TAIWAN SECURITY BRIEF

DISINFORMATION, CYBERSECURITY, & ENERGY CHALLENGES

Edited by Yuki Tatsumi,
Pamela Kennedy, and Jason Li

STIMSON

TAIWAN SECURITY BRIEF

DISINFORMATION, CYBERSECURITY, & ENERGY CHALLENGES

Edited by Yuki Tatsumi,
Pamela Kennedy, and Jason Li

STIMSON

Visit www.stimson.org for more information about Stimson.

Contents

"In challenges where nonstate actors are some of the most important stakeholders and problem-solvers, there is room for Taiwan to tackle both its own nontraditional security issues and assist with others that transcend borders and statehood."

Preface

It is my pleasure to introduce a new series of policy briefs from the Stimson Center's East Asia Program, the *Taiwan Security Brief*. Under the longtime expertise and care of the late Alan D. Romberg, the East Asia Program analyzed the nuances of cross-Strait relations, interpreting and advising on the complex situation for policymakers and experts on both sides of the Pacific. Behind the scenes, Alan mentored younger scholars in the field, from Stimson colleagues to visiting fellows. With Alan's passing, the East Asia Program has taken his work as inspiration—to rigorously examine security issues relating to Taiwan, to deliver astute recommendations, and to seek out emerging experts. In this spirit, the *Taiwan Security Brief* features early-career experts who are actively working on these issues and contributing to the body of written analysis.

This first volume, *Disinformation, Cybersecurity, & Energy Challenges*, scrutinizes three critical issues for Taiwan. The policy briefs assess the impact of each challenge on Taiwan and make recommendations for policymakers to seek creative solutions. While security studies of Taiwan often focus on cross-Strait relations, nontraditional security challenges—cross-border, non-military issues—pose significant threats to Taiwan's future prosperity and stability. These three briefs provide valuable insights into the nature of the challenges and the way forward.

My thanks to the three authors of this volume for committing to the project, and to Pamela Kennedy and Jason Li for preparing the manuscript for publication. We are grateful for the support of the Taiwan Economic and Cultural Representative Office as we brought this project from concept to reality in our first year without Alan's guidance. It is my hope that this project will continue to amplify the voices of the next generation of scholars on Taiwan, and cultivate new ideas and perspectives in the policy community.

Yuki Tatsumi
Co-Director, East Asia Program
The Stimson Center

Abbreviations

AI	Artificial intelligence
APT	Advanced Persistent Threats
CISO	Chief Information Security Officer
DCS	Department of Cybersecurity
DEF	Digital Economy Forum
DPP	Democratic Progressive Party
EDGE	Enhancing Development and Growth through Energy
FiT	Feed-in-Tariff
GCTF	Global Cooperation and Training Framework
GDP	Gross domestic product
GHG	Greenhouse gas
G-ISAC	Government Information Sharing and Analysis Center
GW	Gigawatts
ICEF	Information, Communication, and Electronic Force Command
ICT	Information and communications technology
IoT	Internet of Things
JUSEP	Japan-U.S. Strategic Energy Partnership
KMT	Kuomintang
LNG	Liquid natural gas
MND	Ministry of National Defense
MOE	Ministry of Education
MOEA	Ministry of Economic Affairs
MOST	Ministry of Science and Technology
NCC	National Communications Commission
NCCSC	National Communications and Cyber Security Center
NCCST	National Center for Cybersecurity Technology
NICSO	National Information and Communications Security Office
NICST	National Information and Communication Security Taskforce
N-ISAC	National Information Sharing and Analysis Center
NSC	National Security Council
N-SOC	National Security Operations Center
SPA	Sales and purchase agreement
TWNCERT	Taiwan National Computer Emergency Response Team
VPN	Virtual proxy network

Introduction

PAMELA KENNEDY AND JASON LI

Nontraditional security challenges—issues that transcend borders and occur outside the threat of military conflict—demand collaboration between a range of state and nonstate actors, from international organizations to NGOs.[1] The concept of nontraditional security is particularly important for Taiwan. The island faces myriad security threats, from natural disasters like typhoons and flooding to frequent cyberattacks. Because it operates under uncommon political constraints, Taiwan must rely on unofficial partnerships, side meetings, and other atypical means of functioning in the global community. As external diplomatic pressure limits Taiwan's activities in multinational organizations like ICAO and the WHO, it is critical that Taipei continue looking for creative means of safeguarding its security in cooperation with international partners and domestic actors. Taiwan already works closely with the United States to expand its international cooperation on an array of issues through the Global Cooperation and Training Framework, a series of training programs that connects experts from Taiwan and the U.S. with regional partners. There is room to expand and replicate this model.[2] Even the Taiwan Relations Act itself, which lays out parameters for the U.S.'s unofficial relations with Taiwan, is a creative means of engaging with Taiwan in a manner that is adjacent to, but not within, a state-centric framework.

Taiwan is a case study in policy responses to gray-zone strategies as well. The line between traditional and nontraditional security threats to Taiwan is porous, with frequent gray-zone activities that encompass information warfare, economic coercion, and military actions short of conventional war.[3] In this concept, there is significant space for exploring the dimensions of 21st century security threats, and Taiwan has valuable experience countering these evolving threats. Across the wide spectrum of warfare, Taiwan's current and potential future approaches to these challenges, such as disinformation campaigns, cyberattacks, and energy blockades, will serve as important lessons for other countries facing similar challenges.

Taiwan therefore offers insights, expertise, and opportunities for cooperation on nontraditional security issues. This collection of essays examines three nontraditional challenges: disinformation, cybersecurity, and energy security. The three authors, who are emerging experts on Taiwan, assess their chosen topic by analyzing the Taiwan government's current policies and making recommendations to increase security. The three articles show how these multifaceted security challenges require a more contemporary approach to security, and how Taiwan's unique situation provides opportunities for innovation.

In the first essay, "Confronting the Challenge of Online Disinformation in Taiwan," Dr. Lauren Dickey, an analyst at the Center for Naval Analyses, details the extensive reach of disinformation in Taiwan. Dr. Dickey shows how Taiwan's high level of connectivity—with more than 90 percent of individuals using the internet—and open society make it vulnerable to efforts to influence public opinion. The Taiwan government's policies attempt to balance between preserving freedom of expression and reducing the spread of disinformation, with both government and non-governmental initiatives. Dr. Dickey, emphasizing the importance of guarding against disinformation in the leadup to Taiwan's 2020 elections, recommends expanding government resources for these initiatives, strengthening partnerships with the private sector and other democracies, and training the public to identify disinformation. For this problem, Dr. Dickey's assessment epitomizes the all-society characteristic of a nontraditional security approach.

The second essay, "Cybersecurity as a *Sine Qua Non* of Digital Economy: Turning Taiwan into a Reliable Digital Nation?" by Bo-jiun Jing, a Ph.D. candidate at the School of Global Affairs at King's College London, looks at the necessity of a strong cybersecurity regime to reaching Taiwan's digital economy aspirations. Taiwan's powerhouse status in high-tech industries, from semiconductors to consumer electronics, means cybersecurity is critical, but Mr. Jing identifies challenges Taiwan must overcome: the effectiveness of its cybersecurity policy apparatus, a shortage of skilled professionals in cybersecurity, and the small size of the indigenous cybersecurity industry. Mr. Jing recommends that Taiwan work with international partners like the U.S. and the E.U. to expand collaboration on cybersecurity, as well as deepening contact between the government and the cybersecurity private sector. Mr. Jing's analysis notes that Taiwan's vulnerability as a top target of cyberattacks could be turned into an advantage for developing expertise needed in cyber environments across the world.

"Taiwan's Energy Security: Challenges and Opportunities," the third essay, by Chen-Sheng Hong, a WSD-Handa Fellow in residence at Pacific Forum, evaluates Taiwan's precarious energy security situation, focusing on energy availability, infrastructure, and governance. Mr. Hong observes Taiwan's exposure to international factors that could impact its energy imports and its insufficient energy reserves. Mr. Hong emphasizes the complexity of the energy security problem by assessing the Taiwan government's policies to reduce disruption, diversify sources, and increase renewable energy use. His recommendations include increased communication between the government, energy developers, and the public to cultivate understanding of Taiwan's energy policy and goals, and deepening cooperation with international partners on solutions to energy security threats. Though the problem of Taiwan's energy supply seems to be a domestic issue at first glance, Mr. Hong makes it clear that other countries face this challenge as well, and it is through cooperation on energy technology, infrastructure, and supply that the challenge can be overcome.

It is striking that while these are three large issues in their own right, they are also entangled with Taiwan's traditional security concerns, falling squarely within the gray zone. Successful disinformation campaigns could sway public opinion to be more favorable towards unification with China—or at least more distrustful of the Taiwan government—exacerbating the risks in cross-Strait relations. Cyberattacks could stunt the growth of Taiwan's digital economy and jeopardize the private information of the population, the government, and the private sector. Insufficient energy imports could cause blackouts that cripple Taiwan's ability to support native industries or defend the island. Taiwan might be the best example in Asia of how blurry the lines between traditional and nontraditional security can be, and how these issues require cooperation between the government, the private sector, the public, and international partners. In challenges where nonstate actors are some of the most important stakeholders and problem-solvers, there is room for Taiwan to tackle both its own nontraditional security issues and assist with others that transcend borders and statehood.

ENDNOTES

1. Mely Caballero-Anthony, *An Introduction to Non-Traditional Security Studies: A Transnational Approach*, Los Angeles: SAGE, 2015, p. 14-15.

2. Kurt Tong, "Taiwan's International Role and the GCTF," (speech, Sigur Center for Asian Studies, Washington, D.C., 2 March 2016) https://2009-2017.state.gov/e/eb/rls/rm/2016/253915.htm.

3. For definitions and attributes of gray zone activities, see Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe, "Gaining Competitive Advantage in the Gray Zone," RAND Corporation (2019), p. 7-12, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf.

Confronting the Challenge of Online Disinformation in Taiwan

LAUREN DICKEY

Background

In her 2018 National Day address, Tsai Ing-wen identified several elements at the core of Taiwan's national security. Alongside the need to establish Taiwan's strategic importance, upgrade national defense capabilities, and seek new development opportunities, Tsai also spoke about "preventing foreign powers from infiltrating and subverting [Taiwan's] society, ensuring that [Taiwan's] democratic institutions and social economy function normally." With China clearly in mind as the island's single existential threat, she issued a strong warning to any state or nonstate actor that sought to undermine Taiwan's democracy through disinformation campaigns and the spread of false information intended to mislead the public, damage the island's information security, or interfere with democratic processes. In Tsai's words, Taiwan is on the "frontline" of Chinese pressure and activities that seek to undercut the island's vibrant democracy and present a significant albeit nontraditional security challenge to the island.[1]

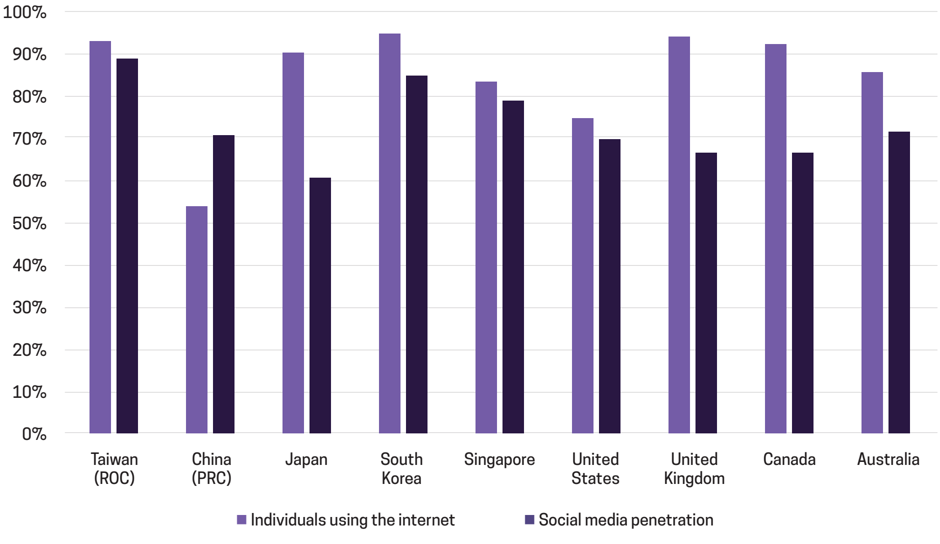
This paper focuses on the tools and tactics of Chinese efforts to shape public opinion in Taiwan. These efforts increasingly rely on the Internet-aided intentional dissemination of false information, referred to in this analysis as disinformation—not to be confused with misinformation, which is the unintentional spreading of false information.[2] Attribution remains a persistent problem in assessing the scope and impact of disinformation campaigns, and verifiable evidence of Chinese involvement in disinformation operations executed through bots and humans on social media platforms is minimal. However, the Chinese have a history of meddling in the domestic politics of Taiwan.[3] More recently, Chinese actors have demonstrated a sophisticated understanding of the use of Internet platforms to manipulate public sentiment across the Strait.[4] Disinformation campaigns in Taiwan have appeared aimed at shaping the domestic political narrative, interfering in Taiwan's domestic political processes by tarnishing the reputation of the Democratic Progressive Party (DPP), generating support for Kuomintang (KMT) candidates, and/or amplifying contradictions that exist within the Taiwan public. The cumulative effects of a disinformation campaign pose a significant set of nontraditional security challenges to the freedom, fairness, and sustainability of the island's democracy.

In the wake of the 2018 local elections, and with Taiwan's presidential elections approaching in January 2020, the necessity of ensuring that Taiwan can hold free and fair elections *without* foreign interference has become a central focus of Taiwan's nontraditional national security agenda. Actors on the opposite side of the Taiwan

Strait can leverage Chinese-language online and social media platforms as a way to disseminate messages quickly and rapidly across the island. Taiwan is vulnerable to Chinese interference via traditional and new media platforms not only as a result of a shared language, culture, and history but also because it is a free and open democratic society.[5] From Beijing's perspective, the same openness that characterizes Taiwan's vibrant democracy can be exploited to shape public opinion—amplifying extreme voices and creating divisions among the people (and voters) of Taiwan. The government of Taiwan believes that its ability to mitigate or counter narratives advanced by Chinese actors and disseminated in both traditional and online media is critical to ensuring preservation of the democratic freedoms enjoyed by the island's 23 million people.

The opportunity for Chinese state actors to leverage online and social media platforms in Taiwan for the dissemination of narratives that may undercut the island's democracy is facilitated by Taiwan's high level of connectivity. (See Figure 1.) According to data from the International Telecommunications Union and Hootsuite, Taiwan has among the highest internet penetration rate in the Indo-Pacific region at 92.78 percent. Of its active internet users, nearly 90 percent have a social media presence. Given that Taiwan has a mobile phone subscription rate of 123.66 per 100 people in 2018—a level notably higher than the regional average of 109.7 subscriptions per 100 people—much of this online activity is certain to be conducted via mobile browsing and apps.[6]

FIGURE 1: Internet and social media penetration (2017-2018)



SOURCE: ITU and Hootsuite

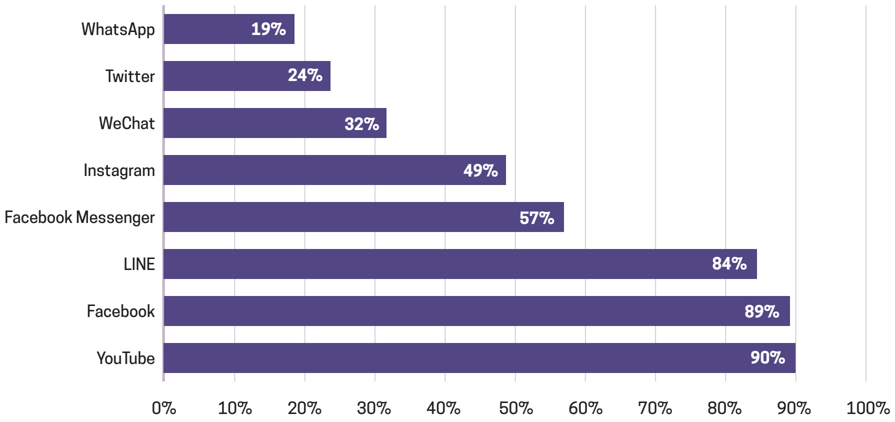
This high level of connectivity, particularly in comparison with other regional countries, undoubtedly generates many socioeconomic and business opportunities for the people of Taiwan. But it also brings with it a greater susceptibility to foreign influence activities online or via smartphone apps by China that aim to impact public opinion and interfere in domestic politics.

Impact on Taiwan

The overall impact of efforts by Chinese state actors to leverage online and social media in influencing public opinion on Taiwan is difficult to accurately and fully assess. This is due, in part, to the challenges inherent in attributing the origins of online commentary or tracing the paths of information disseminated through social media networks back to state-affiliated actors in China.[7] These challenges aside, this section focuses on several discrete instances in which Chinese-language online and social media platforms in Taiwan have been manipulated by actors believed to be located in China in an attempt to influence public sentiments.[8] These examples of how disinformation is spread—and the effects it can have—provides insight into how Chinese actors are leveraging online and social media platforms to delegitimize certain political actors or behaviors and, at the same time, expose and manipulate political fractures among the people of Taiwan.

Existing evidence suggests that Chinese efforts to shape or influence public opinion on Taiwan occur on the island's most popular social media platforms. According to data compiled by We Are Social and Hootsuite in January 2019, YouTube, Facebook, and Line are the most popular platforms in Taiwan by user

FIGURE 2: Percentage of Taiwan internet users on social media (as of January 2019)



SOURCE: Globalwebindex, Q2 and Q3 2018, via Hootsuite numbers (See Figure 2).[9] Domestic platforms like PTT (批踢踢), a Reddit-like message board, and Dcard (狄卡), a social networking site for university students, are also used widely among Taiwan's youth and students. All of these platforms have hosted videos, messages, or other forms of Chinese-language disinformation aimed at influencing public perceptions. These social media platforms have been used periodically by "cyber armies" (網軍) to transmit what Nicholas Monaco of Google Jigsaw refers to as "manual propaganda," the organized online messaging and disinformation campaigns carried out by human cyber armies in support of political objectives.[10]

Efforts to disseminate disinformation and influence public perceptions via social media in Taiwan have focused on using some of the island's most popular social media platforms to influence the domestic political narrative in Taiwan and amplify existing political divides on the island. The Reddit-like PTT has, for instance, been used to spread disinformation about Taiwan's diplomatic relations in a clear effort to distract and undercut policymakers. After Burkina Faso severed ties with Taiwan in May 2018, a message began to circulate on PTT that Honduran officials were in Beijing and would be the next country to swap recognition.[11] The post was subsequently traced by Taiwan's National Security Council to an IP address in China.[12] Since it is not technically difficult to disguise or alter the origination location of an IP address—as anyone that has used a virtual proxy network (VPN) to access websites from within China knows well—whether this particular disinformation campaign originated from the Chinese state is not publicly known.

On Facebook, individual users and group pages have similarly been mobilized in an effort to disseminate messages that seek to shape public perceptions of Taiwan's political leadership. Prior to the 2016 presidential elections in Taiwan, Chinese netizens gained access to Facebook pages typically blocked by the Great Firewall. Comments were posted to the Facebook pages of then-candidate Tsai Ing-wen, the Democratic Progressive Party, and other Taiwan media outlets with an "unwarranted degree of animosity."[13] In this instance, the "cyber army" mobilized to tarnish a political candidate and her party. Prior to the 2018 nine-in-one elections, several analysts described a surge in fake Facebook profiles and groups—as well as PTT posts—that had been set up to generate traction for political candidates, including then-Kuomintang mayoral candidate Han Kuo-yu of Kaohsiung.[14] The so-called "Han Kuo-yu wave" appears powered at least partially by a surge of internet users sharing messages that praise KMT candidates and attack DPP candidates, including specific attacks targeting his then-opponent at the polls, Chen Chi-mai.[15] Beyond electoral politics, netizens presumed to be based in China—as indicated through small linguistic differentiators—have also sought to buy control of Facebook groups or to hire group managers that "support peaceful reunification" (支持和平統一).[16] At the time of writing, Facebook has not explicitly identified any disinformation campaigns targeting Taiwan. However, it is worth noting that in

August 2019 both Facebook and Twitter identified campaigns on their respective platforms conducted as part of a "coordinated state-backed operation" by Chinese state actors with an aim of shaping public opinion about protests in Hong Kong.[17] Given these revelations, one may surmise that similar large-scale efforts organized by Chinese state actors may also be present on Facebook and/or Twitter in Taiwan.

Similar efforts to shape perceptions have occurred on the popular mobile phone chat app Line. Information on Line is primarily disseminated via closed groups, making the precise path of disinformation from source to effect difficult to accurately ascertain. What can be known, however, is the content of the messages circulated on Line. For instance, according to reports from pan-green newspaper *Liberty Times*, a rumor was circulated via Line that pension reforms enacted by the Tsai administration in mid-2017 included a clause stipulating that pension payments would be frozen for citizens traveling overseas.[18] This attempt to undercut the Tsai administration's pension reforms was publicly refuted by the Office of the President's Pension Reform Committee.[19] Taiwan's National Security Council further attributed the source of disinformation targeting the Pension Reform Committee to content farms (內容農場) in China, such as COCO01.[20]

Effective disinformation campaigns traditionally "draw on preexisting divides" in a society to build "content for which there is [perceived] societal demand."[21] In the case of Taiwan, disinformation campaigns carried out by China seek to further divide support for any pro-Taiwan platforms and, instead, create a narrative that supports Beijing's political objective of unification. These efforts take the DPP as a primary target because the DPP's platform is viewed by Beijing as "stubbornly [sticking] to 'Taiwan independence' and [refusing] to recognize the 1992 Consensus."[22] By comparison, the KMT—which in recent decades has been Beijing's preferred political party—is a benefactor of disinformation and social media campaigns believed to originate from China. Regardless of political party, however, combatting disinformation and fake news online is an undertaking that requires support from both sides of the political aisle as well as the people of Taiwan.

Current Policies

In combatting the spread of disinformation, fake news, or "manual propaganda" on social media, the Taiwan government has had to strike a balance between tightening regulations without stifling freedoms of expression. Mitigating the spread of disinformation also requires input from the private sector, the creators of the platforms on which disinformation is spread. Current policies in Taiwan recognize the multi-faceted approach that is needed and include a combination of government-led initiatives, amendments to national legislation, and non-governmental initiatives.

Government mechanisms and initiatives. Under Tsai Ing-wen's leadership, the government has bolstered institutional mechanisms and responsibilities for tackling the spread of fake news on social media. In September 2018, for instance, the Ministry of Justice's Investigation Bureau (法務部調查局) established a big data and public opinion task force (大數據輿情小組).[23] As of mid-2019, there was little publicly available information on the task force, including how it is staffed, its mission and responsibilities, or any news about the efficacy of the task force in dealing with disinformation.[24]

Separately, the national security institutions of Taiwan, including the Ministry of National Defense (MND; 國防部) and the National Security Council (NSC; 國安局), have sought to strengthen efforts to combat fake news within the context of the island's national security. In a session at the Legislative Yuan's Foreign Affairs and National Defense Committee (立法院外交及國防委員會) on countermeasures to China's "fake information," leadership from MND and the NSC stressed that fake news disseminated by China must be collected in the aggregate and processed through machine learning and big data in order to identify trends in Chinese tactics.[25] The MND's collection of and response to disinformation, particularly from Chinese sources, is coordinated by the Countering Fake News Rapid Respond Group (反制假訊息快速處理小組). According to media reports, this group targets false narratives about Taiwan—not just the island's military—that may be disseminated through military communities, including via newspapers and online content.[26] Like the Ministry of Justice, these efforts have received little public media coverage at the time of this writing.

Government institutions have also increased their efforts to assist in the fact-checking of public information and news stories. The Executive Yuan homepage, for instance, features a sub-page titled "Real-time News Clarification" (即時新聞澄清). This page identifies erroneous reporting, collecting false stories from local print and online platforms pertaining to any government agency and correcting the record with the real stories.[27]

National legislation. Both the executive and legislative branches of the island's government have introduced amendments to existing laws to curb the spread of disinformation and fake news. The Cabinet introduced amendments to at least seven existing pieces of legislation to fight false narratives and disinformation.[28] For example, the Disaster Prevention and Protection Act (災害防救法) was amended in May 2019 to impose penalties on those who spread false information about disasters and, as a result, cause harm to the public.[29] Under the Radio and Television Act (廣播電視法) and the Satellite Broadcasting Act (衛星廣播電視法), domestic media entities which broadcast false news reports which harm public interests and/or disrupt public order face increased fines.[30] Chung T'ien Television (中天電視), SET News (三立新聞), and TVBS are among those fined under the amended legislation for not fact-checking content and intentionally spreading content that harms public interests and well-being.[31]

Additionally, in the wake of a June 2019 public protest against Chinese-owned media outlets in Taiwan (拒絕紅色媒體、守護台灣民主), there appears to be increased domestic political support for future legislation that would penalize any organization that supports or enables the interests of a foreign power.[32] How national legislation is crafted or, in some cases, retooled to support a stronger defense of Taiwan's information landscape merits continued tracking.

Non-government responses. Private sector tech companies play an increasingly important role in combatting unwanted attempts to influence the populace of Taiwan via social media platforms. Popular chat app Line has, for instance, introduced an official account bot known as "Line Rumor Verification (謠言查證)." If a user has concerns about the veracity of an article shared within the app, they can post it to the account where bots will verify or refute the story.[33] The Line bot joins several existing widgets within the app, such as CoFacts (真的假的) and Aunt Meiyu (美玉姨), that seek to diminish the spread of false information in the app by allowing users to report and check on possible fake stories.[34] These app-specific initiatives are supplemented with stand-alone websites, including Rumor & Truth (蘭姆酒吐司) and MyGoPen, which debunk false stories found on social media and lifestyle websites.[35] The extent to which these bots are used by the general public to fact-check is, however, not readily known.

Efforts to combat disinformation have also taken root in civil society. For instance, the Taiwan FactCheck Center (台灣事實查核中心) was established by two civil society organizations, MediaWatch (台灣媒體觀察教育基金會) and weReport (優質新聞發展協會).[36] With ties to the journalism community in Taiwan, this center stands to offer an important contribution to refuting false narratives in the media. Their fact-checking findings are disseminated online as well as across social media platforms. Of note, the Center is certified by the non-partisan International Fact-Checking Network and serves as Facebook's in-country third-party partner for localized campaigns to counter the spread of disinformation and fake news.[37]

Recommendations

Combatting the spread of disinformation, fake news, and other forms of "manual propaganda" is a difficult task—and one that many modern democracies are similarly confronting. For Taiwan, this effort takes on particular urgency in a period of heightened tensions in Taipei's relationship with Beijing and in advance of the island's 2020 elections. Strengthening Taiwan's ability to defend against false information intentionally disseminated through social media requires the laser focus of government policy and resources, including in the following recommended ways:

- ***Bolster government resources for agencies and actors that assist in combatting disinformation.*** New and existing government organizations tasked with identifying and countering false narratives disseminated online must receive continued government support to function as desired. Interagency cooperation should be strengthened, ensuring that government actors can jointly tackle the challenge of disinformation.

- ***Strengthen public-private partnerships.*** The government should consider leveraging the private tech sector's expertise where possible in order to strengthen government abilities to mitigate the potential effects of disinformation. Similarly, private sector companies should develop clearer policies for dealing with manipulated or fake information—and apply these policies more aggressively to prevent the spread of disinformation.
- ***Leverage advanced technologies, like machine learning, in combatting disinformation without sacrificing traditional mechanisms.*** As cybersecurity expert Alex Stamos has noted, machine learning can help identify and shut down malicious actors operating in large scale on social media platforms. Machine learning may also help stymie disinformation that is picked up by recommendation engines and spread to other users.[38] Where machine learning falls short, however, is its ability to comprehend or understand news like humans do.[39] An over-reliance on machine learning to identify false news and disinformation would be unwise.
- ***Share experiences combatting disinformation with other like-minded partners.*** Taiwan is not the only democracy to grapple with the security challenges of disinformation—nor is it the only democracy to seek balance in policies that combat the malign effects of disinformation without undercutting individual freedoms. Taiwan should share its experiences combatting disinformation from China with other like-minded partners, helping them understand both the reality of the challenge and the possible avenues for policy responses.
- ***Expand public education and media literacy.*** The next generation of youth in Taiwan should continue to be taught how to discern fact from fiction in the island's academic curricula. Users of Line and other social media apps who are older and may statistically be more vulnerable to false news stories should also be targeted by media literacy campaigns. Within Taiwan's media sector, the government should consider the utility of requiring journalists and broadcasters to participate in mandatory fact-checking training programs.
- ***Ensure continued transparency.*** Lies are most easily exposed by promulgating the truth. The government of Taiwan should strive to be ahead of the curve, communicating policies or national developments to the people through online and traditional media.

Lauren Dickey is an analyst at the Center for Naval Analyses (CNA). The views expressed herein are her own and do not represent the views of her employer or the U.S. Navy.

ENDNOTES

[1] "Full text of President Tsai Ing-wen's National Day address," *Focus Taiwan News Channel*, 10 October 2018, http://focustaiwan.tw/news/aipl/201810100006.aspx.

[2] On the difference between misinformation and disinformation, see, e.g., Valerie Strauss, "Word of the year: misinformation. Here's why." *Washington Post*, 10 December 2018, https://www.washingtonpost.com/education/2018/12/10/word-year-misinformation-heres-why/.

[3] See, e.g., Michael M. Tsai and Po-Chang Huang, "China's United Front Strategy and its Impacts on the Security of Taiwan and the Asia-Pacific," *Fletcher Security Review* 3, no. 1 (2017); Peter Mattis, "China's Espionage Against Taiwan (Part I): Analysis of Recent Operations," China Brief 14, no. 21, 7 November 2014, https://jamestown.org/program/chinas-espionage-against-taiwan-part-i-analysis-of-recent-operations/.

[4] See, e.g., Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument," *American Political Science Review* 111, no. 3 (2017): 484-501; Mark Stokes and Russell Hsiao, *The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics* (Arlington, VA: Project 2049), 14 October 2013, p. 29.

[5] Tsai Ing-wen, "The Taiwan Relations Act at Forty and U.S.-Taiwan Relations," (VTC speech, CSIS, Washington, DC, 9 April 2019) https://www.csis.org/events/taiwan-relations-act-forty-and-us-taiwan-relations.

[6] United Nations International Telecommunication Union (ITU), "Statistics" and "Mobile Cellular Subscriptions," accessed 18 August 2019, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx; Hootsuite, "The Global State of Digital in 2019 Report," accessed 7 July 2019, https://hootsuite.com/pages/digital-in-2019.

[7] On the challenges involved in attribution of online disinformation to specific actors, see e.g. Office of the Director of National Intelligence, "A Guide to Cyber Attribution," 14 September 2018; Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," Hoover Institution Aegis Paper Series No. 1607, 2016.

[8] In addition to Chinese actors, other research indicates that domestic actors in Taiwan have previously initiated political disinformation campaigns. See, e.g., Man-Chun Ko and Hsin-His Chen, "Analysis of Cyber Army's Behaviours on Web Forum for Elect Campaign," Proceedings of the Asia Information Retrieval Societies Conference (2015).

[9] Hootsuite, "Digital 2019: Taiwan," accessed 7 July 2019, https://www.slideshare.net/DataReportal/digital-2019-taiwan-january-2019-v01.

[10] Nicholas J. Monaco, "Computational Propaganda in Taiwan: Where Digital Democracy Meets Automated Autocracy," working paper No. 2017.2, University of Oxford, p. 9.

[11] Chris Horton, "Burkina Faso Cuts Ties With Taiwan, Dealing It Another Blow," *New York Times*, 24 May 2018, https://www.nytimes.com/2018/05/24/world/asia/taiwan-burkina-faso-diplomatic-relations.html; Tu11252007 (anson), "News: Evolution of Chinese Cyber Army Fake News" (新聞: 中國網軍反串文再進化 假新聞亂竄誠信), PTT, 31 May 2018, 17:11, https://www.ptt.cc/bbs/WomenTalk/M.1527758942.A.567.html.

12. “National Security Offices: PTT has become Beijing’s Bastion for Tearing into Taiwan with Fake News” (國安單位：PTT竟成北京撕裂台灣的假新聞登陸堡壘), *LINE Today*, 22 October 2018, https://today.line.me/tw/pc/article/%E5%9C%8B%E5%AE%89%E5%96%AE%E4%BD%8D%EF%BC%9APTT%E7%AB%9F%E6%88%90%E5%8C%97%E4%BA%AC%E6%92%95%E8%A3%82%E5%8F%B0%E7%81%A3%E7%9A%84%E5%81%87%E6%96%B0%E8%81%9E%E7%99%BB%E9%99%B8%E5%A0%A1%E5%A3%98-NJlDwm; Herbert Lin, “Attribution of Malicious Cyber Incidents: From Soup to Nuts,” Hoover Institution Aegis Paper Series No. 1607, 2016.

13. Jessica Drun, “Taiwan’s Social Media Landscape: Ripe for Election Interference?,” Center for Advanced China Research, 13 November 2018, https://www.ccpwatch.org/single-post/2018/11/13/Taiwans-Social-Media-Landscape-Ripe-for-Election-Interference; Monaco, “Computational Propaganda in Taiwan: Where Digital Democracy Meets Automated Autocracy,” p. 23; “Chinese Cyber Army in Online Forums, Celebrity Facebook Pages…and the DPP: Welcome to Democratic Taiwan” (中國網民洗版媒體、名人臉書…民進黨：歡迎光臨民主自由的台灣), *The News Lens*, 21 January 2016, https://www.thenewslens.com/article/34934; “Chinese Netizens in Emotionally-Charged Taiwan Media War on Facebook” (中網友臉書戰台媒 表情包大戰), *Liberty Times*, 23 January 2016, https://news.ltn.com.tw/news/novelty/breakingnews/1582592.

14. Much like the challenge of attribution, the efficacy of these groups and their influence upon the electorate requires further study. See, e.g., Paul Huang, “Chinese Cyber-Operatives Boosted Taiwan’s Insurgent Candidate,” *Foreign Policy*, 26 June 2019, https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/; “Follow the Investigative Reporter to Chase the Cyber Army, “Fake Foreigners” Advocate for Han Kuo-yu Wave on PTT” (跟著資料記者追網軍，「假外國人」如何在PTT鼓吹韓流), *Commonwealth,* 23 April 2019, https://www.cw.com.tw/article/article.action?id=5094848.

15. “Han Kuo-yu’s Popularity to the Other Side of the Strait? Internet searches of “Han Kuo-yu” Reach High in China” (韓國瑜紅到對岸？「韓國瑜」在中國搜尋熱度高), *Liberty Times*, 11 November 2018, https://news.ltn.com.tw/news/politics/breakingnews/2608989; Chris Horton, “Specter of Meddling by Beijing Looms Over Taiwan’s Elections,” *New York Times*, 22 November 2018, https://www.nytimes.com/2018/11/22/world/asia/taiwan-elections-meddling.html;

16. “Mainland China’s Acquisition of “Taiwan Fan Groups, Recruitment of Local Cyber Army for Surprising Salaries Exposed!” (陸狂收購「台灣粉絲團」招募在地網軍驚人價格曝光), *EBC Financial News*, 6 April 2019, https://fnc.ebc.net.tw/FncNews/life/75896.

17. “Information operations directed at Hong Kong,” Twitter Safety, 19 August 2019, https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html; Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior From China,” Facebook Newsroom, https://newsroom.fb.com/news/2019/08/removing-cib-china/.

18. “National Security Offices: Protests on Pension Reform have Chinese Interference” (國安單位：反年改陳抗 有中國勢力介入), Liberty Times, 18 July 2017, https://news.ltn.com.tw/news/focus/paper/1119633.

19. Presidential Office, “Clarification on the Erroneous News: “The Government Seeks to Withhold Pension from Those Going Abroad” (有關「政府以退休金為質威脅人民出國就要申報」錯誤資訊之澄清), Pension Reform Committee, 17 July 2017, https://pension.president.gov.tw/News_Content.aspx?n=24EEE60D085C3437&s=03BEA1A211D5A972.

20. "National Security Offices: Protests on Pension Reform have Chinese Interference" (國安單位: 反年改陳抗 有中國勢力介入), *Liberty Times*, 18 July 2017, https://news.ltn.com.tw/news/focus/paper/1119633; COCO01 homepage, accessed 7 July 2019, https://www.coco01.today/. For a list of other known content farms, see Ketty W. Chen and J. Michael Cole, "CCP and proxy disinformation: Means, practices, and impact on democracies," Sinopsis Policy Brief, 26 July 2019, https://sinopsis.cz/en/ccp-and-proxy-disinformation-means-practices-and-impact-on-democracies/.

21. Dean Jackson,"Issue Brief: How Disinformation Impacts Politics and Publics," National Endowment for Democracy, 29 May 2018, https://www.ned.org/issue-brief-how-disinformation-impacts-politics-and-publics/.

22. *China's National Defense in the New Era*, State Council Information Office, 24 July 2019, http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm.

23. "National Security Bureau: Master Public Opinion for Government Reference" (國安局: 掌握輿情供政府參考), *CNA*, 14 September 2018, https://www.cna.com.tw/news/aipl/201809140128.aspx.

24. The task force initially found "unequivocal evidence" that Beijing was responsible for several fake news stories in 2018. See Chien Li-chung et al, "China using fake news to divide Taiwan," *Taipei Times*, 16 September 2018, http://www.taipeitimes.com/News/front/archives/2018/09/16/2003700513.

25. "Countering China's Fake Messages, Ministry of Defense Sets up Rapid Response Team" (反制中國假訊息 國防部成立快速處理小組), *CNA*, 1 May 2019, https://www.cna.com.tw/news/aipl/201905010229.aspx.

26. Ibid.

27. Executive Yuan, "Real-Time News Clarification" (即時新聞澄清), News & Announcements (新聞與公告), accessed 7 July 2019, https://www.ey.gov.tw/Page/5519E969E8931E4E; "Cabinet launches website to combat fake news," *Focus Taiwan News Channel*, 10 May 2018, http://focustaiwan.tw/news/asoc/201805100027.aspx.

28. "Taiwan imposes stiff penalties on spread of 'fake news,'" *Focus Taiwan News Channel*, 7 May 2019, http://focustaiwan.tw/news/aipl/201905070012.aspx.

29. Under the amended Act, punishment varies by the level of damage to the public that results. If false information results in death, the offending individual may receive up to a life sentence in prison. "Taiwan imposes stiff penalties on spread of 'fake news,'" *Focus Taiwan News Channel*, 7 May 2019, http://focustaiwan.tw/news/aipl/201905070012.aspx.

30. Matthew Strong, "Taiwan to raise fines for unfair reporting," *Taiwan News*, 12 December 2018, https://www.taiwannews.com.tw/en/news/3595403; Shelley Shan, "NCC to meet broadcasters over combating fake news," *Taipei Times*, 19 September 2018, http://www.taipeitimes.com/News/taiwan/archives/2018/09/19/2003700720; National Communications Commission, *Radio and Television Act*, amended 13 June 2018, https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=P0050001.

31. "NCC Chung T'ien Fined for Violation of Fact-Checking" (NCC: 中天違反事實查證再罰160萬), *Liberty Times*, 25 July 2019, https://news.ltn.com.tw/news/life/paper/1305626.

32. Shelley Shan, "NCC draft to add security act changes," *Taipei Times*, 27 June 2019, http://www.taipeitimes.com/News/taiwan/archives/2019/06/27/2003717674; "Ketagalan Boulevard Anti-China Media March, Large Numbers Protest in Rain" (凱道反親中媒體遊行 大批民眾冒雨相挺), *CNA*, 23 June 2019, https://www.cna.com.tw/news/firstnews/201906235002.aspx.

33. "LINE Promotes 'Rumor Verification' Official Account, Successfully Beats Lies in One Second" (LINE推「謠言查證」帳號1秒成功打假), *CNews*, 29 March 2019, https://cnews.com.tw/134190329a02/.

34. Cofacts homepage, accessed 7 July 2019, https://cofacts.gov.tw/; gov, "About," accessed 7 July 2019, http://gov.asia/#section-2; Joyu Wang and Chuin-Wei Yap, "Know-It-All Robot Shuts Down Dubious Family Texts," *Wall Street Journal*, 28 February 2019, https://www.wsj.com/articles/know-it-all-robot-shuts-down-dubious-family-texts-11551370040.

35. Rumor & Truth, "About Us" (關於我們), accessed 7 July 2019, https://www.rumtoast.com/%E9%97%9C%E6%96%BC; MyGoPen, "About Us" (關於我們), accessed 7 July 2019, https://www.mygopen.com/search/label/%E8%AC%A0%E8%A8%80.

36. Taiwan FactCheck Center, "Organization Structure" (組織結構), accessed 7 July 2019, https://tfc-taiwan.org.tw/about/oganization.

37. "Fact-checking on Facebook: What Publishers Should Know," Facebook, accessed 5 August 2019, https://www.facebook.com/help/publisher/182222309230722.

38. Alexander Stamos, "Artificial Intelligence and Counterterrorism: Possibilities and Limitations," (testimony, U.S. House of Representatives Committee on Homeland Security Subcommittee on Intelligence and Counterterrorism, Washington, DC, 25 June 2019).

39. See, e.g., James Vincent, "Why AI isn't going to solve Facebook's fake news problem," *The Verge*, 5 April 2018, https://www.theverge.com/2018/4/5/17202886/facebook-fake-news-moderation-ai-challenges.

Cybersecurity as a *Sine Qua Non* of Digital Economy: Turning Taiwan into a Reliable Digital Nation?

BO-JIUN JING

Background

With the dramatic increase in interconnectivity of digital technologies and the deepening integration of digital products and services into every aspect of life, digital tools have become double-edged swords. While the rapid developments of ultra-high-speed internet, smartphones, the Internet of Things (IoT), cloud computing, artificial intelligence (AI), and big data have made economic activities more convenient and efficient, they have also triggered a host of concerns about cybersecurity risks. The number of IoT connected devices worldwide, for example, is estimated to grow exponentially from 14.2 billion in 2019 to 25 billion by 2021.[1] Taiwan is fully embracing this IoT trend and is expected to play a significant role in supplying IoT sensors and chips to the world. A key rationale is that IoT technology enables objects to communicate with each other and generate data of use, providing the potential for the Fourth Industrial Revolution. However, the externally-oriented nature and significant data proliferation of the emerging IoT and other digital technologies pose potential risks of massive cybersecurity incidents, which were less likely to happen a decade ago.[2] In view of the threat, according to the World Economic Forum's Regional Risks for Doing Business 2018 report, business leaders from Taiwan and other Asian and Oceanian countries rate cyberattacks as the top risk of doing business across East Asia and the Pacific.[3]

In East Asia, Taiwan presents a unique case for cybersecurity development not only because of its solid high-tech industrial economy, but also because of the geopolitical dynamics in the China-Taiwan relationship and the Indo-Pacific region. On the one hand, Taiwan has excelled in industries such as information and communications technology (ICT), semiconductors, and consumer electronics to support its economic lifeline. On the other hand, Taiwan's international space has long been challenged by China's sovereignty claims over the island. Taiwan's distinctive status in the high-tech value chains and geopolitical configuration has made it a high-profile target for cyberattacks. In August 2018, Taiwan Semiconductor Manufacturing Company was attacked by a variant of WannaCry ransomware due to an onsite operator's mistake of not following the company's standard operating procedures. The incident forced the world's largest independent semiconductor foundry to halt production lines in three plant locations for three days, erasing around NT$5.2 billion (US$170 million) from its total revenue during the third quarter of 2018.[4] In 2017, the Taiwan government faced 20 to 40 million hacking attempts per month, most of which were believed to be launched by Chinese hackers.[5] The National Security Bureau—Taiwan's principle intelligence service—faced at least 230,000 cyberattacks in 2017.[6] According to the Executive Yuan's Department of Cybersecurity, 360 cyberattacks on government systems were successful throughout 2017, 288 of which originated from China.[7]

Against the backdrop of an increasingly risky cyber domain, Taiwan's current president, Tsai Ing-wen, has made enhancing cybersecurity a major national security priority. Since taking office in May 2016, Tsai has reiterated that "cybersecurity is national security" – a catchphrase used as the title for the first-ever National Cybersecurity Strategy Report released by her National Security Council (NSC) in September 2018.[8] The report, together with the Executive Yuan's National Cyber Security Program of Taiwan (2017-2020), outlines the details for the Tsai administration's cybersecurity strategy and highlights its ultimate vision to "build a safe and reliable digital nation."[9] Tsai's cybersecurity team is fully aware that this non-traditional security dimension has an important bearing on the two flagship economic policies unrolled by her administration – the Digital Nation and Innovative Economic Development Program (2017-2025) and the Five-Plus-Two Innovative Industries Plan (5+2 Plan). The former, also known as "Digi+," for development, innovation, governance, inclusion, and upgrading, aims to grow Taiwan's digital economy from NT$3.4 trillion (US$110 billion, 20.3% of GDP) in 2015 to NT$4.8 trillion (US$155 billion, 25.2% of GDP) in 2020, then to NT$6.5 trillion (US$210 billion, 29.9% of GDP) in 2025.[10] The latter promotes five pillar industries across the island: smart machinery, the Internet of Things (or dubbed the "Asia Silicon Valley" project), green energy, biomedical, and defense—plus new agriculture and the circular economy.[11] Achieving these ambitious goals requires efforts to strengthen cybersecurity ecosystem, because any massive cybersecurity breaches would take a heavy toll on Taiwan's development and confidence in digitization. As Lee Der-tsai, an NSC senior advisor in charge of cybersecurity policy, has noted: "no cybersecurity, no digital economy."[12] In other words, cybersecurity is a *sine qua non* of Taiwan's aspiration for its digital economy.

Following this introductory section, this brief examines challenges facing Taiwan's dream of becoming a reliable digital country. It then assesses the current polices promoted by the Tsai administration under the banner of "cybersecurity is national security." The concluding paragraphs provide some policy suggestions for Taiwan's policymakers to consistently enhance cybersecurity and build a dynamic digital economy.

Key Challenges

While the Taiwan government's increased awareness of and rising interest in cybersecurity may bode well for its digital transformation ambition, how to soften, if not fully address, the negative impact of the technological evolutions remains the critical question for Tsai to translate rhetoric into reality. Her administration's main challenge lies in how it modernizes the regulatory and legal frameworks to not only provide adequate protection in the cyber realm, but also cultivate an environment that encourages digital innovation and entrepreneurship within the cybersecurity field.

The cybersecurity administration of Taiwan was first established at the dawn of the 21st century. In 2001, the Executive Yuan during the Chen Shui-bian administration approved the Mechanism Program of Security in Establishing National Information and Communication Infrastructure (2001-2004), known as the Phase 1 Mechanism Program. Based on this groundbreaking policy, the National Information and Communication Security Taskforce (NICST) was established within the Executive Yuan in the same year. Since then, NICST has been responsible for cybersecurity policy planning and implementation, as well as interagency coordination. Meanwhile, the Phase 1 Mechanism Program moved to the second phase (2005-2008) under Chen's second term, and later carried out for another two phases (2009-2012 and 2013-2016) by President Ma Ying-jeou.[13] While the first three phases of the cybersecurity policy focused on improving intragovernmental measures, the fourth phase began to emphasize the importance of collaborating with the private sector to enhance cybersecurity mechanisms, as well as boosting domestic cybersecurity industry (see Table on page 26).[14] Although the continued efforts throughout these four phases of the policy arguably improved Taiwan's cybersecurity landscape, the increasingly sophisticated cyber networks on the systemic level, coupled with some domestic constraints in Taiwan, present three major challenges for the current administration to keep up with formulating feasible policy under its National Cyber Security Program of Taiwan (2017-2020), or the Phase 5 Program.

The first challenge is a potential lack of effectiveness of organizational and legal structures of the Taiwan government's cybersecurity apparatus. Prior to Tsai's inauguration in May 2016, while the NICST existed to act as a centralized interagency mechanism to supervise cybersecurity governance in Taiwan, its secretariat—the Office of Information and Communications Security—was only at the ad-hoc level within the Executive Yuan. Moreover, despite the executive orders or codes of practice regulating cyber operations of government agencies, the island lacked a cybersecurity law to strengthen the authority of the government institutions responsible for cybersecurity. During Tsai's first two years as president, her administration addressed these two issues by reorganizing the abovementioned office into a higher-level Department of Cybersecurity (DCS) in August 2016 and pushing for the Cyber Security Management Act that was passed by the Legislative Yuan in May 2018. The Act, which came into force in January 2019, gave the Executive Yuan the authority to impose such requirements as a cybersecurity risk assessment, disclosure, and emergency response plan on government agencies (except military and intelligent agencies), government-affiliated business and foundations, and critical infrastructure operators.[15] According the Executive Yuan's Office of Homeland Security, critical infrastructure covers eight areas: central and local governments, energy, water, high-tech parks, communications, transportation, banking and finance, and emergency rescue services and hospitals.[16] However, how to properly designate which private entities are considered critical infrastructure providers and how to streamline standard operating procedures for prevention of and response to cybersecurity incidents remain challenging tasks for the government.

The Taiwan Government's Cybersecurity Program under Chen and Ma (2001-2016)		
Program	Years (President)	Core Elements
Phase 1 Mechanism Program	2001-2004 (Chen)	▪ Categorize government entities by cyber threat levels ▪ Inaugurate the National Information and Communication Security Taskforce (NICST) ▪ Establish cybersecurity protection systems for 3,713 government agencies across the country ▪ Promote cybersecurity awareness in the government
Phase 2 Mechanism Program	2005-2008 (Chen)	▪ Include educational organizations in the cybersecurity protection systems, expanding the number of agencies included in the systems to 6,797 ▪ Establish the National Security Operations Center (N-SOC) ▪ Push for establishing the Chief Information Security Officer (CISO) positions in the government
Phase 3 Development Program	2009-2012 (Ma)	▪ Implement more than 30 action plans to increase cybersecurity readiness and improve information sharing mechanism ▪ Promote cybersecurity awareness in civil society ▪ Enforce the Personal Data Protection Act (2012) ▪ Establish the Government Information Sharing and Analysis Center (G-ISAC)
Phase 4 Development Program	2013-2016 (Ma)	▪ Cooperate with the private sector to reform the Security Operations Center (SOC) ▪ Initiate action plans to boost domestic cybersecurity industry. ▪ Expand cybersecurity talent initiatives and promote international exchange ▪ Increase cybersecurity incident simulation exercises

SOURCE: Huang, Hsini and Tien-Shen Li, "A Centralised Cybersecurity Strategy for Taiwan," *Journal of Cyber Policy*. Vol. 3, No. 3 (2018). 347-348; Executive Yuan. "National Strategy for Cybersecurity Development Program (2013-2016)." December 2013. 13-25; and Executive Yuan. National Cyber Security Program of Taiwan (2017-2020). November 2017. 17-23.[17]

The second challenge is the cyber skills shortage. Knowledge-intensive areas like cybersecurity require a high volume of qualified professionals. But with a shortage of skilled workers, demand has outpaced supply by a large margin. Although higher education in Taiwan is known for its training in ICT-related and electrical engineering specializations, the island is not immune to this global talent struggle. In fact, the situation is tougher for Taiwan as it has suffered a significant brain drain in recent years, exemplified by the ongoing trend of Taiwan high-tech professionals seeking jobs in Silicon Valley, Tokyo, Singapore, or megacities in China such as Shanghai or Beijing for higher salary, career potential, or lower housing price-to-income ratio.[18] In 2017, according to Taiwan government statistics, there were only about 8,500 professionals working in the private cybersecurity industry and 8,200 in the public sector or critical infrastructure.[19] In the government, there were only 672 civil servants solely assigned to handle cybersecurity, falling far short of DCS's ideal headcount of 1,224 full-time cybersecurity professionals for the government agencies.[20]

The final challenge relates to the development of Taiwan's cybersecurity industry. The Tsai administration has aimed to develop a competitive indigenous cybersecurity industry in hope of achieving "cybersecurity industry autonomy."[21] Nevertheless, the size of the island's cybersecurity industry is relatively small, and domestic companies involved in the cybersecurity market are mainly small and medium-sized enterprises with relatively few human and capital resources.[22] In 2017, the output of Taiwan's cybersecurity companies was NT$38.8 billion (US$1.25 billion), and there were fewer than 200 cybersecurity companies in Taiwan.[23] This can be attributed to the fact that most end users in Taiwan, be they corporate or individual, rely on foreign products such as Symantec, Check Point, and Cisco for their security needs in the cyber domain.[24] Moreover, according to Huang Hsini and Li Tien-shen, issues like the strict initial public offering rules against the software companies, as well as the risk-averse atmosphere in the capital market that neither encourage nor incentivize companies to invest in early-stage research and development, are major obstacles along Taiwan's cybersecurity industry development trail.[25]

Current Policies

Amid the ongoing cybersecurity challenges, the Tsai administration has unveiled a series of policies to enhance the cybersecurity ecosystem while pursuing greater prosperity in the digital economy. Besides enacting the Cyber Security Management Act and establishing DCS in the Executive Yuan, the government has also created or remodeled other new agencies, developed training programs, and collaborated more with the private sector to boost its cybersecurity ecosystem.

The current cybersecurity regime in Taiwan has been transformed into an "Iron Triad" consisting of the National Information and Communications Security

Office (NICSO) under the NSC, DCS under the Executive Yuan, and the National Communications and Cyber Security Center (NCCSC) under the National Communications Commission (NCC). NICSO reports directly to the president, whereas DCS falls under the premier's responsibility. As for NCCSC, it was inaugurated by Tsai in November 2018 to serve as a cybersecurity arm for NCC, which is an independent statutory authority responsible for regulating telecommunications and broadcasting services. The newly-founded entity focuses on protecting critical information infrastructure networks and promoting related cooperation with international partners.[26] At the inauguration ceremony of NCCSC, Tsai instructed the "Iron Triad" to jointly accelerate the process of strengthening cybersecurity mechanism, reiterating that the task is in the first line of national security defense.[27]

The establishment of DCS also added more staffing for Taiwan to protect its digital territory. As mentioned, DCS—the secretariat of NICST charged with coordinating cyber strategy, procedures, and policy—was upgraded from a small office during the first three months of Tsai's presidency. Before the reorganization, there were only two full-time employees on the office's payroll, while the others, about 11 to 13 officials from other agencies including the Ministry of Economic Affairs (MOEA) and Ministry of Science and Technology (MOST), were working on concurrent or temporary bases.[28] Now there are 16 permanent personnel positions plus five to seven officials temporarily assigned to the department from other agencies, making the body a 21 to 23-member cybersecurity brain trust that helps push forward its cybersecurity initiatives.[29]

The institutionalization of DCS has helped the Taiwan government to streamline political efforts behind cybersecurity. Apart from making the Cybersecurity Act a reality, DCS has also completed the tasks of setting up the National Information Sharing and Analysis Center (N-ISAC) and strengthening the Taiwan National Computer Emergency Response Team (TWNCERT) within the National Center for Cybersecurity Technology (NCCST), which has existed since 2001 and is now under the supervision of DCS to provide government agencies with technical services on cybersecurity.[30] During the second half of this year, DCS is slated to complete the upgrade on the National Security Operations Center (N-SOC) and put the regulations under the Cybersecurity Act into force for private entities designated as critical infrastructure operators. These initiatives will help Taiwan solidify the mechanisms of pre-incident prevention and protection (SOC), during-incident response and control (CERT), and post-incident forensics and sharing (ISAC) to effectively tackle cyber issues. There is some evidence that the new initiatives are essential for Taiwan to protect its cyberspace. In June of this year, DCS found a data breach in the Ministry of Civil Service's system allegedly exposed the detailed personal data of over 240,000 civil servants. After receiving the notice from DCS, the ministry officially reported the case to NCCST.[31] The DCS and NCCST, as well the whole "Iron Triad" system, should use this opportunity to improve their crisis management and review the security measures to prevent any future hacks.

In the military realm, Tsai inaugurated the Information, Communication and Electronic Force Command (ICEF) in June 2017, establishing the fourth branch of the Republic of China Armed Forces. The creation of ICEF—the first of its kind in the world—represents an elevated position of cyberwarfare in Taiwan's national defense strategy.[32] Its main missions, detailed by Tsai, include coordinating the efforts of different units that deal with information, communication, and electronics within the defense ministry, cooperating with other government agencies to protect confidential information, nurturing talent pools of cybersecurity professionals within the defense field, and partnering with the private sector to boost innovation in the cyber fourth service.[33] A key rationale behind this move is to foster the island's cybersecurity industry. As the Tsai administration strives to connect cybersecurity development with the defense industry under its 5+2 Plan, the formation of ICEF can open more cybersecurity contracts to domestic companies, thereby helping Taiwan to simultaneously upgrade its capabilities and self-sufficiency of the cybersecurity and defense industries.

Taiwan's ambition to pursue "cybersecurity industry autonomy" is also reflected in the growing size of its cybersecurity budget, which skyrocketed from NT$1.5 billion (US$48 million) in 2017 to NT$3.7 billion (US$119 million) in 2018.[34] Moreover, for future government plans that exceed NT$1 billion (US$32 million) in budget, at least 5% must be used for cybersecurity. For government initiatives budgeted between NT$100 million (US$3 million) and NT$1 billion (US$32 million) or below NT$100 million (US$3 million), the requirements are 6% and 7% respectively.[35] The increased financial resourcing has not only raised demand for cybersecurity products and services, but also enabled authorities in Taiwan to orchestrate relevant training schemes. A cybersecurity academy, for instance, was officially launched by DCS in October 2018. At its initial stage, the newly-formed institute offers cybersecurity training programs to professionals in industries related to financial technology and IoT.[36] Other entities involved in the training aspect of cyber policy, such as the Ministry of Education (MOE), Ministry of National Defense, MOEA, and MOST, are adopting an interagency approach to promote cybersecurity education via industry-academia cooperation, internships, and contests.[37]

In its Action Plan for Cybersecurity Industry Development (2018-2025) released in October 2018, the Executive Yuan has set goals to grow the total output of Taiwan's cybersecurity industry from NT$38.8 billion (US$1.25 billion) in 2017 to NT$55 billion (US$1.77 billion) in 2020, then to NT$78 billion (US$2.52 billion) in 2025.[38] With the aforementioned promotion of cybersecurity education designed by various government entities, it also aims to increase the total number of professionals in the field from 16,700 in 2017 to 18,425 in 2020, then to 21,000 in 2025.[39] Besides the determination to improve the cybersecurity ecosystem, the success of the cybersecurity initiatives still hinges on the competitiveness of the services or products offered by companies in Taiwan. For example, the Taiwan government in recent years has urged its civil servants to use Juiker, a freeware app for instant communications developed by the island's Industrial Technology Research Institute. In reality, however, most government officials are still relying on the Japanese app Line for their on-the-job communications, despite the confidential nature of their work, due to its user-friendly interface and large pool of users.

Policy Recommendations

That Taiwan has a profound interest in the success of cybersecurity and digital transformation polices is not in doubt. Given the existing groundwork laid by Tsai and her predecessors, Taiwan can take further steps to help itself to have the digital cake and eat it.

First, Taiwan should continue to partner with the United States through its two bilateral cooperation platforms, the Digital Economy Forum (DEF) and the Global Cooperation and Training Framework (GCTF), to hold joint programs and workshops germane to cybersecurity issues in the digital era.[40] Since their launches in 2015 under the Ma administration, there have been four major events under DEF and 18 workshops under GCTF at the time of this writing.[41] DEF focuses on the digital economy areas such as digital trade and investment, digital innovation, and smart technology, whereas GCTF covers a broader range of topics ranging from public health to women's empowerment to energy efficiency. However, GCTF also touches upon such digital issues as e-commerce and cybersecurity. In May of this year, GCTF brought together 41 participants from 25 Indo-Pacific partners, including Chile and Mexico for the first time, to join a workshop on network security and emerging technologies.[42] The event, co-hosted by Japan, could act as a springboard for further international cooperation on cybersecurity. Moreover, the government must continue its ongoing initiative to invite experts from the U.S. Computer Emergency Readiness Team and Department of Homeland Security to offer advice on strengthening its cybersecurity mechanism.[43] Given the rapid pace of digital change, this kind of workshop or exchange program should be further expanded by Taiwan. The inaugural Taiwan-European Union Dialogue on Digital Economy in June of this year was significant progress and should be referenced as a blueprint for future cooperation with other regional partners like Japan and Singapore.[44]

Second, leveraging Taiwan's advantages in analyzing and fighting against cyberattacks can be essential to the effectiveness of the island's cybersecurity industry policy. As Philip Hsu has noted, Taiwan has been recognized as one of the top targets of advanced cyberattacks globally, especially those in the format of Advanced Persistent Threats (APTs).[45] Most of these APTs are believed to be launched by China to conduct cyber espionage on government agencies and private companies, making Taiwan's cyberspace a virtual land of unique APT malicious software.[46] Moreover, cybersecurity professionals could find many more iterations of Chinese malware in Taiwan because Chinese hackers had been testing tools on the island before taking them global, according to the head of DCS Jyan Hongwei.[47] Although Hsu has argued that there is uncertainty about whether Taiwan's unique threat environment is relevant to the rest of the world's cyber needs, the island's increased expertise on a variety of cyber strategies merits attention. Robyn Klingler-Vidra notes that the Taiwan government's efforts to "turn lemons into lemonade" might work given that the "white hat" hackers protecting Taiwan's digital territory could translate into entrepreneurial experts poised to build top cybersecurity companies.[48] In view of the "lemons," Taiwan's ongoing preparation to share Chinese hacker data with private companies to help train AI software to combat future cyberattacks is a step forward for its "lemonade" goal.[49]

Last, the Taiwan government should proactively expand contact with the cybersecurity community in the private sector. Apart from supporting the island's largest annual cybersecurity conference, CYBERSEC, and engaging with the experts and practitioners through the event, the government should seek to hold more conferences related to cyber issues or digital economy through its ongoing Strategy Review Board mechanism under the Executive Yuan. The board's conventions focused on cybersecurity industry in 2017, 5G application in 2018, and smart-living display technology in 2019, providing experts in both the public and private sectors the chance to share and promote best practices in digital areas.[50] This kind of event should be further developed and held regularly. Moreover, the government should continue to send its officials to join the world's largest hacker conferences such as Black Hat Briefings and DEF CON to keep up with cybersecurity trends.[51] Furthermore, as mentioned above, there are many ICT and cybersecurity professionals from Taiwan working on the global stage. To gather latest technological and commercial information on the ground and implement cybersecurity initiatives at full steam, the public sector must reach out to and work closely with the existing network of cybersecurity experts from Taiwan around the world.

ENDNOTES

[1] Gartner, "Gartner Identifies Top 10 Strategic IoT Technologies and Trends," press release, 7 November 2018, https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends.

[2] Mario Spremić and Alen Šimunic, "Cyber Security Challenges in Digital Economy," *Proceedings of the World Congress on Engineering* 1 (2018), p. 341-346.

[3] World Economic Forum, "Regional Risks for Doing Business 2018," November 2018, p. 22, https://www.weforum.org/reports/regional-risks-for-doing-business.

[4] Sydney Peng, "The Real Reason Behind the TSMC Cyber Attack," *CommonWealth Magazine*, 21 November 2018, https://english.cw.com.tw/article/article.action?id=2194.

[5] Chuan Ku and Hsiu-chuan Shih, "Taiwan Addressing Cybersecurity Talent Shortage amid China Threat," *Focus Taiwan*, 5 April 2018, http://focustaiwan.tw/news/aipl/201804050011.aspx.

[6] Tian-bin Luo, "Qu nian zao hai ke gong ji yu 23 wan ci guo an ju: dou cheng gong zhen ce zu jue"「去年遭駭客攻擊逾23萬次 國安局: 都成功偵測阻絕」[Having been attacked by hackers more than 230,000 times, National Security Bureau: All of them were successfully detected and blocked], *Liberty Times*, 2 September 2018, https://news.ltn.com.tw/news/politics/breakingnews/2538679.

[7] Hsin-fang Lee and Jonathan Chin, "Chinese Hackers Getting Sophisticated," *Taipei Times*, 5 April 2018, http://www.taipeitimes.com/News/front/archives/2018/04/05/2003690700.

[8] National Security Council, "Guo jia zi tong an quan zhan lue bao gao: zi an ji guo an" 「國家資通安全戰略報告: 資安即國安」 [National Cybersecurity Strategy Report: Cybersecurity is National Security], September 2018, https://www.president.gov.tw/Issue/439.

[9] Ibid; and Executive Yuan, "National Cyber Security Program of Taiwan (2017-2020)," November 2017, https://nicst.ey.gov.tw/en/807491F2A43DF876.

[10] Executive Yuan, "Shu wei guo jia·chuang xin jing ji fa zhan fang an (2017-2025 nian)"「數位國家·創新經濟發展方案（2017-2025年）」[Digital Nation and Innovative Economic Development Program (2017-2025)], October 2017, p. 15 and 63, https://drive.google.com/file/d/0B3y3eToRMV-_cWJ2ZGNlLUtaamM/view.

[11] See Timothy Ferry, "The 5+2 Industrial Innovation Plan," *Taiwan Business Topics*, 8 May 2017, https://topics.amcham.com.tw/2017/05/52-industrial-innovation-plan/.

[12] Yan-fen Huang, "Guo an hui zi xun wei yuan Lee Der-tsai: tui dong guo jia ji zi an zhan lue, han wei shu wei guo tu an quan" 「國安會諮詢委員李德財: 推動國家級資安戰略, 捍衛數位國土安全」 [National Security Council Senior Advisor Lee Der-tsai: Promoting National-level Cybersecurity Strategy and Defending Digital Homeland Security], *iThome*, 17 March 2017, https://www.ithome.com.tw/news/112773.

[13] The title of the program was changed to the National Information and Communication Security Development Program (or National Strategy for Cybersecurity Development Program as translated in some government documents in English) during the third and the fourth phases under Ma. They are also known as the Phase 3 Development Program and the Phase 4 Development Program.

14. Hsini Huang and Tien-Shen Li, "A Centralised Cybersecurity Strategy for Taiwan," *Journal of Cyber Policy* 3, no. 3 (2018): p. 347-348; Executive Yuan, "National Strategy for Cybersecurity Development Program (2013-2016)," December 2013, p. 13-25, https://nicst.ey.gov.tw/File/8D9C0DC93AFCE58B?A=C; and Executive Yuan, "National Cyber Security Program of Taiwan (2017-2020)," p. 17-23.

15. Cyber Security Management Act, https://nicst.ey.gov.tw/en/3FF2617AC997EFB7/b4ec6082-25af-4b76-af94-05ea27a0507b.

16. Executive Yuan, "National Cyber Security Program of Taiwan (2017-2020)," p. 3-4.

17. Ibid.

18. See Simon Denyer, "Taiwan battles a brain drain as China aims to woo young talent," *The Washington Post*, 15 April 2018, https://www.washingtonpost.com/world/asia_pacific/taiwan-battles-a-brain-drain-as-china-aims-to-woo-young-talent-away/2018/04/13/338d096e-3940-11e8-af3c-2123715f78df_story.html; and Alisha Haridasani, "Big Prices in Little Taipei: Why is property so expensive in Taiwan's capital?" CNN, 23 April 2015, https://edition.cnn.com/2015/04/22/business/taiwan-taipei-expensive-housing-market/index.html.

19. Executive Yuan, "Zi an chan ye fa zhan xing dong ji hua (2018-2025)"「資安產業發展行動計畫（2018-2025）」[Action Plan for Cybersecurity Industry Development (2018-2025)], October 2018, p. 29, https://nicst.ey.gov.tw/File/D91D4144C09405D0?A=C.

20. Xin-fang Li, "Zheng yuan lan cai da zao shi jie ji zi an yan xun ji gou"「政院攬才 打造世界級資安研訓機構」[The Executive Yuan recruits talents and build a world-class cybersecurity research and training institute], *Liberty Times*, 5 April 2018, https://news.ltn.com.tw/news/politics/paper/1189990.

21. National Security Council, "National Cybersecurity Strategy Report: Cybersecurity is National Security," p. 10, 40-49, 52-53.

22. Executive Yuan, "Action Plan for Cybersecurity Industry Development (2018-2025)," p. 18-19.

23. Ibid. p. 12-14; and U.S. Commercial Service, Taipei, "Cyber Security: Overview, Regulatory Trends, and Opportunities in Taiwan," July 2017, p. 3, https://build.export.gov/build/idcplg?IdcService=DOWNLOAD_PUBLIC_FILE&RevisionSelectionMethod=Latest&dDocName=eg_tw_113364.

24. U.S. Commercial Service, Taipei, p. 3.

25. Huang and Li, p. 353-354. A similar view was expressed by Edward Wei-Kuang Lee, a security and trust advisor at Google Cloud, during author's online interview on 19 June 2019.

26. Zi-yu Pan, "Guo jia tong xun ji wang ji an quan zhong xin cheng li kang xia wu da ren wu"「國家通訊暨網際安全中心成立 扛下五大任務」[The National Communications and Cyber Security Center was established, tasked with five major missions], *Central News Agency*, 16 November 2018, https://www.cna.com.tw/news/ahel/201811160271.aspx.

27. Office of the President, Republic of China (Taiwan), "Zong tong chu xi guo jia tong xun ji wang ji an quan zhong xin (NCCSC) jie pai yi shi"「總統出席國家通訊暨網際安全中心 (NCCSC) 揭牌儀式」[President attended the inauguration ceremony of the National Communications and Cyber Security Center], 15 November 2018, https://www.president.gov.tw/News/23892.

28. Author's correspondence with officials in the Executive Yuan, 27 June 2018.

29. Ibid. There are three sections under DCS: Comprehensive Planning Section, Technology Development Section, and Notification and Response Section. Also see Xin-fang Li, "Zheng yuan zi an chu 8.1 gua pai 21 ren cheng jun." 「政院資安處8.1掛牌 21人成軍」[Executive Yuan's Department of Cybersecurity to be inaugurated on August 1 with 21 people], 24 July 2016, https://news.ltn.com.tw/news/focus/paper/1014161.

30. For more details about NCCST, see "About NCCST" at https://www.nccst.nat.gov.tw/About?lang=en; for details about N-ISAC, see "Introduction of National Information Sharing and Analysis Center (N-ISAC)" at https://www.nccst.nat.gov.tw/NISAC?lang=en; and for details about TWNCERT, see "Mission" at https://www.twncert.org.tw/mission.

31. Yu-yang Liao, Cheng-chung Wang, and Evelyn Kao, "Government confirms massive civil servant personnel data hack," *Focus Taiwan*, 25 June 2019, http://focustaiwan.tw/news/aipl/201906250018.aspx.

32. Philip Hsu, "Chinese Hacking Against Taiwan: A Blessing for the United States?" *The Diplomat*, 23 January 2018, https://thediplomat.com/2018/01/chinese-hacking-against-taiwan-a-blessing-for-the-united-states/.

33. Sophia Yeh and Elaine Hou, "Information, Communication and Electronic Warfare Command Formed," *Focus Taiwan*, 29 June 2017, http://focustaiwan.tw/news/aipl/201706290027.aspx.

34. Executive Yuan, "Action Plan for Cybersecurity Industry Development (2018-2025)," p. 47.

35. Ibid. p. 48.

36. Zheng-han Luo, "Guo jia zi an ren cai pei xun xin zhan lue, xing zheng yuan zi an xue yuan ben zhou kai pao"「國家資安人才培訓新戰略, 行政院資安學院本周開跑」[The new strategy of national cybersecurity talent training: the Executive Yuan's cybersecurity academy starts this week], *iThome*, 23 October 2018, https://www.ithome.com.tw/news/126584.

37. U.S. Commercial Service, Taipei, p. 7.

38. Executive Yuan, "Action Plan for Cybersecurity Industry Development (2018-2025)," p. 12, 30.

39. Ibid. p. 29.

40. Tania Garcia-Millan, "Modernizing Taiwan's Legal Framework to Drive a Digital Transformation," in *Perspectives on Taiwan: Insights from the 2018 Taiwan-U.S. Policy Program*, Bonnie S. Glaser and Matthew P. Funaiole, eds., Center for Strategic and International Studies, March 2019, p. 7-8.

41. For details on DEF, see American Institute in Taiwan (AIT), "Remarks by AIT Director Kin Moy at the Digital Economy Forum – Smart Technology Symposium," 25 April 2017, https://www.ait.org.tw/remarks-ait-director-kin-moy-digital-economy-forum-smart-technology-symposium-tuesday-april-25-2017/; and AIT, "Remarks by AIT Director Kin Moy at the Symposium on Social Innovation and Digital Transformation," 25 June 2018, https://www.ait.org.tw/remarks-by-ait-director-kin-moy-at-the-symposium-on-social-innovation-and-digital-transformation/. For details on GCTF, see AIT, "Remarks by AIT Director W. Brent Christensen at the U.S.-Taiwan Business Forum," 10 June 2019, https://www.ait.org.tw/remarks-by-ait-director-w-brent-christensen-at-the-u-s-taiwan-business-forum/.

42. AIT, "Remarks by AIT Deputy Director Raymond Greene at Opening Ceremony of GCTF on

Network Security and Emerging Technologies," 28 May 2019, https://www.ait.org.tw/remarks-by-ait-deputy-director-greene-at-opening-ceremony-of-gctf-on-network-security-and-emerging-technologies/.

43. Crystal D. Pryor, "Taiwan's Cybersecurity Landscape and Opportunities for Regional Partnership," in *Perspectives on Taiwan*, Glaser and Funaiole, eds., p. 14.

44. Pei-chun Tang and Emerson Lim, "Taiwan, EU establish high-level dialogue on digital economy," *Focus Taiwan*, 7 June 2019, http://focustaiwan.tw/news/aeco/201906070011.aspx.

45. Philip Hsu, "Taiwan's Emerging Push for 'Cyber Autonomy,'" *China Brief*, The Jamestown Foundation 18, no. 3 (July 2018), https://jamestown.org/program/taiwans-emerging-push-for-cyber-autonomy-2/.

46. Hsu, "Chinese Hacking Against Taiwan: A Blessing for the United States?"

47. Kathrin Hille, "Taiwan to share Chinese hacks data with private companies," *Financial Times*, 22 October 2018, https://www.ft.com/content/e3e39f54-d5fc-11e8-ab8e-6be0dcf18713.

48. Robyn Klingler-Vidra,, "Cybersecurity as national security, and economic opportunity, in Taiwan," *Asia Dialogue*, 23 November 2018, https://theasiadialogue.com/2018/11/23/cybersecurity-as-national-security-and-economic-opportunity-in-taiwan/.

49. Hille.

50. Ya-juan Huang, "Zi an hui yi jian yan lai kui: liang ge yue nei ti xing dong fang an"「資安會議建言 賴揆: 兩個月內提行動方案」[Cybersecurity SRB Conference offers suggestions, Premier Lai: Propose actiona plan within two months], Central News Agency, 22 November 2017, https://www.cna.com.tw/news/aie/201711220271.aspx; the Executive Yuan, "5G SRB hui yi deng chang shou ri ju jiao ying yong pin pu yu chuang xin chuang ye"「5G SRB會議登場 首日聚焦應用、頻譜與創新創業」 [5G SRB Conference took place, the first day focuses on applications, spectrum, innovation, and start-up], 29 October 2018, https://www.ey.gov.tw/Page/9277F759E41CCD91/b9c39677-ae9f-4c0c-b874-5fcf1abfa65e; and Hong-da Zheng, "Zheng yuan: pan xian shi ke ji wan shan chan ye ying yong chuang 2030 zhi hui sheng huo xin mian mao" 「政院: 盼顯示科技完善產業應用 創2030智慧生活新面貌」[Executive Yuan: Hope display technology can improve industrial application, creating a new look of smart living by 2030], United Daily News, 9 July 2019, https://udn.com/news/story/7238/3918975.

51. The Executive Yuan has budgeted plans to send officials to attend these conferences. See the Executive Yuan, "108 nian du xing zheng yuan dan wei yu suan" 「108年度行政院單位預算」 [Executive Yuan's Annual Budget, 2019], p. 111, https://www.ey.gov.tw/Page/94F2BA3DA2D0C24/f09fb851-da75-4b21-b528-cda932e3e7bc.

Taiwan's Energy Security: Challenges and Opportunities

CHEN-SHENG HONG

With Taiwan's scarce indigenous energy resources and minimal spare electricity capacity as well as heavy dependence on imported energy, energy security is one of its most critical national security issues. The current administration in Taipei has acknowledged the energy security challenges and launched several policies to secure domestic energy supply, as well as ensure energy safety and minimize environmental and human damage. How to ensure the island's energy security without compromising negative social effects and environmental damage will be a serious topic for the current and future administrations. Feasible solutions must not only focus on domestic policy development but also international cooperation.

For a framework to identify Taiwan's energy security challenges and evaluate the effectiveness of the current government's energy security policies, this article will use the "four As of energy security" framework introduced by the Asia Pacific Energy Research Center's 2007 report on energy security, as it constitutes a generic concept of energy security.[1] The four As include: (1) availability (uninterrupted availability of the energy source); (2) accessibility (issues such as geopolitical, geographical, workforce, technological, and other constraints that create barriers to energy supply accessibility); (3) affordability (energy price); and (4) acceptability (environmental impacts of the energy system). As experts may classify different components in an energy security framework into different dimensions, the components may overlap or interact with each other.

Background

Taiwan's primary energy supply mostly comes from oil, coal, and natural gas, representing 48.28 percent, 29.38 percent and 15.18 percent of Taiwan's energy supply in 2018 respectively. Other energy sources in the energy supply represent 7.15 percent of energy supply, including nuclear (5.38 percent), biomass and waste (1.13 percent), hydro (0.29 percent), solar PV and wind (0.28 percent), and solar thermal (0.07 percent).[2] Petroleum products and electricity are the two major final forms of energy consumption. With growing consumption of electricity, the energy mix plays a key role in influencing the composition of Taiwan's energy supply. In 2018, coal-fired and LNG-fired electricity were the two major sources, accounting for 45.53 percent and 34.26 percent respectively.[3]

Availability

In the four As framework, the most important challenge of Taiwan's energy security is energy availability. As Taiwan is an island without enough indigenous energy production, and energy demands have grown over the past decade by 11 percent (from 78,621,150 kloe in 2008 to 87,298,023 kloe in 2018),[4] it is critical to ensure sufficient and uninterrupted energy supply. Although Taiwan currently has a sufficient energy supply because it can meet domestic energy consumption,[5] it relies heavily on energy imports. Its energy import dependence has been between 97 percent and 98 percent for the past 10 years, reflecting a strong reliance on imported oil, coal, and LNG. Taiwan also imports nuclear power, though the proportion has gradually declined since 2014.[6] Taiwan's energy supply also highly relies on oil and coal, above 75 percent in the total energy supply for the past ten years, an insufficient diversification of energy sources despite gradual increases in natural gas and renewable energy.[7]

Accessibility

Apart from energy availability, Taiwan also faces some challenges in other energy security dimensions. The ability to access energy sources is a major challenge to security, and the energy-importing country's geopolitical conditions and availability of energy infrastructure influence energy supply.[8]

Taiwan's major oil suppliers are in the Middle East, with Saudi Arabia, Kuwait, and Oman being the three largest oil exporters. Taiwan's only non-Middle East sources for oil are Angola and Indonesia, and imports from Angola have declined dramatically since 2018, probably influenced by the country's oil output decrease last year.[9] Taiwan's coal imports are only slightly more diverse, with the four major suppliers from 2014 to 2018 being Australia, Indonesia, Russia, and South Africa. Among these critical sources, Taiwan is increasing its imports from Russia and decreasing imports from Indonesia, so that Russia has surpassed Indonesia and become the island's second-largest coal import source since 2017.[10] For LNG, Taiwan imports from Qatar in particular, as well as from Malaysia, Indonesia, and other sources. After signing long-term supply contracts with capacity owners of liquefaction projects in Australia, the U.S., and Papua New Guinea, Taiwan has further diversified its LNG imports.

In terms of infrastructure, accessibility of natural gas depends largely on huge infrastructure investments and long-term sales contracts. As the world's fifth-largest LNG importer,[11] the availability of LNG infrastructure is an important factor, but Taiwan currently has only two LNG receiving terminals with supply capacity of 16 million tons per year.[12] Japan, another major LNG importing nation, in comparison has 34 receiving terminals with 40 percent utilization rate.[13] Renewable energy has particular challenges to accessibility, such as the limited access to advanced technology. The 2019 White Paper issued by the American Chamber of Commerce in Taipei observes that the reliability of renewable energy in the current system depends on large-scale power storage facilities and smart grid investments, technology that is still expensive and developing.[14]

Affordability

When assessing energy affordability, the value of energy imports in the nation's GDP and per capita energy imports provide benchmarks.[15] The energy import expenditure and burden on the population in Taiwan is increasing. According to the Bureau of Energy, the value of energy imports in Taiwan's GDP has increased in the past three years, growing from 5.68 percent of GDP in 2016 to 8.43 percent in 2018. The higher this proportion, the heavier the energy import expenditure. The growing price of per capita energy imports confirms the growing burden on the people of Taiwan: Between 2016 and 2018, the price of per capita energy imports has had a 53 percent increase from USD 1,324.99 to USD 2,031.10.[16]

Acceptability

Finally, while greenhouse gas (GHG) emissions are a major concern in energy acceptability, nuclear waste from nuclear power plants is actually the most controversial acceptability challenge in Taiwan. Taiwan's radioactive waste from nuclear power plants includes both high-level waste (materials derived from the reprocessing of spent nuclear fuel) and low-level waste (rags, papers, filters, equipment, and so forth). Taiwan currently has 18,422 metric tons of high-level waste and 111,807 barrels (of 55 gallons each) of low-level waste temporarily stored in the three operating nuclear power plants, and 100,277 barrels of low-level waste temporarily on Orchid Island.[17] Though Taiwan has rapidly decreased its nuclear waste production over the past ten years,[18] it has not found a final disposal location for radioactive waste, due to rejections from cities and counties.[19]

Impact on Taiwan

The energy situation in Taiwan has implications for its energy security. Since Taiwan lacks sufficient energy source diversification and relies heavily on imports, Taiwan's energy availability is vulnerable to fluctuations of global markets, especially the oil market, and to changes in its exporters' geopolitical conditions. This is also an energy accessibility issue. A recent example is the June 13, 2019 attack on an oil tanker carrying 75,000 tons of naphtha from the Middle East to Taiwan's state oil refiner CPC Corporation.[20] After the attack, the global oil price rose, increasing oil prices in Taiwan.[21] Apart from oil, most of Taiwan's current LNG imports must travel through the South China Sea and the Malacca Strait; any conflict in these regions may impact Taiwan's LNG supply.

In addition, cross-Strait relations and cyberattacks also influence Taiwan's energy accessibility in terms of geopolitical and infrastructure conditions. If there is a confrontation in the Strait, a Chinese naval blockade could divert shipments of oil and natural gas, crucially impacting the island's economy. Further, as cyberattacks have emerged as a new threat to global security, a cyberattack on energy infrastructure is a potential problem. The case of Ukraine in December 2015 is instructive. A power company in western Ukraine reported "interference," leaving the region without energy. The Ukraine Security Service accused Russia in the cyberattack.[22]

The lack of enough LNG receiving terminals will cause the overuse of existing terminals. According to the CPC Corporation, the total utilization rate of Taiwan's LNG receiving terminals has reached 103 percent, and this will increase the operating risk of the terminals.[23] In addition, as the government wants to raise the percentage of natural gas in the energy mix to 50 percent by 2025 and the natural gas consumption is expected to reach 24.9 million tons by that time,[24] the current supply capacity of the two receiving terminals is not sufficient. This will lead to a supply gap and influence the stability of the natural gas supply.

In addition, the rising cost of energy imports, as a percentage of GDP and per capita, will make Taiwan's economic growth vulnerable to the global energy market. Researchers Chuang and Ma also point out that a higher per capita energy import indicates a hidden energy efficiency problem.[25]

The controversial nuclear waste problems have developed into a debate about whether to restart construction of Lungmen Nuclear Power Plant (also called plant No. 4) which was deferred in 2014. Supporters of nuclear power say that it is less polluting than fossil fuel and can be a baseload power source,[26] as the nuclear plants can continuously operate, while solar and wind power are less reliable. But opponents argue that there is no good solution for final disposal of nuclear waste, and that Taiwan, prone to earthquakes, could face an accident like Japan's Fukushima Daiichi nuclear disaster after the Tohoku earthquake and tsunami on March 11, 2011.[27] There is a political element to the nuclear power debate as well. The ruling party, the Democratic Progress Party, is generally anti-nuclear, while the opposition party, Kuomintang, is pro-nuclear.[28] In the November 2018 referendum, a question about nuclear power revealed the public generally supports nuclear power:

> "Do you agree with abolishing the first paragraph of Article 95 of the Electricity Act, which means abolishing the provision that 'all nuclear-energy-based power-generating facilities shall cease to operate by 2025'?"

5.89 million voters said "yes" and 4.01 million "no," showing a lack of public support for the current government's goal of a "nuclear-free homeland" by 2025. In compliance with the result of the referendum, the Legislative Yuan abolished the provision of Article 95 on stopping operations of nuclear energy facilities in 2025.[29]

Current Policies

The most important task to address energy security challenges in Taiwan is to increase energy diversification and independence without influencing the stability of the energy supply, as well as managing the growing energy demand. Since taking office in 2016, President Tsai has been trying to achieve these goals by supporting energy transition through several policies. The Guideline on Energy Development launched in 2017 emphasized diversification and independence of the energy supply, strengthening energy-saving on the demand side, and use of smart systems.[30]

First, regarding energy diversification, Taiwan has tried to diversify its energy source suppliers, such as the U.S. Though oil imports still mainly come from the Middle East, Taiwan has tried to seek other potential sources. For instance, in July 2018, Taiwan refiner Formosa Petrochemical Corporation announced that it bought 1 million barrels of crude oil from the U.S. for the first time.[31] Also, the CPC Corporation recently signed a 25-year deal with Cheniere Energy Inc., a U.S. LNG company, to purchase 2 million tons of LNG per year starting in 2021.[32] The CPC Corporation also seeks international cooperation through signing a joint long-term sales and purchase agreement (SPA) with the Japanese energy company JERA to purchase LNG from Mozambique.[33] This is CPC's first co-purchase deal with a foreign partner, and both sides can exchange LNG based on the other's supply and demand under the SPA.

In addition, since managing the energy mix is a key issue in Taiwan's energy security challenges, the government aims at facilitating renewable energy development, which can help increase energy independence, decrease energy import expenditures, and mitigate GHG emissions. In 2017, the government announced a target future energy mix of 50 percent natural gas, 30 percent coal, and 20 percent renewable energy by 2025.[34] Also, the government passed the Amended Renewable Energy Development Act in April 2019 to set a goal of total installed capacity of 27 gigawatts (GW) of renewable energy by 2025. According to the Bureau of Energy, through June 2019, the total capacity of renewable energy is 7 GW, of which solar power accounts for 3.4 GW and wind for 0.7 GW.[35] The government wants to increase the installed capacity of solar and wind power to 20 GW and 4.2 GW respectively by 2025.[36]

Though there is still a huge gap between the current capacity and the future target, the government has launched several policies to facilitate this development. In 2017, the government implemented the "Two-year Solar PV Promotion Plan" and the "Four-year Wind Power Promotion Plan" to promote solar and wind power development.[37] The amendment of the Electricity Law in 2017 also permitted consumers to buy electricity directly from independent clean electricity generators through the state-owned power transmission system. This can help to liberalize Taiwan's renewable energy supply and attract more renewable energy investors.[38]

The government also uses the Feed-in-Tariff (FiT), a policy tool that pays owners of generators a certain amount per unit of electricity sent to the grid. FiT rates are set above the retail cost of electricity to increase renewable energy investment. Taiwan's FiT scheme provides a 20-year fixed tariff through power purchase agreements between producers and Taipower.[39]

Regarding smart systems, which can enable the integration of large-scale renewable energy generation, the government has engaged in the development of a smart grid since 2010, when it launched the 2010 National Master Plan on Energy Conservation and Carbon Reduction. With evolving smart grid technology, in 2018 Taiwan further established the first offshore large-scale micro grid in Chimei township of the Penghu archipelago.[40] In 2010, the government also launched the Taiwan National Advanced Metering Infrastructure Deployment Plan to promote smart meter investment which could increase customers' ability to manage their demand and minimize GHG emissions through allowing for real-time monitoring of a household's electricity consumption and pricing.[41] The government aims to have 1 million smart meters installed by 2020 and 3 million by 2024.[42]

Recommendations

1. Enforce smart grid security mechanisms and share experience with Japan, South Korea, and the U.S.

Since a smart grid encompasses power generation and consumption, the reliability of the system is important. Researchers Bari et al. have pointed out the challenge of ensuring cybersecurity in a smart grid and mentioned that advanced cyberattacks can eventually compromise the stability of the grid through disrupting information access to undermine power delivery, exposing user information and providing unauthorized access to the system.[43]

As the Taiwan government has actively promoted the development of smart grid systems, it is critical to enforce smart grid security mechanisms to avoid advanced cyberattacks. Since Japan, South Korea, and the U.S. are also developing smart grid systems, Taiwan should share the experience with these countries and discuss how to prevent cyberattacks on smart grid systems together.

2. Improve education on energy-saving literacy

Apart from improving the technical capability to address the energy security problem, it is also important to enhance public literacy on saving energy. Chuang and Ma point out that energy security could also be achieved through energy demand growth control to reduce pressure on the energy supply.[44] If public awareness on energy saving is raised, people can manage their energy demand and decrease unnecessary waste and GHG emissions. The government can use social media to promote energy-saving literacy and provide educational materials for schools and universities. The government has already worked on this issue, but it should continue to increase the public's participation in energy-saving activities.

3. Increase communication with the renewable energy developers when establishing an affordable and attractive Feed-in-Tariff rate for renewable energy investment

Though the government uses the FiT to attract renewable energy investment, renewable energy developers protested[45] when the new FiT rate for 2019 was revealed to have a greater decrease than the average reduction in the global renewable energy industry;[46] the lower FiT rates will raise the cost of renewable energy investment. The government finally compromised and decreased the rate of decline.[47]

The government should communicate more with renewable energy developers when establishing the FiT rate and avoid frequent policy changes. If the government fails to establish an attractive FiT rate or changes its policy too often, the interest of renewable energy developers will decrease and harm the confidence of foreign renewable energy investors.

4. Secure the energy supply and diversify energy sources by considering exploring methane hydrates with Japan

As the government aims to phase out nuclear power in the future and increase renewable energy and natural gas, there two problems that must be addressed: whether renewable energy can ensure a stable energy supply, and how to decrease energy imports while increasing natural gas usage. To address these problems, the government should consider a relatively new source of energy, methane hydrates. This is a source of methane found in ice on the edges of continental shelves, containing 160 cubic meters of natural gas per cubic meter of methane hydrates.[48] Japan is one of the most active nations in exploring methane hydrates, as it also lacks indigenous energy and relies heavily on natural gas imports. In 2013, Japan successfully extracted natural gas from methane hydrate deposits.[49] Apart from Japan, China and the U.S. are among the states also exploring this possibility.

Though the government has not shown much attention and interest in this source, recently, a team of researchers from Taiwan and France extracted methane ice off the southwestern coast of Taiwan in June 2018.[50] Though exploring methane hydrates is controversial as it may have a huge environmental impact, the government should consider studying the feasibility of this source and working with Japan in the surrounding ocean.

5. Seek international cooperation opportunities with the U.S. under Asia EDGE and the GCTF

Taiwan should be more active in engaging in energy diplomacy. For instance, the U.S. launched the Enhancing Development and Growth through Energy (Asia EDGE) in July 2018 as a way to increase U.S. private sector investment in the Indo-Pacific region's energy sector, as part of the U.S. Indo-Pacific Strategy. Asia EDGE has four strategic focuses: (1) strengthening the energy security of allies and partners; (2) creating open, efficient, rule-based, rule-based, and transparent energy markets; (3) improving free, fair, and reciprocal energy trading relationships; and (4) expanding access to affordable, reliable energy.[51] These objectives meet Taiwan's requirements. Since Taiwan has gradually increased LNG imports from the U.S., seeking more cooperation opportunities with the U.S. in the energy sector with the focus on LNG through Asia EDGE can bring mutual benefits, not only securing Taiwan's LNG supply but also expanding U.S. LNG export capabilities.

In addition, Taiwan can consider utilizing the Global Cooperation and Training Framework (GCTF), which was established in 2015 by the U.S. and Taiwan governments to expand U.S.-Taiwan cooperation in addressing global challenges,[52] to work with the U.S. to co-host a workshop on energy security. Countries in the Indo-Pacific region could join to exchange information and share experience, potentially figuring out possible solutions to Taiwan's challenges. The workshop can also be expanded to include Japan, as it has a similar energy situation.

6. Consult with the U.S. and Japan on construction of LNG infrastructure under JUSEP

Taiwan is now considering not only expanding its existing LNG terminals but also developing new terminals to achieve its LNG target in 2025. Since the U.S. and Japan established the Japan-U.S. Strategic Energy Partnership (JUSEP) in November 2018 to facilitate investment in LNG supply and infrastructure projects,[53] the Taiwan government can consider seeking LNG import terminal infrastructure investment from the U.S. and Japan under JUSEP. In addition, Taiwan can also seek consulting on LNG infrastructure with the U.S. and Japan, as it did with Osaka Gas Engineering Co., Ltd. in May 2018 with CPC Corporation and Taipower.[54]

ENDNOTES

[1] Asia Pacific Energy Research Centre, *A Quest for Energy Security in the 21st Century: Resources and Constraints* (2007), https://aperc.ieej.or.jp/file/2010/9/26/APERC_2007_A_Quest_for_Energy_Security.pdf.

[2] Bureau of Energy, Ministry of Economic Affairs, “107 nian neng yuan gong xu gai kuang” 「107年能源供需概況」[Energy Supply and Demand Situation of Taiwan in 2018], 1 August 2019, https://www.moeaboe.gov.tw/ECW/populace/content/SubMenu.aspx?menu_id=6977.

[3] Bureau of Energy, Ministry of Economic Affairs, “Fa dian jie gou”「發電結構」[Energy mix], 15 August 2019, https://www.moeaboe.gov.tw/ECW/populace/web_book/WebReports.aspx?book=M_CH&menu_id=142.

[4] Bureau of Energy, Ministry of Economic Affairs, “Wu, neng yuan xu yao” 「伍、能源需要」[5. Energy demand], 15 August 2019, https://www.moeaboe.gov.tw/ECW/populace/web_book/WebReports.aspx?book=M_CH&menu_id=142.

[5] The total energy supply 2018 was 148,923,600 kiloliters of oil equivalent (kloe) and total energy consumption was 87,298,000 kloe. Bureau of Energy, Ministry of Economic Affairs, “107 nian neng yuan gong xu gai kuang” 「107年能源供需概況」[Energy Supply and Demand Situation of Taiwan in 2018].

[6] Bureau of Energy, Ministry of Economic Affairs, “Neng yuan an quan zhi biao”「能源安全指標」[Energy security indicator], and “Neng yuan gong ji (an zi chan yu jin kou bie)”「能源供給 (按自產與進口別) 」[Energy Supply (by indigenous & imported], 27 June 2019, https://www.moeaboe.gov.tw/ECW/populace/web_book/WebReports.aspx?book=Q_CH&menu_id=143.

[7] Ibid.

[8] Asia Pacific Energy Research Centre.

[9] Paul Burkhardt, “Angola’s Oil Revival Depends Heavily on Foreign Influence,” *Bloomberg*, 5 June 2019, https://www.bloomberg.com/news/articles/2019-06-05/angola-s-oil-revival-depends-heavily-on-foreign-influence.

[10] Bureau of Energy, Ministry of Economic Affairs, Energy Statistics Database, https://www.moeaboe.gov.tw/wesnq/Views/A01/wFrmA0102.aspx; and “Russian coal exports to Taiwan rise,” *Argus Blog*, 12 March 2019, https://www.argusmedia.com/en/news/1864072-russian-coal-exports-to-taiwan-rise.

[11] Florence Tan, “Taiwan’s CPC to start building third LNG terminal by mid-2019,” *Reuters*, 12 March 2019, https://www.reuters.com/article/us-ceraweek-energy-cpc-taiwan/taiwans-cpc-to-start-building-third-lng-terminal-by-mid-2019-idUSKBN1QT2MT.

[12] Yuyang Liao, “Neng yuan zhuan xing cheng gong yu fou xue zhe: di san jie shou zhan shi guan jian” 「能源轉型成功與否 學者: 第三接收站是關鍵」[Scholar: the third receiving terminal is key for success in energy transition], *Central News Agency*, 4 September 2018, https://money.udn.com/money/story/5641/3348136; Energy Knowledge Database, “Tian ran qi di san jie shou zhan de ‘hui bi ti dai xui zheng fang an’ jiang kai fa mian ji suo jian wei 23 gong qing, zheng qu huan cha ping shen tong guo”「天然氣第三接收站的『迴避替代修正方案』將開發面積縮減為23公頃, 爭取環拆評審通過」[The alternative proposal of natural gas third receiving terminal decreases development

areas to 23 hectares to pass the Environmental Impact Comparative Analysis], *Industrial Technology Research Institute*, 4 September 2018, https://km.twenergy.org.tw/Data/db_more?id=3566.

13. Ibid.

14. American Chamber of Commerce in Taipei, "Energy Committee: 2019 White Paper Issues," https://amcham.com.tw/2019/05/2019-energy-committee-position-paper/.

15. Ming Chih Chuang and Hwong Wen Ma, "An assessment of Taiwan's energy policy using multi-dimensional energy security indicators," *Renewable and Sustainable Energy Reviews* 17 (2013) p. 301-311.

16. Bureau of Energy, Ministry of Economic Affairs, Energy Statistics Database.

17. Fuel Cycle and Materials Administration, Atomic Energy Council, "He neng dian chang yong guo he zi ran liao zhu cun biao" 「核能電廠用過核子燃料貯存表」[Nuclear power plant's nuclear power waste storage table], updated 13 August 2019, https://www.aec.gov.tw/焦點專區/乾式貯存管制/管制動態/核能電廠用過核子燃料貯存表--218_224_3436_3502.html, and "He dian chang fang she xing fei qi wu"「核電廠放射性廢棄物」[Nuclear power plant radioactive waste], updated 5 August 2019, https://www.aec.gov.tw/fcma/管制動態/放廢設施管制/核電廠放射性廢棄物--2_32_56.html.

18. Ibid.

19. Lee-jung Liu and Evelyn Kao, "Restarting No.4 nuclear plant project could cost NT$70 billion: AEC," *Focus Taiwan*, 14 March 2019, http://focustaiwan.tw/news/aeco/201903140013.aspx.

20. Liang-Sa Loh and Yimou Lee, "Taiwan's CPC says naphtha tanker hit by suspected attack in Middle East," *Reuters*, 13 June 2019, https://www.reuters.com/article/us-mideast-tanker-evacuation-cpc-taiwan/taiwans-cpc-says-naphtha-tanker-hit-by-suspected-attack-in-middle-east-idUSKCN1TE1H1.

21. "Oil prices spike after apparent tanker attack in Gulf of Oman," *CBS News*, 13 June 2019, https://www.cbsnews.com/news/oil-tanker-attack-gulf-of-oman-crude-prices/; Chia-jung Wu, Ting-ting Han, and Emerson Lim, "Fuel prices in Taiwan to rise due to Middle East tensions," *Focus Taiwan*, 16 June 2019, http://focustaiwan.tw/news/aeco/201906160006.aspx.

22. Pavel Polityuk, "Ukraine to probe suspected Russian cyber attack on grid," *Reuters*, 31 December 2015, https://www.reuters.com/article/us-ukraine-crisis-malware/ukraine-to-probe-suspected-russian-cyber-attack-on-grid-idUSKBN0UE0ZZ20151231.

23. Liao.

24. Zhiming Chen, "Tian ran qi gong ying yi bao he zhong you: bi xu xing jian di san zuo ye hua jie shou zhan" 「天然氣供應已飽和 中油: 必須興建第三座液化接收站」[Natural gas supply has saturated CPC: it is necessary to build a third LNG receiving terminal], *Taoyuan Newsletter*, 10 April 2019, https://tyenews.com/2019/04/13485/.

25. Chuang and Ma.

26. Shyi-min Lu, "Nuclear power is the best for the environment," *Taipei Times*, 5 December 2017, http://www.taipeitimes.com/News/editorials/archives/2017/12/05/2003683438/1.

27. Nicolas Freschi, "Taiwan's Nuclear Dilemma," *The Diplomat*, 14 March 2018, https://thediplomat.com/2018/03/taiwans-nuclear-dilemma/.

28. Joseph Yeh, "KMT presidential contenders back continued use of nuclear power," *Focus Taiwan*, 3 July 2019, http://focustaiwan.tw/news/aipl/201907030023.aspx.

29. Sean Lin, "Provision on halting nuclear power plants removed," *Taipei Times*, 8 May 2019, http://www.taipeitimes.com/News/taiwan/archives/2019/05/08/2003714760.

30. Bureau of Energy, Ministry of Economic Affairs, *Guidelines on Energy Development* (April 2017), https://www.moeaboe.gov.tw/ECW/english/content/SubMenu.aspx?menu_id=1519.

31. Florence Tan, "Taiwan's Formosa buys first U.S. crude to replace Mideast oil: official," *Reuters*, 23 July 2018, https://uk.reuters.com/article/us-taiwan-formosa/taiwans-formosa-buys-first-u-s-crude-to-replace-mideast-oil-official-idUSKBN1KD0RU?rpc=401&.

32. Jess Macy Yu, Julie Gordon, and Henning Gloystein, "Cheniere signs 25-year LNG sales deal with Taiwan's CPC," *Reuters*, 11 August 2018, https://www.reuters.com/article/us-cheniere-energy-taiwan/cheniere-signs-25-year-lng-sales-deal-with-taiwans-cpc-idUSKBN1KW03E.

33. Judy Lo, "Taiwan's CPC partners with Japan's JERA on a 17-year LNG purchase deal," *Taiwan News*, 14 May 2019, https://www.taiwannews.com.tw/en/news/3701181.

34. Judy Lin, "Taiwan to generate 20% of power from renewables by 2025: Tsai," *Taiwan News*, 15 February 2017, https://www.taiwannews.com.tw/en/news/3095302.

35. Bureau of Energy, Ministry of Economic Affairs, "Fa dian liang zhuang zhi rong liang (li nian)"「發電量裝置容量(歷年)」[Total Installed Capacity (Historical)], 15 August 2019, https://www.moeaboe.gov.tw/ECW/populace/web_book/WebReports.aspx?book=M_CH&menu_id=142.

36. "Solar, wind power generation hits new high in Taiwan," *Taiwan Today*, 17 April 2018, https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=132786.

37. Office of Energy and Carbon Reduction, Executive Yuan, "Tai yang guang dian 2 nian tui dong ji hua"「太陽光電2年推動計畫」[Two-year Solar PV Promotion Plan], and "Feng li fa dian 4 nian tui dong ji hua"「風力發電4年推動計畫」[Four-year Wind Power Promotion Plan], https://www.ey.gov.tw/oecr/70E89A5AB119AD8E.

38. Li-yun Huang and Ko Lin, "Taiwan passes law to liberalize green energy supply," *Focus Taiwan*, 11 January 2017, http://focustaiwan.tw/news/aeco/201701110029.aspx.

39. "Taiwan feed-in tariff 2019: Is it enough?" Watson Farley & Williams, 6 February 2019, https://www.wfw.com/articles/taiwan-feed-in-tariff-2019-is-it-enough/.

40. Renée Salmonsen, "Taiwan's first island energy grid activated," *Taiwan News*, 15 May 2018, https://www.taiwannews.com.tw/en/news/3431194.

41. Hwa Meei Liou, "The Development of Electricity Grid, Smart Grid and Renewable Energy in Taiwan," *Smart Grid and Renewable Energy* 8 (June 2017), p. 163-177, https://doi.org/10.4236/sgre.2017.86011.

42. Department of Information Services, Executive Yuan, "Low-voltage smart meters promote energy conservation." 3 October 2016, https://english.ey.gov.tw/News3/9E5540D592A5FECD/91894952-bbc6-4d12-b205-72341ae7cf8c.

43. Ataul Bari, Jin Jiang, Walid Saad, and Arunita Jaekel, "Challenges in the Smart Grid Applications: An Overview," *International Journal of Distributed Sensor Networks* (2014), p. 1-11, https://doi.org/10.1155/2014/974682.

44. Chuang and Ma.

45. Ted Chen, "Solar FIT cuts unacceptable: industry groups," *Taipei Times*, 5 December 2018, http://www.taipeitimes.com/News/biz/archives/2018/12/05/2003705493.

46. "Taiwan Proposes Offshore Wind Feed-in-Tariff Cut," 30 November 2018, *Offshore Wind*, https://www.offshorewind.biz/2018/11/30/taiwan-proposes-offshore-wind-feed-in-tariff-cut/; and Sharon Chen, "Obscured policies in Taiwan's FIT scheme to impact on sustainable development of local solar supply chain," *PV Magazine*, 12 December 2018, https://www.pv-magazine.com/2018/12/12/obscured-policies-in-taiwans-fit-scheme-to-impact-on-sustainable-development-of-local-solar-supply-chain/.

47. Ted Chen, "Final feed-in-tariff set for wind firms," *Taipei Times*, 31 January 2019, http://www.taipeitimes.com/News/front/archives/2019/01/31/2003708970; and "Taiwan feed-in tariff 2019: Is it enough?" Watson Farley & Williams.

48. Paulina R. Pena, "Securing Taiwan's Energy Supply through Methane Hydrates and International Cooperation," *Global Taiwan Brief* 3, issue 20 (17 October 2018), http://globaltaiwan.org/2018/10/vol-3-issue-20/.

49. Hiroko Tabuchi, "An Energy Coup for Japan: 'Flammable Ice,'" *The New York Times*, 14 March 2013, https://cn.nytimes.com/business/20130314/c14methane/zh-hant/dual/.

50. Chia-nan Lin, "Expert urges continued research of methane hydrates," *Taipei Times*, 24 July 2018, http://www.taipeitimes.com/News/taiwan/archives/2018/07/24/2003697279.

51. U.S. Department of State, "Asia EDGE – Enhancing Development and Growth through Energy," https://www.state.gov/asia-edge/.

52. Kurt Tong, "Taiwan's International Role and the GCTF," (speech, Sigur Center for Asian Studies, Washington, D.C., 2 March 2016) https://2009-2017.state.gov/e/eb/rls/rm/2016/253915.htm.

53. Agency for Natural Resources and Energy, Ministry of Economy, Trade, and Industry, "Joint Statement on Japan-United States Strategic Energy Partnership," 20 March 2019, https://www.enecho.meti.go.jp/en/category/others/jusep/; and White House, "U.S.-Japan Joint Statement on Advancing a Free and Open Indo-Pacific Through Energy, Infrastructure and Digital Connectivity Cooperation," White House, 13 November 2018, https://www.whitehouse.gov/briefings-statements/u-s-japan-joint-statement-advancing-free-open-indo-pacific-energy-infrastructure-digital-connectivity-cooperation/.

54. Osaka Gas, "Osaka Gas Engineering to Provide Consulting Service on Construction of LNG Receiving Terminals in Taiwan," 17 May 2018, https://www.osakagas.co.jp/en/whatsnew/1270944_11885.html.

About the Experts

Authors

LAUREN DICKEY is a research analyst with the Center for Naval Analyses China-Indo-Pacific Division, where she is a member of the Indo-Pacific Security Affairs Program. Her current research focuses on Chinese military strategy and Chinese activities in the Indo-Pacific. Dickey received a Ph.D. in War Studies at King's College London and the National University of Singapore, where she researched modern Chinese strategy toward Taiwan. Previously, she worked as a research assistant at the Council on Foreign Relations in Washington, D.C. She holds an M.A. in International Studies and Diplomacy from the School of Oriental and African Studies, University of London, and a B.A. in Asian Studies and Chinese from the University of Oregon. She was a Chinese Language Flagship scholar and Critical Language Scholarship recipient during her undergraduate studies and a Rotary Ambassadorial Scholar during her Master's degree. Dickey is professionally fluent in Mandarin Chinese.

CHEN-SHENG HONG is a Resident WSD-Handa Fellow at Pacific Forum, a Honolulu-based foreign policy research institute focusing on the Indo-Pacific region. His research focuses on energy and developmental issues in the East and Southeast Asia. Before starting his fellowship, he was a research associate at the Taiwan-ASEAN Studies Center in the Chung-Hua Institution for Economic Research, where he analyzed Southeast Asian economic development and Taiwan-ASEAN relations. Prior to this position, he was a research fellow with the Southeast Asia Program at the Stimson Center in Washington, D.C., researching Mekong regional renewable energy development. Before joining Stimson, he completed a research internship at the Stockholm Environment Institute Asia Center in Bangkok, contributing to a project on the climate and developmental impacts of energy infrastructure under China's Belt and Road Initiative in Southeast Asia. He earned his M.A. in International Studies and Diplomacy from the School of Oriental and African Studies, University of London, and B.A. in Political Science from National Cheng-Chi University in Taiwan.

BO-JIUN JING is a Ph.D. candidate in the Lau China Institute at King's College London. His research focuses on Taiwan's foreign policy towards Southeast Asia, U.S.-China-Taiwan relations, and the international political economy of the Indo-Pacific. His articles on ASEAN-Taiwan relations, Taiwan's domestic politics, and cross-Strait relations have appeared on the National Bureau of Asian Research's Brief Series, the Chinese (Taiwan) Yearbook of International Law and Affairs, The Straits Times, Bangkok Post, and The Diplomat. He is the author of the monograph *Taiwan and Southeast Asia: Opportunities and Constraints of Continued Engagement* (University of Maryland School of Law, 2016). Prior to pursuing doctoral studies, he worked as a Research Associate at the Lee Kuan Yew School of Public Policy in Singapore and as an Associate Researcher at the Mainland Affairs Council in Taiwan. He holds an M.A. in International Relations and International Economics from the Johns Hopkins University School of Advanced International Studies (SAIS) and a B.A. in Political Science and Economics from National Taiwan University.

Stimson Staff

YUKI TATSUMI is the Director of the Japan Program and Co-Director of the East Asia Program. Previously, she was a Research Associate at the Center for Strategic and International Studies and the Special Assistant for Political Affairs at the Embassy of Japan in Washington. She is the author of numerous books, monographs, and articles on the Japanese defense establishment, the U.S.-Japan alliance, and security dynamics and challenges in Northeast Asia. In September 2006, she testified before the House Committee on International Relations, and she is a recipient of the 2009 Yasuhiro Nakasone Incentive Award. In 2012 she was awarded the Letter of Appreciation from the Ministry of National Policy of Japan for her contribution in advancing mutual understanding between the United States and Japan. A native of Tokyo, she holds a B.A. in liberal arts from the International Christian University in Tokyo, Japan and an M.A. in international economics and Asian studies from the Johns Hopkins University SAIS.

PAMELA KENNEDY is a Research Analyst with the East Asia Program. Her research interests include Northeast Asian international relations, U.S. alliances in Asia, and the role of the U.S. in the Indo-Pacific region. She holds an M.A. in International Relations and International Economics from the Johns Hopkins University SAIS and a B.A. summa cum laude in Government and East Asian Studies from the College of William and Mary. Prior to joining Stimson, she interned with the Center for Strategic and International Studies' Japan Chair and the Reischauer Center for East Asian Studies. She was also previously an Associate Examiner with the Federal Reserve Bank of San Francisco, where she reviewed Asian and American banks for safety and soundness.

JASON LI is a Research Assistant with the East Asia Program. His research focuses on U.S.-China relations, cross-Strait relations, and grand strategy in Asia-Pacific. He has also researched the nexus of Chinese infrastructure development and Beijing's relations with developing countries. Prior to joining Stimson, Jason interned with the Center for Strategic and International Studies' Freeman Chair in China Studies. He holds a B.A. from McGill University where he graduated with first class honours in Political Science.

About Stimson

The Stimson Center is a nonpartisan policy research center working to solve the world's greatest threats to security and prosperity. Think of a modern global challenge: refugee flows, arms trafficking, terrorism. These threats cannot be resolved by a single government, individual, or business. Stimson's award-winning research serves as a roadmap to address borderless threats through collective action. Our formula is simple: we gather the brightest people to think beyond soundbites, create solutions, and make those solutions reality. We follow the credo of one of history's leading statesmen, Henry L. Stimson, in taking "pragmatic steps toward ideal objectives." We are practical in our approach and independent in our analysis. Our innovative ideas change the world.

About the East Asia Program

The East Asia Program conducts research on vital regional security issues such as cross-Strait relations between the PRC and Taiwan, U.S. alliance relationships with Japan and South Korea, and China's foreign policy in developing states. The program's researchers seek to provide insights and recommendations for policymakers in the U.S. and in the region. Through dialogues, seminars, and reports, the program promotes a fruitful exchange of views on current challenges and helps develop innovative and pragmatic policy solutions.

DISINFORMATION, CYBERSECURITY, & ENERGY CHALLENGES

Security studies of Taiwan often focus on cross-Strait relations, but nontraditional security challenges—cross-border, non-military issues—pose significant threats to Taiwan's future prosperity and stability. Moving beyond a state-centric conception of security to a broader concern with the well-being of communities and individuals, a nontraditional security approach emphasizes collaboration between many partners. How can Taiwan leverage state and nonstate cooperation to effectively mitigate this type of security issue? What can other governments learn from Taipei's experience? In this collection of policy briefs, three emerging experts analyze the impact of several nontraditional security challenges in Taiwan—online disinformation, cybersecurity in the digital economy, and energy security—and discuss creative solutions.

STIMSON