinking without intentions to compete in an arms race to actively plan and acquire weapons and equipment that meet our demands for defensive operations, and build up our forces based on our military strategy of “resolute defence and multi-domain deterrence”.’

Taiwan’s current capability build-up highlights six categories and cyber warfare is one of them. Taiwan also ‘plans to acquire joint capabilities focused on standoff strike; counter-air operations; sea control operations; homeland defense; information, electronic, and cyber operations, and joint C2ISR.’ Establishment of ICEF in 2017 can be seen in as an attempt of strengthening Taiwan’s cyber capabilities, whose mission was to:

> ‘…to integrate the information, communications and electronic capabilities of the Army, Navy and Air Force. In peacetime, its mission is to protect the various information communications and electronic systems of the Armed Forces, defend national defense information networks and support national-level cyber defense. In wartime, the ICEFCOM’s mission will be to ensure the effective operation of the Armed Forces’ command and control networks, information security, and intelligence, surveillance and reconnaissance systems to protect homeland security.’ (NDR 2017)

In order to further strengthen its cyber capabilities, Taiwan also plans to shift resources ‘to high level cyber security scientific research’, promote ‘transnational talent exchange and research cooperation’ and ‘cultivate high quality cyber security talent’, so as to develop Taiwan as ‘cyber security research and training hub in Asia-Pacific’ and to establish ‘Cyber Security Center of Excellence’.

Furthering of capabilities can also be observed in Taiwan’s participation in cyber drills and competition. In this regard, NDR 2021 underlines:

> To deal with cyber threats, the Armed Forces are dedicated to maintain cyber security by performing multiple approaches, such as cyber defense and cyber battlefield management. We have created a training site for cyber offenses and defenses with simulated scenarios for realistic cyber warfare drills in which the participants are divided into group A and group B to execute a force-on-force cyber operational training. We continue verifying the effectiveness of our cyber warfare gears and the quality of our specialists in cyber warfare by following the training requests of “being tough and difficult for achieving excellence and robust.

Taiwan also organises annual ‘Han Kuang*’* exercise, with cyber drills as a part of it. The focuses of the exercise include: protecting cyberspace, improving early warning, enhancing command and control, protecting critical information facilities, countering unmanned aerial vehicles (UAV) and guided weapon attacks, verifying the abilities of the deployment of new capabilities, coordination of interagency efforts, and integration of joint firepower (Abrams 2019). While participating in another cyber drill, Taiwan also claimed, ‘ROC came in an impressive 2nd place in the 2017 DEFCON CTF, showing the world its remarkable capabilities of information security’ (NDR 2017).

Various comparisons of military strength between Taiwan and China reveal that the balance is in the favour of China (Brimelow 2022). Even in terms of military expenditure, Taiwan is way behind China (12155 and 252304 M. USD respectively in 2020) (SIPRI 2020). Although, Taiwan does not explicitly mentions number of military personnel involved in defending Taiwan’s cyberspace, however it boasts about its talented hackers and using their skills. ‘There are bountiful high-quality information-related talents and high level hackers in Taiwan' 'Since 2016, Taiwan has promoted training course of "Taiwan Cool Hacker"' (NDR 2021).

Taiwan's capabilities can also be observed in terms of global and regional indices and rankings, issued by various studies. According to one of the studies, Taiwan ranked ninth in the Australian Strategic Policy Institute (ASPI) cyber maturity in the Asia-Pacific report. Taiwan received a weighted score of 56.9, which was based on governance, financial cybercrime enforcement, military application, digital economy and business, and social engagement (Hanson, Uren 2017). Another study claims, 'Taiwan ranked 18th place in Global Government AI Readiness Index 2021." It further states, "Taiwan is a good example for other countries in East Asia, scoring 70.49 out of 100 in Innovation Capacity and having established an R&D framework based on co-innovation between Taiwanese and international companies (Pablo, Annys 2021).'

Yet another study expresses, "Taiwan would be hypothetically ranked 26th out of 122 economies, when considering its performance in only three (of the four) pillars of the Network Readiness Index: Technology, People, and Governance." The study also claims, "As for its region—Asia & Pacific—Taiwan would be hypothetically ranked 7th out of 22 economies. Its overall score is greater than the regional average, as are its scores in each of the three pillars. Taiwan is the region's top performer when it comes to ICT usage and skills of Individuals."

Taiwan's cyber capabilities cannot be just quantified in numbers and rankings, it should also be seen in the backdrop of 'Taiwan Relations Act'. After joining office President Biden, in 2021, pointed out in his Interim National Security Strategic Guidance that Taiwan is a critical economic and security partner with the U.S., and the U.S. will assist Taiwan in its self-defence and international participation. The US in its 'Indo-Pacific Strategy Report' mentions,

> The objective of our defense engagement with Taiwan is to ensure that Taiwan remains secure, confident, free from coercion, and able to peacefully and productively engage the mainland on its own terms. The Department is committed to providing Taiwan with defense articles and services in such quantity as may be necessary to enable Taiwan to maintain a sufficient self-defense capability.

Since 2008, the US Administrations have notified Congress of more than $22 billion in foreign military sales (FMS) for Taiwan.

The involvement of the US itself plays a great role in enhancing Taiwan's cyber capabilities. Moreover, the US sophisticated FMS to Taiwan also act as another factor in strengthening Taiwan's capabilities. In this regard, to further bolster Taiwan's capabilities, Julia Cunico advocates a 'US-Japan-Taiwan trilateral cooperation'. Julia also asserts, 'Because cyber threats range across a broad spectrum, there are a number of steps that Taipei, Tokyo, and Washington can take to institutionalize cyber cooperation.' Julia further emphasises, 'US-Japan-Taiwan cooperation on offensive cyber weapons is a bridge too far, establishing strong ties in cyber defence would lay the foundation should offensive cooperation be necessary. This potential alone would signal to Beijing that escalating Chinese cyber activities could have a substantial cost' (Cunico, Liao 2015)

In 2020, 'Nearly 15 million cyber incidents' were reported against Taiwan (TWCERT 2020), on the other hand number of reported incidents against China 'were 101.3 thousands' (CNCERT 2020). In 2019 report, Taiwan reported 12 million 'Indicators of Compromise' whereas China reported 107.8 thousands. Number of reported incidents against Taiwan has been increasing with each passing year (refer to Table 1). The incidents against Taiwan in 2020 were separated separated in 11 categories, out of which 'intrusion and botnet' were 'the top two common types of attacks of cybersecurity in 2020' (APCERT 2020). As far as vulnerabilities are concerned, more than 1200 vulnerabilities were reported in 2020, out of which 'SQL-injection, Remote code execution, and information leakage' were the top three most common types of vulnerabilities (APCERT 2020). It is obvious from these reports that Taiwan, being a small island, faces way more cyber incidents in comparison to that of China and keeping Taiwan on its toes.

Conclusion

Taiwan's NCSS, enable government departments and ministries to translate a government's national security vision into coherent and implementable policies. It also provide guidance to policy-makers regarding cyber policy priorities and potential resource allocations. NCSPs includes political, internal security, stakeholders' participation framework at national level and NDRs discuss cyber security in Taiwan's military domain. These documents do convey Taiwan's strategic thinking to other states and the international community at large. It also encourages international exchanges with like-minded partners. Nevertheless, due to unique cross strait relation, Taiwan's participation in international activities remain fairly limited. Still Taiwan enjoys the advantage of well-developed ICT industry and skilled human resource, which can be utilised properly for national cyber security and related R&D purposes.

Although China's growing cyber capabilities is a huge concern for Taiwan, but at the same time it also acts as a catalyst for developing Taiwan's cyber security framework. In spite of the fear of a possible cross-strait conflict, Taiwan's NCSPs or NDRs do not declare where the red lines are; or what acts in cyberspace would be considered by Taiwan as unacceptable or equivalent to war. Hence, NCSPs do not serve the purpose of being a deterrent as it may first require developing advanced and sophisticated capabilities. Nevertheless, the document acts as a blueprint for building 'Taiwan as a safe and resilient smart country', which is also reflected in Taiwan's confident policy posture, proactive defence strategy, attempt of building a 'National Cyber Security United Defence System' and enhance the resilience of critical infrastructure. Building 'resilient cyberspace' is a key feature of Taiwan's NCSPs, which implies having the ability to prepare for, respond to and recover from (even the worst case scenario - China's attack) cyber-attacks. Thus, in spite of the name being invisible from NCSPs, China as a threat, is pretty much present in NCSPs. On the other hand Taiwan's NDRs do explicitly mention China many times as an eminent threat and also analyses the nature of threats posed (including cyber, cognitive, public opinion, psychological and other form of warfare). NDRs does not shy away from providing guidelines for government agencies to operate both in the situation of peace and conflict.

Cyber issues started emerging as international issue in late 2000 and the two largest economies started discussing cyber issues as late as 2013, however Taiwan has been working on developing cyber policy and strategy as early as 2001. These documents do an excellent work not just by putting forward Taiwan's policies, priorities, plans and strategies but also by classifying and allocating the works to respective organisations, with the option of reviewing the works before completion. It would be interesting to see how much of the current Program has been transformed into actual capabilities, once it is reviewed as it would form the basis of Taiwan’s next National Cyber Security Program.

Figures and Table

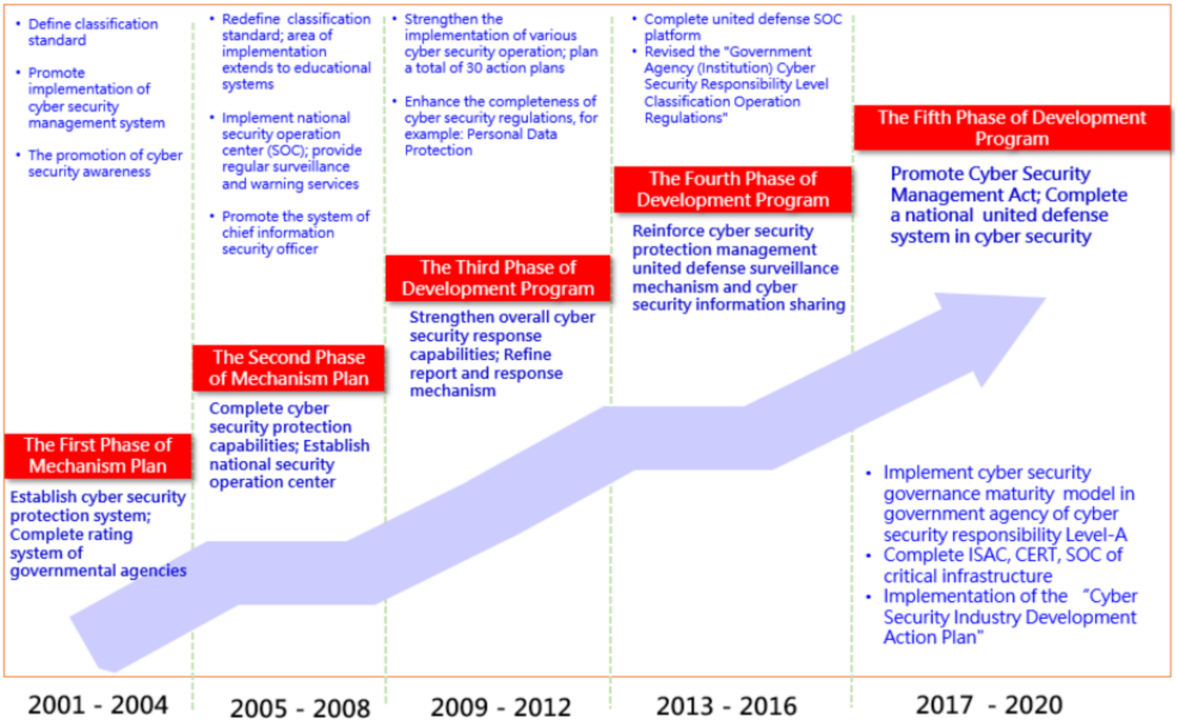
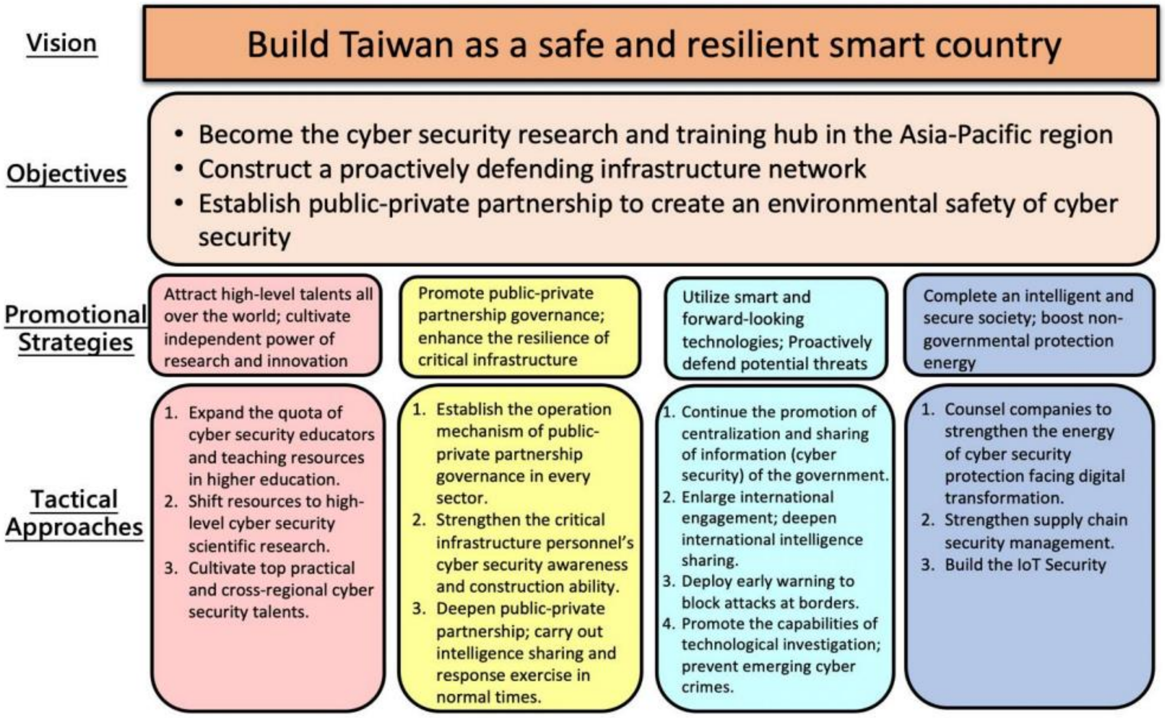

• Define classification standard
• Promote implementation of cyber security management system
• The promotion of cyber security awareness
The First Phase of Mechanism Plan
Establish cyber security protection system; Complete rating system of governmental agencies
• Redefine classification standard; area of implementation extends to educational systems
• Implement national security operation center (SOC); provide regular surveillance and warning services
• Promote the system of chief information security officer
The Second Phase of Mechanism Plan
Complete cyber security protection capabilities; Establish national security operation center
• Strengthen the implementation of various cyber security operation; plan a total of 30 action plans
• Enhance the completeness of cyber security regulations, for example: Personal Data Protection
The Third Phase of Development Program
Strengthen overall cyber security response capabilities; Refine report and response mechanism
• Complete united defense SOC platform
• Revised the "Government Agency (Institution) Cyber Security Responsibility Level Classification Operation Regulations"
The Fourth Phase of Development Program
Reinforce cyber security protection management united defense surveillance mechanism and cyber security information sharing
The Fifth Phase of Development Program
Promote Cyber Security Management Act; Complete a national united defense system in cyber security
• Implement cyber security governance maturity model in government agency of cyber security responsibility Level-A
• Complete ISAC, CERT, SOC of critical infrastructure
• Implementation of the "Cyber Security Industry Development Action Plan"
2001 - 2004
2005 - 2008
2009 - 2012
2013 - 2016
2017 - 2020

Fig. 1. Five Phases of National Cyber Security Program of Taiwan

(Source: NCSP 2021-24)



Vision

Build Taiwan as a safe and resilient smart country

Objectives

- Become the cyber security research and training hub in the Asia-Pacific region
- Construct a proactively defending infrastructure network
- Establish public-private partnership to create an environmental safety of cyber security

Promotional Strategies

Attract high-level talents all over the world; cultivate independent power of research and innovation

Promote public-private partnership governance; enhance the resilience of critical infrastructure

Utilize smart and forward-looking technologies; Proactively defend potential threats

Complete an intelligent and secure society; boost non-governmental protection energy

Tactical Approaches

1. Expand the quota of cyber security educators and teaching resources in higher education.
2. Shift resources to high-level cyber security scientific research.
3. Cultivate top practical and cross-regional cyber security talents.

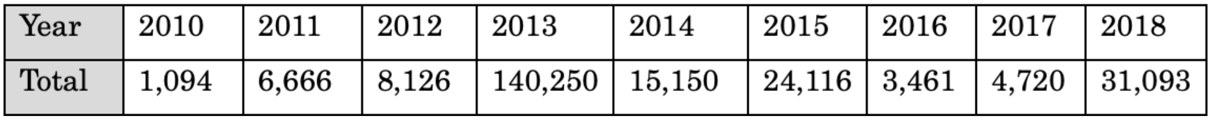
1. Establish the operation mechanism of public-private partnership governance in every sector.
2. Strengthen the critical infrastructure personnel's cyber security awareness and construction ability.
3. Deepen public-private partnership; carry out intelligence sharing and response exercise in normal times.

1. Continue the promotion of centralization and sharing of information (cyber security) of the government.
2. Enlarge international engagement; deepen international intelligence sharing.
3. Deploy early warning to block attacks at borders.
4. Promote the capabilities of technological investigation; prevent emerging cyber crimes.

1. Counsel companies to strengthen the energy of cyber security protection facing digital transformation.
2. Strengthen supply chain security management.
3. Build the IoT Security

Fig. 2 Sixth Phase of Taiwan's National Cyber Security Program

(Source: NCSP 2021-24)



Year	2010	2011	2012	2013	2014	2015	2016	2017	2018
Total	1,094	6,666	8,126	140,250	15,150	24,116	3,461	4,720	31,093

Table 1. Reported Incidents (Year Wise)

(Source: TWCERT, 2020)

References

Abrams Abigail. 2019. ‘Here's What We Know So Far About Russia's 2016 Meddling’, 18 April, https://time.com/5565991/russia-influence-2016-election/ (accessed on 25 January 2022).

Allen Kenneth W., Blasko Dennis J., John F. Corbett, Jr. 2016 ‘The PLA’s New Organizational Structure: What is Known, Unknown and Speculation, Parts 1 & 2’, https://jamestown.org/wp-content/uploads/2016/02/The_PLA_s_New_Organizational_Structure_Parts_1_and_2_01.pdf?x60211 (accessed on 19 February 2022)

Asia Pacific CERT. 2020. APCERT Annual Report 2020, https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2020.pdf (accessed on 05 March 2022)

Asia Pacific CERT. 2019. APCERT Annual Report 2019, https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2019.pdf (accessed on 07 March 2022)

Bolt Paul J. and Shearn Benjamin. 2015. ‘Cyberpower and Cross-Strait Security’, in Chu Ming-chin Monique and Kastner Scot L. (ed), *Globalization and Security Relations across the Taiwan Strait*. London: Routledge.

Brimelow Benjamin. 2022. ‘New Pentagon charts lay out China's growing military advantage over Taiwan’, 18 January, https://www.businessinsider.in/international/news/new-pentagon-charts-lay-out-chinas-growing-military-advantage-over-taiwan/articleshow/88977859.cms (accessed on 18 February 2022)

Costello John. 2016. ‘The Strategic Support Force: China’s Information Warfare Service’, *China Brief* Vol. 16 Issue 3. https://jamestown.org/program/the-strategic-support-force-chinas-information-warfare-service/#.VxZ3sdR97IW (accessed on 24 February 2022)

Cunico Julia, Liao Nien-chung Chang, Daichi Uchimura, and John K. Warden. 2015. ‘Cybersecurity cooperation with Taiwan: an opportunity for the US-Japan alliance’, Pacific Forum CSIS, https://www.files.ethz.ch/isn/187513/Pac1504.pdf (accessed on 23 March 2022)

Demms Jens. 2015. ‘Cross-Strait Cyberspace: Between Public Sphere and Nationalist Battleground’, in Crookes Paul Irwin and Knoerich Jan (eds), *Cross-Taiwan Strait Relations in an Era of Technological Change*. London: Palgrave Macmillan.

Dewar Robert S. 2014. ‘The “Triptych of Cyber Security”: A Classification of Active Cyber Defence’, in P.Brangetto, M.Maybaum, J.Stinissen (eds), *6th International Conference on Cyber Conflict.* Tallin: NATO CCD COE Publications.

Eric Luiijf, Kim Besseling, and Patrick De Graaf. 2013. ‘Nineteen National Cyber Security Strategies,’ International Journal of Critical Infrastructures, Vol. – 9, No. 1-2, 3-31.

Global Times. 2016. ‘Zhongguo zhanlue zhiyuan budui quanqiu shouchuang huo jiang’ (中国战略支援部队全球首创或将配神龙空天飞机) [China's strategic support force is the world's first or will be equipped with Shenlong aerospace aircraft], 16 January, https://mil.huanqiu.com/article/9CaKrnJTdfI (accessed on 29 December 2021)

Gold Michael and Wu J.R. 2015. ‘Taiwan seeks stronger cyber security ties with U.S. to counter China threat’, 30 March, https://www.reuters.com/article/us-taiwan-cybersecurity-idUSKBN0MQ11V20150330 (accessed on 27 February 2022)

Gold Michael. 2013. ‘Taiwan A “Testing Ground” for Chinese Cyber Army’, 19 July, http://in.reuters.com/article/taiwan-cyber-idINDEE96H0KX20130718 (accessed on 09 February 2022)

Hanson Fergus, Uren Thomas (eds). 2017. ‘Cyber Maturity in the Asia-Pacific Region 2017’, The Australian Strategic Policy Institute, International Cyber Policy Centre, http://ad-aspi.s3.ap-southeast-2.amazonaws.com/2017-12/ASPI%20Cyber%20Maturity%202017_AccPDF_FA_opt.pdf?VersionId=hDv5_AxfVWgwCA_q8it1_H1wkH_HwZjb (accessed on 13 March 2022)

Hsiao Russel. 2013. ‘Critical Node: Taiwan’s Cyber Defense and Chinese Cyber Espionage’, China Brief, Vol. XIII, Issue 24

Hsu Philip. 2018. ‘Taiwan’s Multipronged Quest for National Cybersecurity’, 26 July 2018, https://international.thenewslens.com/article/100683 (accessed on 27 December 2021).

Ilina Armencheva. 2015. ‘Aspects of Policies and Strategies for Cyber Security in The European Union’, Journal of Defence Resources Management, Vol. 6, No. 2, 37-44.

International Telecommunication Union. 2011. *ITU National Cybersecurity Strategy Guide*. Geneva: International Telecommunication Union. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf (accessed on 29 Nov 2021)

Klimburg Alexander (Ed.). 2012. *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE Publication.

Klimburg Alexander and Tirmaa-Klaar Heli. 2011. *Cybresecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*. Belgium: European Parliament.

Kruger Dan and Carbone John N. 2014. ‘Radically Simplifying Cybersecurity’, in Sang C. Suh, U. John Tanik, John N. Carbone, Abdullah Eroglu (eds), *Applied Cyber-Physical System.* New York: Springer, 51-61.

Li Zhang. 2012. ‘A Chinese Perspective on Cyber War’, *International Review of the Red Cross*, Vol. 94, No. 886, 801-807.

Lo Tien-pin and Chen Wei-han. 2015. ‘NSB to set up cybersecurity arm to fend off China’**,** 24 February, http://www.taipeitimes.com/News/taiwan/archives/2015/02/24/2003612132 (accessed on 19 January 2022)

McAfee Report. 2018. ‘Economic Impact of Cybercrime – No Slowing Down’, https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf (accessed on 18 January 2022)

Pablo Fuentes Nettel, Annys Rogerson, Tom Westgarth, Kate Iida, Horlane Mbayo, Alejandra Finotto, Sulamaan Rahim and André Petheram. 2021. ‘Government AI Readiness Index 2021’, Oxford Insights, https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/61e95661c567937d21998d14/1642681965033/Gov_AI_Readiness_2021.pdf (accessed on 16 March 2022)

Pryor Crytal D. 2019. ‘Taiwan’s Cybersecurity Landscape and Opportunities for Regional Partnership’, in Glaser Bonnie S. and Funaiole Matthew P. (eds) *Perspectives on Taiwan: Insights from the 2018 Taiwan-U.S. Policy Program*, Center for Strategic and International Studies (10-15) https://www.jstor.org/stable/resrep22549.5?seq=1 (accessed on 19 January 2022).

Republic of China, Ministry of National Defense. 2021. National Defense Report 2021.

Republic of China, Ministry of National Defense. 2021. National Defense Report 2019.

Republic of China, Ministry of National Defense. 2021. National Defense Report 2017.

Republic of China, Ministry of National Defense. 2021. National Defense Report 2015.

Republic of China, Ministry of National Defense. 2021. National Defense Report 2013.

Republic of China, National Information and Communication Security Taskforce. 2004, *Establishing National Information And Communication Infrastructure Security Mechanisms Plan (2005-2008).* https://www.mnd.gov.tw/Upload/201110/10-%E8%B3%87%E8%A8%8A%E5%AE%89%E5%85%A8%E6%A9%9F%E5%88%B6-%E8%8B%B1%E6%96%87.pdf (accessed on 29 December 2021)

Republic of China, National Information and Communication Security Taskforce. 2020. National Cyber Security Program of Taiwan 2021-24

Republic of China, National Information and Communication Security Taskforce. 2016. National Cyber Security Program of Taiwan 2017-20

Republic of China, National Information and Communication Security Taskforce. 2012. National Strategy for Cyber Security Development Program 2013-16

Republic of China, National Information and Communication Security Taskforce. 2008. National Cyber Security Program of Taiwan 2009-12

Republic of China, National Information and Communication Security Taskforce. 2004. National Cyber Security Program of Taiwan 2005-08

Republic of China, National Information and Communication Security Taskforce. 2001. National Cyber Security Program of Taiwan 2001-04

Republic of China. 2010. ‘2010 nian zitong anquan zhengce baipishu’ (2010年资通安全政策白皮书) [ICT Security Policy White Paper 2010]

Robyn Klinger-Vidra. 2018. '*Cyber Security as National Security and Economic Opportunity in Taiwan*', 14 November, https://taiwaninsight.org/2018/11/14/cybersecurity-as-national-security-and-economic-opportunity-in-taiwan/ (accessed on 19 January 2022)

Sharma Munish. 2016. 'China's Emergence as a Cyber Power', *Journal of Defence Studies*, Vol. 10, No. 1 January-March 2016, pp. 43-68. http://www.idsa.in/system/files/jds/jds_10_1_2015_chinas-emergence-as-a-cyber-power.pdf (accessed on 18 January 2022)

SIPRI. 2020. SIPRI Military Expenditure Data 2020, https://sipri.org/sites/default/files/Data%20for%20all%20countries%20from%201988%E2%80%932020%20in%20constant%20%282019%29%20USD%20%28pdf%29.pdf (accessed on 19 February 2022)

Stokes Mark A., Lin Jenny and Hsiao L.C. Russell. 2011. 'The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure', Project 2049, https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf (accessed on 18 December 2021)

Su Yung-yao and William Hetherington. 2019. 'National Security A Top Priority: Tsai', 12 November, https://www.taipeitimes.com/News/front/archives/2019/11/12/2003725681 (accessed on 19 December 2021)

Tiezzi Shannon. 2014. 'Taiwan Complains of "Severe" Cyber Attack from China', 15 August, http://thediplomat.com/2014/08/taiwan-complains-of-severe-cyber-attacks-from-china/ (accessed on 18 January 2022)

United Nations Institute for Disarmament Research. Conference Report, http://www.unidir.org/files/medias/pdfs/conference-report-eng-0-373.pdf (accessed on 27 November 2021)

US Department of Defense. 2010. *Department of Defence Dictionary of Military and Associated Terms*. Joint Publication 1-02, 08 November 2010 (As Amended Through 15 February 2016). https://irp.fas.org/doddir/dod/jp1_02.pdf (accessed on 27 Nov 2021)

US Department of Defense. 2011. *Department of Defense Strategy for Operating in Cyberspace*. Washington DC.

US Department of Defense. 2018. *Cyberspace Operations*. Joint Publication 3-12, 08 June 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (accessed on 19 Dec 2021)

Zappone Chris. 2014. 'Taiwan A Canary in the Coalmine of Cyber Warfare' 08 December, http://www.theage.com.au/it-pro/security-it/taiwan-a-canary-in-the-coalmine-of-cyber-warfare-20141205-120v73.html#ixzz3zxVX4bIv (accessed on 27 February 2022).

ICS OCCASIONAL PAPER *Back Issues*

ICS Occasional Papers showcase ongoing research of ICS faculty and associates on aspects of Chinese and East Asian politics, international relations, economy, society, history and culture.

Issue No/Month	**Title**	**Author**
No.87|March 2021	Politics, Displacement and Identity: Kazakh refugees from Xinjiang in Bhopal during World War II	Madhavi Thampi
No.86|Feb 2021	Democratic Transition, New Taiwanese Identity, and Queer Rights Movements in Taiwan: Assessing the Linkages	Kaustav Padmapati
No.85|Feb 2021	Representation of 'Class' in Chinese Literature during the Reform Period: A Case Study of Wang Shuo's works	Manju Rani Hara
No. 84| Dec 2021	China's Prospects in Afghanistan: Opportunities and Adversities	Ashu Maan
No.83|Dec 2021	Looking Beyond the Crossroads: Rethinking China's Ecological Civilization amidst the COVID-19 Pandemic	Saloni Sharma
No. 82|Dec 2021	China's Environmental Diplomacy: From Sovereignty to Authoritarian Environmentalism	Shagufta Yasmin
No. 81|Dec 2021	Internal Drivers of China's External Behaviour	Shivshankar Menon

PRINCIPAL SUPPORTERS TO ICS RESEARCH FUND

TATA TRUSTS

MINISTRY OF EXTERNAL AFFAIRS
GOVERNMENT OF INDIA

INDIAN COUNCIL OF
SOCIAL SCIENCE RESEARCH

GARGI AND VIDYA
PRAKASH DUTT FOUNDATION

JAMNALAL BAJAJ
FOUNDATION

PIROJSHA GODREJ FOUNDATION

ICS PUBLICATIONS

ICS ANALYSIS
A short brief on a topic of contemporary interest with policy-related inputs

ICS OCCASIONAL PAPER
Platform for ongoing research of the ICS faculty and associates

ICS MONOGRAPH
Authored by the faculty, also emerging from research projects and international conferences

ICS WORKING PAPER
Draft paper of ongoing research

ICS JOURNAL

In its 57th year, *China Report* is a refereed journal in the field of social sciences and international relations. It welcomes and offers a platform for original research from a multi-disciplinary perspective, in new and emerging areas, by scholars and research students. It seeks to promote analysis and vigorous debate on all aspects of Sino-Indian relations, India-China comparative studies and multilateral and bilateral initiatives and collaborations across Asia.

China Report is brought out by Sage Publications Ltd, New Delhi.

Editor	Sreemati Chakrabarti
Associate Editor	G. Balachandirane
Assistant Editor	Rityusha Mani Tiwari
Book Review Editor	Vijay K Nambiar

INSTITUTE OF CHINESE STUDIES
B-371 (3rd floor), Chittaranjan Park,
Kalkaji, New Delhi - 110 019
Landline Telephone: +91-11-4056 4823

http://www.icsin.org/
info@icsin.org

twitter.com/ics_delhi
facebook.com/icsin.delhi
In.linkedin.com/Icsdelhi
soundcloud.com.ICSIN
youtube.com/ICSWEB
instagram.com/icsdelhi