POLICY BACKGROUNDER 21-1

Mutual Legal Assistance in the Digital Age and Taiwan's New Southbound Policy

Russell Hsiao and Zoe Weaver-Lee

November 2021

Global Taiwan Institute

Introduction

Major advancements in human innovation throughout history have always brought about disruptions to our way of life. While the 19th century was defined by the disruptive development of manufacturing processes—followed by a century of revolutions in technology, medicine, and new types of warfare—the 21st century is being disrupted by the information and telecommunications (ICT) revolution, epitomized by the Internet, cloud computing, artificial intelligence (AI) to connect people, businesses, and governments, and perform computations in hitherto unimaginable ways.

The ICT revolution is fueled in part by the digitization of information—compression of data into bytes—which is more capable of being collected, stored, accessed, and transmitted faster, more efficiently, and over multiple mediums of communication technology than ever before. The increased use of new communication technology for daily personal engagements, sophisticated commercial transactions and computations, healthcare, and mission-critical military operations underscore the revolutionary quality of the digital age. Yet, a heavy reliance on digital technology presents new challenges for governments that seek to maximize its benefits, but also minimize the security risks.

"[A] heavy reliance on digital technology presents new challenges for governments that seek to maximize its benefits, but also minimize the security risks."

The Internet, on top of which many communication technologies operate, was designed as a borderless network that is open and accessible. Because of its open nature, of the world's total population of 7.8 billion, there are currently around 4.6 billion Internet users throughout the world. With 298.8 million Internet users as of January 2021, 85.8 percent of the US population accessed the Internet as of 2020.[1] Setting aside the global challenge of the digital divide between the haves and the have-nots, the world has never before been so "connected."[2]

Not only are people more connected with each other than ever before; we are also interacting on this platform with greater sophistication than even just a decade before. Simple text messages, online purchases—some illegal, such as through the dark web—certain types of healthcare, and complex financial transactions can be made through different communication networks like messaging applications. Yet, the increase in the number as well as the sophistication of transactions, such as through cryptocurrencies, involving the use of advanced digital technology have also been closely associated with an increase in cybercrimes.

As of 2020, the global cost inflicted by cybercrime was estimated to be nearly $1 trillion ($945 billion). In the first half of 2019, more than 4 billion personal records were exposed, and as of August 2020, the US was investigating health information breaches for almost 35 million individuals.[3] The perpetrators of such crimes are also not limited by the locality in which they reside as almost all transactions can be performed in cyberspace. "In the U.S., officials from the FBI's IC3 reported that during the pandemic, cybercrime complaints increased from 1,000 to 3,000 to 4,000 daily."[4] Yet, criminal activity has not only become easier on an individual level, but also in the spheres of state-sponsored activities and organized crime.

For example, in February 2016, North Korean hackers used malware to access the Bangladesh central bank's computers and spoof messages to the US Federal Reserve Bank.[5] They transferred $81 million from the central bank's account at the New York Federal Reserve Bank to Philippine banks.[6] Taiwan has experienced its own share of organized cyber-attacks, which have increased 40-fold in 2020 compared to 2018.[7] The ten government agencies that were subject to email data infiltrations in August of 2020, for example, have since attributed the attacks to Chinese Communist Party (CCP)-backed hacking groups in China.[8] While attacks which seek to obtain sensitive documents have largely targeted Taiwan's public sector,[9] private corporations have also been subject to malware breeches. Quanta Computer, a manufacturer of Apple Products in Taiwan, was targeted by anonymous hackers seeking to obtain the blueprints of flagship Apple products. The crime organization also laid claim to previous attacks on Travelex, as well as the New York law firm Grubman Shire Meiselas & Sacks.[10] Cybercrimes affect Taiwan not only by attacking targets within the country but also by exploiting soft targets as part of broader attacks against its networks outside the island.

Criminal activity has become more low-cost and can more easily transcend national borders than ever before. Without adequate law enforcement cooperation mechanisms, the costs for committing cybercrime will remain low, and the benefits high. As such, law enforcement in the digital age requires access to potential sources of evidence that transcend national borders.

These cases represent sophisticated attacks, but they are also just the tip of the iceberg. It should be clear that combatting crimes in the digital age necessitates closer as well as more efficient coordination between law enforcement agencies across the world than ever before. The legal process by which government agencies seek cooperation from other law enforcement agencies are called mutual legal assistance treaties/agreements (MLAT/MLAA). These agreements generally allow for the exchange of evidence and information in criminal and related matters.[11] Not all MLAAs are created the same and are tailored to the specific needs of the bilateral relationship. Such agreements, however, generally cover criminal investigation procedures including interrogating witnesses, providing documents, confirming related parties' identifications and residences, service of documents, assisting procedures in execution for search, seizure, and confiscation; freezing of assets, enforcing a court asset forfeiture order, or enforcing an international asset sharing agreement; and any form of assistance not in violation with the Law and Act of the country requesting for assistance.

"...combatting crimes in the digital age necessitates closer as well as more efficient coordination between law enforcement agencies across the world than ever before."

As of 2021, Taiwan has inked substantial cooperative agreements with several governments in pursuit of mutual legal assistance. Several judicial pacts have been signed between Taiwan and various European nations (including Slovakia, Poland, Germany, the UK, Denmark, and Switzerland) as well as Brazil,[12] which focus on sharing law enforcement experience, criminal extradition procedures, and enhanced legal assistance. Perhaps one the most comprehensive was in cooperation with Poland, which took effect in February of 2021. According to Taiwan's Ministry of Justice, the agreement covers five key areas of cooperation, including "mutual assistance on criminal legal matters, extradition, prisoner transfer, exchange of legal and practical insights, and sharing of information on crimes and crime prevention."[13]

The importance of establishing such agreements cannot be overstated. A prime example that illustrates this point is the challenge posed by data stored in emails. Email is the most prevalent form of electronic communication, making it an essential and valuable source of information for criminal investigation. All internet companies providing commercial e-mail services store customers' e-mail messages in data centers, which are physical facilities containing clusters of networked computer servers that may be used for remote storage, processing, or electronic transmission of data. Major commercial entities maintain and control data centers around the world for various reasons, including to enjoy tax benefits.[14]

The complications posed by such a system were made apparent in a legal case regarding this storage of data that had to be accessed by law enforcement. In *Microsoft v. United States*, prosecutors at the Department of Justice sought and obtained a warrant in 2013 for the information contained in a Microsoft Outlook account. However, the requested information was stored in computer servers based in Dublin, Ireland.[15] While Microsoft challenged the legality of the warrant, arguing that it could only apply to data stored within the United States, The District Court sustained the warrant authorizing the search and held Microsoft in contempt for then failing to produce the data. The case reached the Supreme Court but the legal issue was mooted with the passage of the Cloud Act.

One relevant policy dimension to the Microsoft dispute is the availability and efficacy of alternative means for the government to access data stored overseas. In *Microsoft*, there is no dispute that the company could technically, from within the United States, retrieve the requested information from Ireland. Yet, this question is not a technical one, it is a legal one as well as a matter of policy and international relations.

In an age where information is dispersed and can be stored in data centers across the world, legal issues concerning which jurisdiction has control over the service provider and data, regulating how the data is stored, who controls the data, privacy, access to the data, and use of the data will affect the ability of law enforcement agencies to perform their duties and investigate crimes.

As noted by professors Roderic Broadhurt and Lennon Chang:

> A key problem in the prosecution of cybercrime is that all the elements of the offence are rarely found in the same jurisdiction. Often the offender and the victim and even the evidence are located in different jurisdiction thus requiring a high degree of cooperation between the law enforcement agencies to investigate and prosecute (Brenner 2006). The extent that Asia has been able to address the need for such cooperation is addressed by describing the first international instrument and the role it has played in developing cybercrime law in Asia.[16]

Therefore, the function of MLAAs is clearly a necessity if we want to preserve the benefits and economic efficiency brought about by the Internet and modern communication technologies. Indeed, "MLATs are bilateral agreements that effectively allow prosecutors to enlist the investigatory authority of another nation to secure evidence — physical, documentary, and testimonial — for use in criminal proceedings by requesting mutual legal assistance."[17] Yet, these mechanisms are either woefully inadequate or non-existent in Asia.

Cybercrimes in Asia

For foreign policy and security experts in the United States, Asia is widely considered to be the epicenter of global economic and geopolitical activity in the 21st century.[18] Over the last decade, the US government began a gradual shift in its application of military, economic, and diplomatic resources to the Indo-Pacific region. The region already serves as a key engine for global economic growth and encompasses the fastest growing economies in the world. According to the International Monetary Fund's *Asia Economic Outlook,* Asian economies are expected to contract by 2.2% in 2020 due to the impact of COVID19, but will rebound, growing 6.9% in 2021, as the region continues to be the leader of global growth.[19] According to a McKinsey study, the vast Asia-Pacific region accounts for 45% of global payment revenue.[20] This is not hard to envision given the scale of internet penetration throughout the region.

As of March 2021, there were over 2.7 billion Internet users in Asia, which accounts for more than half of the world's internet users.[21] At 92.4 percent, Taiwan is ranked fourth in terms of Internet penetration in the Asia-Pacific, only behind South Korea, Brunei, and Japan.[22] Other countries in the region also enjoy high Internet-penetration rates such as Malaysia (89%), Thailand (81.5%), Philippines (80.2%), and Vietnam (76.1%).

While many other countries in the Indo-Pacific do not have as high of a penetration rate due to their developing economies, the boom in Internet access in those countries has expanded considerably over recent years and this growth trend is set to continue for the foreseeable future—particularly in the mobile sector. Smartphones, which are essentially handheld personal computers, have seen adoption across Asia continue to increase, with the penetration rate in the region rising to 64% in 2019, and projected to rise to 81% by 2025.[23]

> "In an age where information is dispersed and can be stored in data centers across the world, legal issues concerning which jurisdiction has control over the service provider and data, regulating how the data is stored, who controls the data, privacy, access to the data, and use of the data will affect the ability of law enforcement agencies to perform their duties and investigate crimes."

Just as connectivity is key to economic development, however, increased access and contact have also led to an increase in cybercrimes. The Asia-Pacific region in particular is facing unprecedented levels of complex cybercrime and fraud attacks. As revealed by Check Point Research, APAC is facing significant threats: a 168 percent increase year-on-year in the number of daily attacks in May 2021 compared to May 2020.[24] Underscoring the severity of this challenge, an investigation into cybercrime in Southeast Asia found that malware-infected servers as well as compromised websites were widespread. Among the 270 that were compromised were government portals, which Interpol attributed to an exploitation of "vulnerability in their design applications."[25] According to a *Symantec* 2019 report, Taiwan ranked 8th in the world for malicious email rates at 1 in 163.[26] Saudi Arabia was ranked 1st at 1 in 118.[27] By another measure, for four consecutive years in the late 2000s, Taipei had the most botnet-infected computers among cities in the region.[28]

A recent string of cyber attacks on Asian banks—including some that exploited weaknesses in how institutions use Swift, the international financial messaging service—further underscores the risks.[29] According to one independent survey, more than 80% of Asia-Pacific organizations reported an attack of some form in 2020.[30] The attacks ranged from customers being swindled out of remittances to direct hacks on the banks' core systems.

The cost of cybercrime is enormous. According to a study commissioned by Microsoft, the potential economic loss across Asia Pacific due to cybersecurity incidents can hit a staggering $1.745 trillion (2018).[31] In addition to monetary costs, cybercrimes also pose insecurity to our delicate web of online activity. Costs can thus also include system downtime and outages, reduced efficiency, brand damage and loss of trust, and even damage to employee morale.[32]

The Asia-Pacific also has higher attack rates than the global average in 2020 (3% compared to 1.4% globally).[33] Notwithstanding the staggering data, the extent of Asia's vulnerability is difficult to quantify because of the lack of laws and regulations that would compel companies or governments to disclose attacks, such as through data breach notification laws, adequate capacities to respond to sophisticated cyber intrusions, and mechanisms to facilitate cooperation between law enforcement officials across the region.

Taiwan: The Missing Node

As exemplified by the cases above, international cooperation is essential to combatting transnational cybercrime. Yet, with 15 diplomatic partners, Taiwan is marginalized diplomatically in the international community by the People's Republic of China (PRC). At present, its diplomatic partners and robust unofficial relationships[34] with countries like the United States and Japan,[35] which support its *de facto* independence and international space to engage in functional areas of cooperation, remain its path to international engagement.

With a population size of nearly 23.6 million,[36] its unfavorable diplomatic situation belies the country's outsized strength in terms of its democratic system and economic model. Taiwan is home to a vibrant democracy that supports many international conventions, which it is unable to officially sign onto as a member, and the world's 22nd largest economy in terms of real GDP (purchasing power parity).[37] However, the long-term viability of its political and economic development, as well as its capacity to combat transnational cybercrime, depends in part on its ability to integrate into emerging regional and global institutions. Unfortunately, its international status impedes its ability to negotiate and sign agreements with other national governments.

Law Enforcement in the Context of Cross-Strait Relations

Beijing's claims over Taiwan and its pressure tactics limit the ability of Taipei to engage with other countries not only diplomatically, but also economically due to concerns of the other countries about potential PRC reactions. As the pressure that Beijing exerts is politically motivated, its intended purpose is to interfere in Taiwan's democratic process and represents an attempt to delegitimize the Taiwan government, and specifically, any political parties that do not adhere to its political objectives. This undue limitation transcends high-level politically-sensitive engagement that may confer any real sense of officiality with countries whom Beijing has diplomatic relations and serves Beijing's underlying purpose of isolating Taiwan globally, while coercing its leaders into accepting its terms for political unification.

In terms of law enforcement cooperation, China has not shied from using its coercive strategies to block Taiwan from Interpol membership, including outright claiming its ineligibility based on its "One-China Principle."[38] Efforts for Taiwan to become a member of Interpol have thus been wrought with obstacles, as repeated letters from Taiwan's Criminal Investigation Bureau have been met with the suggestion that its head should "contact Beijing."[39]

Meanwhile, Taiwan's isolation from the international community also poses challenges for Beijing with regard to transnational cybercrime. Considering its lack of access to Interpol databases, Taiwan cannot adequately cooperate in criminal investigations involving PRC fugitives hiding on the island. Additionally, terrorists and saboteurs can easily flow from Taiwan into the PRC. The risks posed by Taiwan's shut-out from Interpol are thus also dealt to Beijing, which makes it in the PRC's best national security interests to allow Taiwan access to international law enforcement channels.[40]

Taiwan's exclusion from Interpol not only inhibits its ability to mitigate an inflow of criminal activity, but also subjects the international community—including Beijing—to virtually undetectable criminal activity exports from Taiwan. As highlighted by Deputy Assistant Secretary of State Rick Waters in October 2021, an unfortunate example of this occurred when a man in Taipei murdered his mother- and father-in-law, abducted a child, and fled the country. Despite Taiwan's attempts to share this information with Interpol members, it was unsuccessful in doing so.[41] The man was eventually arrested by Kurdish police in Iraq after he sent a LINE message

to his wife indicating his whereabouts.[42] In this case and others, Taiwan's ability to share vital information regarding its fugitives at-large is essential, and its difficulties in doing so preventable. As Waters argues, "[w]e view these practical hurdles as endangering all UN members, not just those on Taiwan."[43] An area that is a natural conduit of greater cooperation for Taiwan is the Indo-Pacific region.

Taiwan's New Southbound Policy

Against the backdrop of Taiwan's growing dependence on China, but simultaneously stimulated by the rapidly developing economies of Southeast and South Asia and Taiwan's own changing demographic reality, Taiwan has revitalized a southward all-of-government strategy in the "New Southbound Policy" (NSP).

The NSP—aimed at building economic as well as people-to-people ties between Taiwan and 18 countries across South and Southeast Asia, as well as Australia and New Zealand—has been the hallmark of President Tsai Ing-wen's foreign policy since she came into office in May 2016.

Over two decades ago, Lee Teng-hui (1992-2000), who was then president and chairman of the Kuomintang (Nationalist Party), launched the "Southbound policy" in 1993. Driven by diplomatic necessity and economic motives, the policy was put forward as a broader foreign policy strategy to engage Southeast Asian countries based on Lee's "pragmatic diplomacy" in the face of Beijing's long-standing efforts to isolate Taiwan internationally. Lee's policy was enhanced by Chen Shui-bian (2000-2008) in the first-ever Democratic Progressive Party (DPP) administration by expanding the volume of investments and prioritizing free trade agreements. The latter focus was likely motivated by the PRC's push to negotiate the China-ASEAN free trade agreement (which came into effect in 2010).

While not using the same name, the Southbound policy was continued under the previous Ma Ying-jeou (2008-2016) Administration. Shaped by the Ma Administration's primary focus on improving cross-Strait relations, the government promoted the concept of "viable diplomacy" and ostensibly downplayed the diplomatic elements of the Southbound policy.

From the 2016 campaign trail to the presidential office, the DPP and Tsai have gone to great lengths to argue that the new policy is not just window-dressing on old ideas. In addition to a series of new guidelines and plans, the policy was prioritized when the government established the "New Southbound Policy Office" in the Presidential office.

To further distinguish her administration's initiative from predecessors', President Tsai outlined four prongs to her new approach: 1) developing and sharing talent and resources, 2) developing industrial cooperation and the development of domestic markets, 3) developing manufacturing capabilities, and 4) developing small and medium-sized enterprises.

ASEAN and South Asia nations encompass 33.5 percent of the world's population and have a combined GDP of $6.43 trillion.[44] NSP countries as a bloc represent the second largest trading partner – only behind China, which has been Taiwan's dominant trading partner. The Asian Development Bank estimates that the annual economic growth rate for ASEAN and South Asian countries will be between 4.4 and 9.5 percent in 2021.[45]

Transnational Policing and Demographic Change

The demographic landscape in Taiwan has also changed significantly since the 1990s. Over 90% of foreign workers in Taiwan come from NSP countries. With over 711,000 migrant workers,[46] alongside a fast growing population of "new residents" and their children at nearly one million combined, Taiwan's society today is increasingly diverse.[47]

The top four countries of origin of Southeast Asian migrants are Vietnam, Indonesia, Thailand, and the Philippines. The number of the second-generation immigrants has surpassed 350,000 and 52% of their parent(s) are of Southeast Asian origin, equating to about one in six newborn babies being born to new immigrant families. Second generation immigrants made up 10.7% of 1st through 9th grade students in 2017.[48]

Taiwan has also implemented policies to lift visa restrictions on travelers from NSP countries in hopes of increasing tourism, a strategy which has proven largely successful. Programs which allow short-term visa-free entry and e-visas led to significant increases in tourism from Thailand and Brunei in particular, which expanded 57 percent and 52 percent respectively. Yet, as noted by researchers at CSIS, such lax regulations have also been subject to security concerns.[49] For example, while Taiwan experimented with easing restrictions for Filipino citizens travelling

to Taiwan in 2017, the Taipei Economic and Cultural Office temporarily halted the program due to concerns surrounding Islamist rebels in Marawi. A representative of the office stated that such measures were taken to ensure terrorist leaders "don't enter Taiwan." The program was resumed several months later as the conflict reached a resolution. Considering these visa policies were implemented just prior to the outbreak of the COVID-19 pandemic, there is little data available to determine their implications for Taiwan's domestic security. It should be clear, however, that such initiatives are expected to be expanded in the future.

This trend is poised to continue as the region grows. Yet, the absence of formal diplomatic relations between Taiwan and the target countries under the policy impedes national government-level contacts that can help promote the policy's objectives—which would necessarily include the protection of migrants from those countries. The absence of diplomatic relationship should not come at the expense of legitimate law enforcement cooperation to combat a growing problem facing the entire region. The New Southbound Policy thus serves as an ideal platform to facilitate law enforcement cooperation among key countries.

Existing MLAAs in Asia with Taiwan and the PRC

The maritime and land borders that traditionally served as natural boundaries between these countries are becoming increasingly blurred in the digital age. More people, businesses, and commercial interests cross borders, and increasingly because of the Internet—and dark web—it is not necessary to physically enter another territory to engage with that country. This presents a serious issue for law enforcement agen-

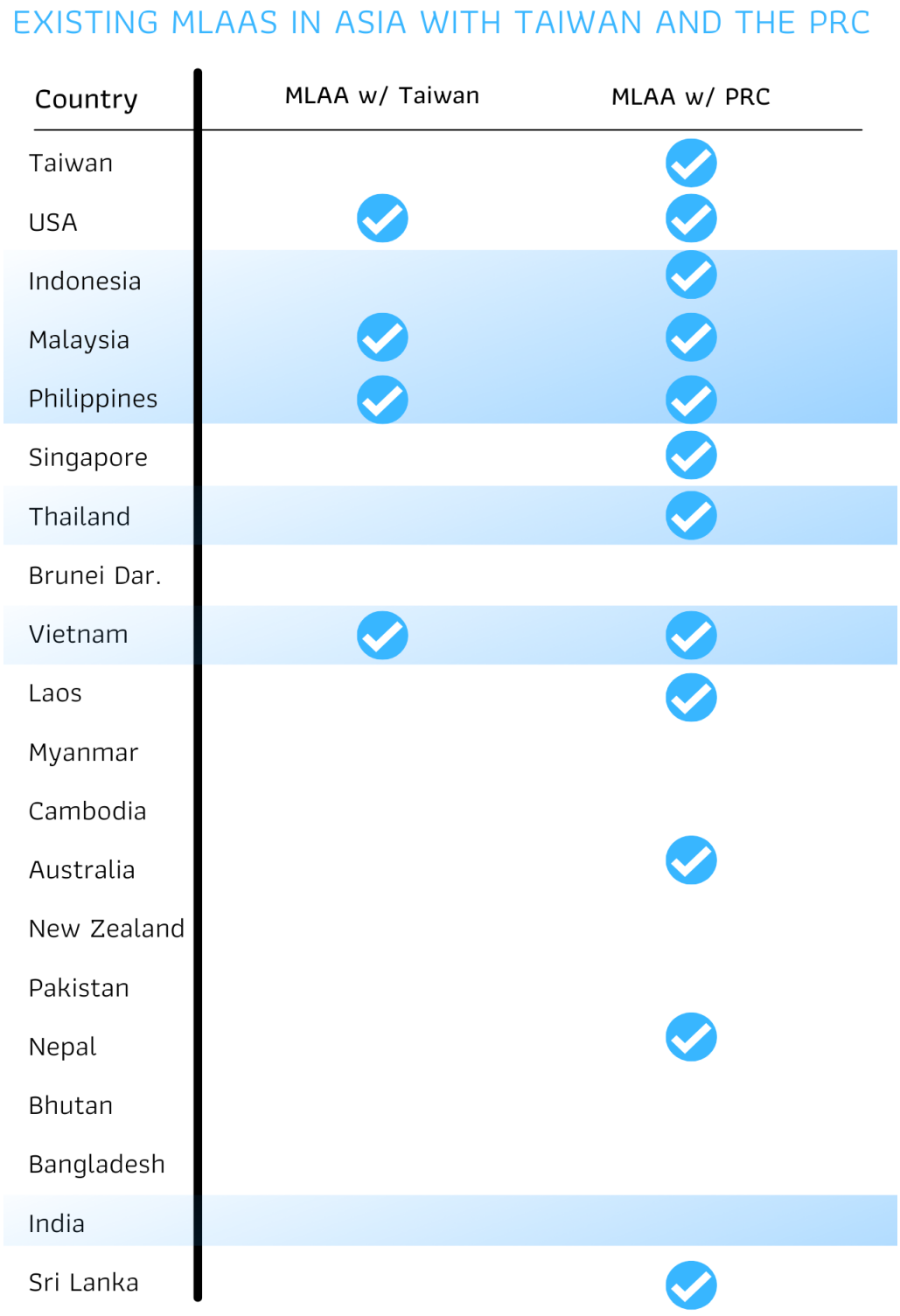

Figure 1: Highlighted sections denote NSP-focused countries

cies that need to enforce domestic laws and keep the peace.

For instance, the PRC, the Philippines, Thailand, and Burma remain the primary sources of drugs smuggled into Taiwan.[50] Through the dark web and advanced encryption techniques, drug dealers are able to coordinate their activities without needing to step foot into the country. This makes transactions of all sorts harder to monitor and trace. In the cyber security world, this situation marks the transition from a perimeter-based defense to a transactional-based defense architecture. Just as technology advances, so too does law enforcement cooperation need to keep pace.

> "The maritime and land borders that traditionally served as natural boundaries between these countries are becoming increasingly blurred in the digital age. More people, businesses, and commercial interests cross borders, and increasingly because of the Internet—and dark web—it is not necessary to physically enter another territory to engage with that country."

The challenges presented by the proliferation of online disinformation also require transnational cooperation. The source of disinformation can originate outside the country in which it affects the targeted audience. In such instances, the servers of the original source may be located in another country and thus require the use of a MLAA, as Microsoft argued in its case, to facilitate the access of information to trace and investigate the case. For instance, content farms in Malaysia have been identified as one of the sources of disinformation that flooded into Taiwan's information space in the lead up to the 2020 presidential and legislative elections.[51]

Despite the growth in people-to-people and economic ties between Taiwan and NSP countries, the legal framework by which law enforcement agencies are able to cooperate with one another to preserve law and order are woefully inadequate given the transnational nature of cybercrime in the digital age.

As noted earlier, the nature of digital crimes makes it necessary for law enforcement agencies to work closer together – but it must be done through a legal mechanism with established protocols that are reconcilable by the domestic law and judicial system. The alternative of permitting extraterritorial actions that in effect impose the domestic law of one country will sow mistrust and lead to greater friction; even leading to the balkanization of the Internet. A legal process by which to exchange information, conduct investigations, and prosecute crimes to deal with these problems can help defuse and regulate procedures by which both sides would agree to abide in order to minimize misunderstanding as well as prevent tensions from flaring up.

Indeed, according to Broadhurst and Chang, "[t]he transitional nature of cybercrime basically requires that states enact laws to harmonize definitions of criminality and enhance mutual cooperation across states."[52] As one example, an issue that affects all society is human trafficking. Strengthening mutual legal assistance with other countries to further curb cross-border human trafficking is thus in the interest of everyone. [53] Yet, Taiwan currently only has two mutual legal assistance agreements with countries covered under the New Southbound Policy: Vietnam and the Philippines, out of the 18 total.

Taiwan-Philippines MLAAs

Taiwan and the Philippines signed a MLAA in 2013. Since its inception, there have been a total of 37 recorded requests made by both sides with 10 requests completed.

In the May 2013 Balintang Channel shooting of a Taiwanese fisherman north of Luzon, the MLAA served as a useful tool that enabled Philippine investigators to travel to Taiwan and gain access to evidence.[54]

More recently, an individual deemed an "economic criminal" by Taipei is reportedly investing a large sum of money into the Philippines. In this case, the MLAA will ostensibly provide the mechanism by which the law enforcement agencies can share information and cooperate. While this particular case presents a unique situation given the individual holds a PRC passport, the case presents an example of the complex legal issues that must be resolved for effective law enforcement.[55]

In September 2017, the president of the Philippines made the claim that an international criminal organization based in Taiwan, with known operations throughout Europe and the Asia-Pacific, is using the Philippines as a transshipment point for drugs and requested US assistance.[56] A more effective and efficient MLAA process could help facilitate better information sharing and transnational investigations into these criminal activities.

Taiwan-Vietnam MLAAs

Taiwan and Vietnam signed a MLAA in 2011. Since its inception there has been a total of 7,304 recorded requests made by both sides with 5,019 completed requests.

Negotiations for an MLAA between the two countries began as early as 2008. In addition to the traditional areas of cooperation, the MLAA with Vietnam also includes areas covering civil matters and family matters, including mutual recognition provisions for certifying documents, divorcing, inheritance, and civil judgment for people in Taiwan and Vietnam.[57]

Both the Taiwanese and Vietnamese governments are very concerned about issues relating to public order, criminal acts, marriage, rights and interests for divorced Vietnamese, and rights for fostering offspring, since these issues can easily arise due to the large number of Vietnamese people in Taiwan.[58]

CRIMINAL INVESTIGATION REQUESTS BY PARTNERSHIP

Partnership	No. of Requests	Completed	In Execution	Completion Rate
Taiwan & USA	209	180	29	86%
	101	87	14	86%
Taiwan & Philippines	13	1	12	8%
	9	9	0	8%
Taiwan & Vietnam	4,292	2,723	1,569	63%
	4,003	3,878	125	97%
Taiwan MLAT Response Rate	4,252	4,075	177	96%

*Figure 2: *Taiwan has also requested legal assistance from other countries with which it has no formal diplomatic ties. There were 196 such cases from 2004 to the end of April 2013. ** In 2000, the United States sent over 500 MLA requests and received over 1,500. In 2014, the United States sent over 1,000 requests and received around 3,250.* [59]

Taiwan-US MLAAs

By way of comparison, the United States and Taiwan signed a MLAA in 2002 and already have 19 years of experience in executing and responding to MLAA requests. In those 19 years, the two sides have submitted a total of 310 requests, of which 267 have already been completed. The high completion rate demonstrates the capacity and efficiency of the MLAA process between the United States and Taiwan.

"In those 19 years, the two sides have submitted a total of 310 requests, of which 267 have already been completed. The high completion rate demonstrates the capacity and efficiency of the MLAA process between the United States and Taiwan."

While every bilateral relationship varies, creating a unified protocol can help streamline and make assistance in cooperation by law enforcement agencies more efficient. For instance, when the US Department of Homeland Security in Los Angeles investigated a Latin American drug cartel, they found that a Taiwanese woman was laundering money from drug trafficking income under the cover of importing, exporting, and selling garments in the United States. The US Department of Justice, pursuant to Taiwan-US Mutual Legal Assistance Agreement, requested Taiwan's Ministry of Justice to assist in seizing the account of the woman involved in money laundering and successfully seized more than US$15 million illegal money laundered by the drug cartels in Taiwanese bank accounts.[60]

Global Cooperation and Training Framework

The Global Cooperation and Training Framework (GCTF) is a multilateral forum coordinated by the United States, Taiwan, and Japan that addresses a wide range of transnational issues and has implemented several initiatives which focus on transnational crime, law enforcement cooperation, and cyber security threats.[61] Beginning in 2018 with the workshop "Combating Transnational Crime and Forensic Science," representatives from key agencies discussed cooperation between law enforcement and intelligence agencies to combat transnational crimes. Representatives from the US Department of Homeland security, US Drug Enforcement Administration, US Secret Service, American Institute in Taiwan (AIT), Taiwan Ministry of Foreign Affairs (MOFA), and Taiwan's Ministry of Justice Investigation Bureau

(MJIB) discussed strategies to target issues such as passport fraud, narcotics trafficking, and counterfeit money.[62]

US agencies have continued to play a key role in the GCTF's focus on transnational and cybercrime, such as their participation in the GCTF's March and May 2019 gatherings. Both workshops were attended by representatives from key agencies such as the Ministry of Justice Agency Against Corruption, US Department of Justice (DOJ), Federal Bureau of Investigation (FBI), the US Department of Homeland Security, the State Department, and the Federal Communications Commission to discuss initiatives to prevent corporate espionage and preserve trade secret protection[63] as well as tackle global information security threats,[64] respectively. Critically, these events underscored Taiwan's valuable experience and role in these issues.

In fact, Taiwan's expertise has led to significant advancements in the GCTF's reach in other fields as well. Its experience in protecting trade secrets and countering digital piracy, for example, provided a foundation for one of its 2020 workshops which focused on intellectual property rights in the modern digital economy.[65] Representatives from the US District Court and the Northern District of California joined the conversation, sharing their own experiences and hoping to bring lessons back to their own organizations. Similarly, Taiwan's impressive record combating COVID-19 served as a backdrop to the 2020 GCTF workshop, "Combating COVID-19 related Crimes." The forum, which was attended by key law enforcement experts from the United States, Taiwan, Japan, and Australia, focused on COVID-19 schemes and disinformation,[66] with which Taiwan is all too familiar.[67]

Perhaps one of the most concrete displays of the importance of Taiwan's role in law enforcement cooperation took place in 2021 through GCTF's program, "Virtual Conference on Combating Cybercrime through International Law Enforcement Collaboration." The attendees, which included Taiwan's National Police Agency, MOFA, and Ministry of Interior as well as FBI crime experts, collaborated on issues related to technology supply chains, tech infrastructure, ransomware, and Taiwan's participation in Interpol. AIT Deputy Director Jeremy Cornforth noted in his opening remarks, "Although Taiwan is prevented from participating meaningfully in Interpol and many other international organizations, today's event will highlight the many ways that Taiwan is sharing its expertise with the international community, as well as how the global cyber community shares lessons with Taiwan in order to tackle the shared challenge of cybercrime."[68] Indeed, the GCTF continues to serve as a key platform for Taiwan to collaborate with its allies on transnational crime and cybersecurity issues. As such, it is critical that Taiwan use this medium to build official law enforcement cooperation agreements.

US Support for Taiwan in Interpol

Although the United States and Taiwan have engaged in extensive discussions surrounding transnational crime in the context of GCTF, for the aforementioned reasons and others, the US also supports Taiwan's entry into Interpol. Following the passage of the 2016 bill cementing US support for Taiwan observer status in Interpol, the United States has made it clear that ongoing international threats make it imperative that Taiwan gain access to Interpol's communications system and databases. This sentiment was reaffirmed by the passage of the TAIPEI Act in 2019, which stipulates that US policy is to advocate for Taiwan's membership in international organizations in which statehood is not a requirement, and push for observership in those for which it is. Despite these developments, several US representatives have proposed additional legislation that directly targets Taiwan's UN participation, citing increased pressure from China. As of April 2021, Congressman John Curtis and a bipartisan coalition introduced Taiwan Solidarity Act, which included a specific section on Taiwan's Interpol observer status. Several other nations have voiced support for Taiwan's participation, demonstrated by calls for its observership during Interpol's general assembly in 2019.

Conclusion

Webs of bilateral and multilateral agreements make up a system to facilitate criminal investigations and prosecutions in the nations that are parties to them. MLATs are the backbone of global cooperation among law enforcement agencies in cases that involve, but are not limited to, "locating and extraditing individuals, freezing assets, requesting searches and seizures, and taking testimony."[69]

As the world "flattens" digitally in the 21st century with ascent of the information revolution, more data is moving online—including that of criminals and their victims increasingly in the "dark web" that requires more sophisticated tracing; the MLAT system has been slow in keep-

ing pace with the rapid changes of data globalization. Indeed, the DOJ estimates that over the past decade the "number of [MLAT] requests for assistance from foreign authorities handled by the Criminal Division's Office of International Affairs has increased by nearly 60 percent, and the number of requests for computer records has increased ten-fold."[70] In light of this growth in reliance on MLAT requests, much must be done to address the issues of jurisdiction over cross-border data transfers, privacy, and legitimate law enforcement needs for evidence.

Some commentators have described MLATs as an expression of state sovereignty. Yet, there exists great ambiguity regarding state sovereignty within cyberspace—if it is even practicable to think in terms of traditional sovereignty in cyberspace. The Internet is a distributed "network of networks" that is transnational in scope, with servers and routers that store, process, and switch information located essentially anywhere in the world that is connected by a communication platform. Although a government must have the right to legitimately regulate activities that have a substantial effect within its territory, the cross-border nature of the Internet necessarily involves legal regimes that extend beyond the national boundaries of a country.

Indeed, "international law has traditionally allowed countries nearly unlimited power to make law territorially subject only to some specific prohibitions, like the human rights norms against genocide and torture." Moreover, "[t]he power to regulate extraterritoriality, while broad, is not unlimited: a state may make law governing 'conduct outside its territory that has or is intended to have substantial effect within its territory...'" Given its multinational roots, it is reasonable that the appropriate legal framework to use in Internet governance would include elements of international law. However, an absolutist approach to state sovereignty in cyberspace is untenable for the preservation of the Internet as we know it.

In addition to United States' efforts to expand its capacity on combatting transnational cybercrime, primarily through the passage of the 2018 CLOUD Act,[71] which provides "trans-border access to communications data in criminal law enforcement investigations," it has a MLAA with Taiwan that has been active since 2002.[72] There is still room for the US to support Taiwan's participation on a multilateral level, however, as even in the most recent cybersecurity summit hosted by the United States, few key Asian nations appear to be on the list of attendees (including only Japan, Korea, India, Singapore, and the UAE).[73]

Considering Taiwan's existing establishment of both forums and bilateral agreements which work toward greater cross-border law enforcement cooperation, Taiwan already has a foundation on which to improve. There are, however, significant steps to be taken in order to appropriately address new risks posed by cybercrime.

"Given its multinational roots, it is reasonable that the appropriate legal framework to use in Internet governance would include elements of international law. However, an absolutist approach to state sovereignty in cyberspace is untenable for the preservation of the Internet as we know it."

As this report has demonstrated, the costs posed by transnational cybercrime to economies and societies are significant regardless of political borders. As such, the establishment of MLAAs should not be zero-sum and, particularly, cooperation between Taiwan and China to combat crimes should not be politicized. Yet an agreement – signed in 2009 – has apparently been shelved due to strained cross-Strait ties.[74] This has proven to not be in the interests of neither China nor Taiwan, which both rely on law enforcement cooperation to effectively address transnational organized crime. An important step would thus be the immediate resumption of cross-Strait dialogue surrounding these topics.

By the same token, the depoliticization of Taiwan's participation in international organizations is not only essential for law enforcement agencies on the island, but also the international community at large. As such, the United States should continue to support Taiwan's participation in Interpol, assist in Taiwan's effort to designate foreign officers in countries without MLAAs, and explore recent US-Taiwan Coast Guard memoranda to help facilitate information and law enforcement cooperation. Of course, these efforts may begin at forums or other existing platforms, such as GCTF. Doing so will not only accomplish specific goals such as establishing a solid mutual legal assistance protocol in New Southbound Policy countries, but also generally promote Taiwan's value to international crime policing systems.

Of course, Taiwan itself will also bear responsibility in the effort to increase attention on these issues. Considering law enforcement cooperation is best facilitated by a standardized protocol, Taiwan should continue to uphold interna-

tional conventions and unilaterally upgrade its national laws to be consistent with the Conseil de l'Europe (COE)'s Budapest Convention and harmonize regulations with international law enforcement best practices. If successful, efforts to increase law enforcement cooperation can boost responses to drug trafficking, human trafficking, maritime piracy, intellectual piracy, and even responding to natural disasters. More importantly, the increasingly complex effort to combat transnational cybercrime will be better facilitated by a well-connected and more cooperative Taiwan.

ENDNOTES

1 "Internet usage in the United States- Statistics & Facts," *Statista*, accessed November 17, 2021, https://www.statista.com/topics/2237/internet-usage-in-the-united-states//.
2 For world population, see: "World Population Projections," *Worldometer,* accessed November 17, 2021, https://www.worldometers.info/world-population/world-population-projections/; for worldwide Internet users, see: "Global digital population as of January 2021," *Statista*, accessed November 17, 2021, https://www.statista.com/statistics/617136/digital-population-worldwide/; for US Internet users, see: "Digital population in the United States as of January 2021,"*Statista*, accessed November 17, 2021, https://www.statista.com/statistics/1044012/usa-digital-platform-audience/; For percentage of Internet users in the US: "Internet user penetration in the United States from 2017 to 2025," Statista, accessed November 17, 2021, https://www.statista.com/statistics/590800/internet-usage-reach-usa/.
3 Zhanna Malekos Smith and Eugenia Lostri, "The Hidden Costs of Cybercrime," McAfee, (December 4, 2020).
4 Ibid.
5 "The Lazarus heist: How North Korea almost pulled off a billion-dollar hack," *BBC News Online*, (June 21, 2021).
6 Jeremy Wagstaff and Jim Finkle, "When mobsters meet hackers- the new, improved bank heist," *Reuters*, (March 30, 2016).
7 Matthew Strong, "Cyberattacks on Taiwan's Ministry of Foreign Affairs increased 40-fold in 2020," *Taiwan News*, (March 30, 2021).
8 Yimou Lee, "Taiwan says China behind cyberattacks on government agencies, emails," *Reuters*, (August 19,2020).
9 Huang Ming-chao, "Taiwan Is Crucial to the Global Fight Against Cybercrime," *The Diplomat,* (December 3, 2020).
10 "Taiwan authorities look to Apple supplier hack," *BBC News Online*, (April 22, 2021).
11 US Department of State, Bureau of International Narcotics and Law Enforcement Affairs, 2012 International Narcotics Control Strategy Report (INCSR), (March 7, 2012).
12 For details on all agreements, see: "Mutual Legal Assistance: News and Events," Taiwan Ministry of Justice, accessed November 17, 2021, https://www.moj.gov.tw/2832/2833/2916/2920/2921/.
13 Taiwan Ministry of Justice, "Milestone agreement on judicial cooperation with Poland enters into effect" (press release), August 6, 2021.
14 An example of this is Microsoft Skype's headquarters in Luxembourg: Kevin J. O'Brien, "Microsoft Inherits Sticky Data Collection Issues from Skype," *The New York Times* (February 24, 2013).
15 Where a customer's e-mail data is stored often depends on which data center is closest to the user. This business practice is undertaken in order to reduce network "latency," which refers to the lag time between when a user requests information from the network and the time it is received. Overall, latency is affected by the data's travel distance, the transmission medium, and the number of switching points along the way called "router hops". Access to this information pursuant to a criminal investigation is therefore a complicated process that requires precisely identifying the location of the stored data.
16 Roderic Broadhurst and Lennon Y.C. Chang, "Cybercrime in Asia: Trends and Challenges," *Handbook of Asian Criminology*, (2012): 49-63.
17 Mark A. Rush and Jared A. Kephart, "Lifting the Veil on the MLAT Process: A Guide to Understanding and Responding to MLA Requests," K&L Gates: *Legal Insight*, (January 20, 2017).
18 Dan Blumenthal, Randall Schriver, Mark Stokes, Russell Hsiao and Michael Mazza, "Asian Alliances in the 21st Century," Project 2049 Institute, (August 30, 2011).
19 International Monetary Fund, "Regional Economic Outlook: Asia and Pacific, May 2017: Preparing for Choppy Seas" (report), May 2017.
20 Vinayak HV, Florent Istace and Raj Kamal, "Insights from McKinsey's Asia-Pacific Payments Map," McKinsey, (September 2012).
21 "Internet Users in the World by Regions," Internet World Stats, accessed November 17, 2021, https://www.internetworldstats.com/stats.htm.
22 "Internet penetration in Asia as of June 2020, by country," Statista, accessed November 17, 2021, https://www.statista.com/statistics/281668/internet-penetration-in-southeast-asian-countries/.
23 Joseph Waring, "Smartphone adoption in Asia tops 50%," *Mobile World Live*, (January 23, 2017).

24 "Cybercrime Attacks Rise 40 Percent Across Asia-Pacific with Identity Attacks Double the Global Average," *Threat-Metrix*, (December 12, 2016).
25 Lindsay Murdoch, "In South-east Asia, cyber criminals make hay of government websites, citizen data," *Sydney Morning Herald*, (April 26, 2017).
26 "Internet Security Threat Report," *Symantec* Vol 24, (February 2019).
27 Ibid.
28 Jianhong Liu, Bill Hebenton and Susyan Jou, *Handbook of Asian Criminology* (New York: Springer Science+Business Media, 2013).
29 "Asia Hacking: Cashing in on cyber crime," *Financial Times*, (September 19, 2016).
30 Shannon Williams, "More than 80% of APAC organizations suffered a cyber attack in 2020- - study," *Security Brief,* (February 1, 2021).
31 "Cybersrecurity threats to cost organizations in Asia Pacific US$1.75 trillion in economic losses," *Microsoft Asia News Center*, (May 18, 2018).
32 Smith and Lostri, "The Hidden Costs of Cybercrime."
33 "Asia's Cybersecurity Attack Rates Surpass Global Trend – Study," *Wealth Briefing Asia*, (September 17, 2020).
34 Bureau of East Asian and Pacific Affairs, Fact Sheet, US Department of State, (September 13, 2017).
35 Taiwan and Japan have been negotiating a mutual legal assistance agreement since as early as 2008.
36 United States Central Intelligence Agency, "East Asia/Southeast Asia: Taiwan," in *The World Factbook 2021*, (Washington, DC: Central Intelligence Agency, 2021), https://www.cia.gov/the-world-factbook/countries/taiwan/#people-and-society.
37 US Central Intelligence Agency, "East Asia/Southeast Asia: Taiwan," in *The World Factbook 2021*.
38 "Taiwan not eligible to join Interpol: mainland spokesperson," *China Daily*, (October 16, 2019).
39 Kelvin Chen, "Taiwan still pursuing INTERPOL membership," *Taiwan News*, (August 19, 2021).
40 A recent and legally significant case to exemplify the difficulties posed by the lack of cross-Strait law enforcement cooperation is the murder of Poon Hiu-wing, a Hong Kong native that travelled to Taiwan with her boyfriend and never returned. The perpetrator, Chan Tong-kai, had to be subsequently brought back to Hong Kong following his arrest and could not be tried for the murder, as it took place in Taiwan. The case became the basis for a newly-proposed extradition law which would allow Hong Kong to transfer criminal suspects to Taiwan and, more contentiously, China. What was intended to be an under-the-table attempt to bring PRC law to Hong Kong soon became reason for historic protest, perhaps the largest and most violent in Hong Kong history. As such, the lack of proper MLAAs between Taiwan and China have created a vacuum in which politically-motivated legal decisions have stood in the way of criminal justice. See: Daniel Victor and Tiffany May, "The Murder Case That Lit the Fuse in Hong Kong," *The New York Times*, (June 15, 2019).
41 Rick Waters, "UN Resolution 2758 Turns 50: Implications for Taiwan" (online seminar, German Marshall Fund, October 21, 2021).
42 Matthew Strong, "Suspect in murder of Taiwan in-laws arrested in Iraq," *Taiwan News,* (August 31, 2019).
43 Rick Waters, "UN Resolution 2758 Turns 50: Implications for Taiwan."
44 Bonnie S. Glaser, Matthew P. Funaiole and Emily Jin, "Unpacking Tsai Ing-wen's New Southbound Policy," *The Diplomat*, (April 1, 2017).
45 Ibid.
46 Taiwan Ministry of Labor, "Foreign Workers in Productive Industries and Social Welfare by Nationality" (data table), October 19, 2021, https://statdb.mol.gov.tw/html/mon/c12030.htm.
47 Huang Hsin-po and Jason Pan, "'New residents' coalition launched," *Taipei Times*, (November 21, 2020).
48 Renee Salmonsen, "Second-generation immigrant students are 1-% of Taiwan's 1st-9th graders," *Taiwan News*, (June 4, 2018).
49 Glaser, Funaiole and Jin, "Unpacking Tsai Ing-wen's New Southbound Policy."
50 US Department of State, Bureau for International Narcotics and Law Enforcement Affairs, International Narcotics Control Strategy Report Vol 1, March 2010.
51 劉致昕, 柯皓翔 and 許家瑜 (Liu Zhi-xin, Ke Hao-xiang and Xu Jia-yu), "The Content Mill Empire Behind Online Disinformation in Taiwan, *The Reporter*, (December 15, 2019).
52 Roderic Broadhurst and Lennon Y.C. Chang, "Cybercrime in Asia: Trends and Challenges," in *Handbook of Asian Criminology*, (February 2, 2012).

53 Michael a. Weber, Katarina C. O'Reagan, Liana W. Rosen, "The State Department's Trafficking in Persons Report: Scope, Aid Restrictions, and Methodology," Congressional Research Service, October 30, 2019.
54 Mark Merueñas, "The many times the Mutual Legal Assistance Treaty aided PHL," *GMA News Online*, (April 30, 2015).
55 Dharel Placido, "PH probes plan of businessman flagged by Taiwan," *ABS CBN News*, (August 24, 2017).
56 "Philippines' Duterte wants U.S. help in fighting drugs, blames triads," *Reuters*, (September 26, 2017).
57 Taiwan International Patent & Law Office, "Taiwan and Vietnam Planning to Enter into Mutual Legal Assistance Agreement" (press release), April 2008.
58 Huynh Tam Sang, "Boosting Taiwan's Vietnam Policy," *Taipei Times,* (July 28, 2021).
59 Taiwan-US: Signed in 2002, Taiwan-Philippines: Signed in 2013, Taiwan-Vietnam: Signed in 2011: Leaf Chiang and Lillian Wu, "Taiwan, U.S. work closely on mutual legal assistance: minister," *Focus Taiwan*, (June 18, 2013). For US data: Rush and Kephart, "Lifting the Veil on the MLAT Process: A Guide to Understanding and Responding to MLA Requests." Data is current as of June 30, 2019: Taiwan Ministry of Justice, "國際司法互助案件數統計 (Statistics of International Mutual Legal Assistance Cases" (data table), June 30, 2019, https://www.moj.gov.tw/Public/Files/201907/62819071016023862a.pdf.
60 Taiwan Ministry of Justice, "Taiwan-US mutual legal assistance: Taipei District Prosecutors Office seized more than US$ 15 million illegal income of drug trafficking in an Taiwan Bank account on behalf of the US" (press release), November 28, 2014.
61 "Global Cooperation and Training Framework (GCTF) Programs," American Institute in Taiwan, accessed November 12, 2021, https://www.ait.org.tw/our-relationship/global-cooperation-and-training-framework-programs-gctf/.
62 American Institute in Taiwan, "Remarks by AIT Director Brent Christensen at GCTF International Workshop on Anti-Corruption" (official text), March 26, 2019.
63 American Institute in Taiwan, "AIT Director Christensen gives remarks at GCTF's Transnational Crime and Forensic Science Workshop [Video]" (press release), August 14, 2018.
64 American Institute in Taiwan, "Remarks by AIT Director Brent Christensen at GCTF International Workshop on Anti-Corruption" (official text), March 26, 2019.
65 "Global Cooperation and Training Framework (GCTF) Programs: Workshop on Trade Secrets Protection and Digital Piracy Prevention (October 15-15, 2020)," American Institute in Taiwan, accessed November 12, 2021, https://www.ait.org.tw/our-relationship/global-cooperation-and-training-framework-programs-gctf/.
66 "Global Cooperation and Training Framework (GCTF) Programs: Combatting COVID-19 related Crimes (October 28, 2020)," American Institute in Taiwan, accessed November 12, 2021, https://www.ait.org.tw/our-relationship/global-cooperation-and-training-framework-programs-gctf/.
67 Bethany Allen-Ebrahimian, "Report: Beijing flooded Taiwan with coronavirus disinformation," *Axios*, May 24, 2021.
68 The American Institute in Taiwan, "The U.S., Taiwan, and Japan Co-host Virtual GCTF Workshop on Combating Cybercrime through International Law Enforcement Collaboration" (press release), October 6, 2021.
69 Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age," Harvard Law School National Security Journal, (January 28, 2015).
70 US Department of Justice, "Mutual Legal Assistance Treaty Process Reform: $24.1 Million in Total Funding," Fiscal Year 2015 Budget Fact Sheet, March 3, 2014.
71 "The CLOUD Act," Electronic Privacy Information Center (blog), updated 2018.
72 Taiwan Ministry of Justice: Laws and Regulations Database, "AGREEMENT ON MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS BETWEEN THE TAIPEI ECONOMIC AND CULTURAL REPRESENTATIVE OFFICE IN THE UNITED STATES AND THE AMERICAN INSTITUTE IN TAIWAN" (official text), March 26,2002.
73 The White House, "Background Press Call on the Virtual Counter-Ransomware Initiative Meeting" (press release), October 12, 2021.
74 Lawrence Chung, "How Taiwanese police cracked NT$83 million ATM heist," *South China Morning Post*, (August 6, 2016).

About the Authors

Russell Hsiao is the executive director of GTI, senior fellow at The Jamestown Foundation, and adjunct fellow at Pacific Forum. He is a former Penn Kemble fellow at the National Endowment for Democracy and visiting scholar at the University of Tokyo's Institute for Advanced Studies on Asia. He previously served as a senior research fellow at The Project 2049 Institute and national security fellow at the Foundation for Defense of Democracies. Prior to those positions he was the editor of *China Brief* at The Jamestown Foundation from October 2007- to July 2011 and a special associate in the International Cooperation Department at the Taiwan Foundation for Democracy. While in law school, he clerked within the Office of the Chairman at the Federal Communications Commission and the Interagency Trade Enforcement Center at the Office of the U.S. Trade Representative. Mr. Hsiao received his J.D. and certificate from the Law and Technology Institute at the Catholic University of America's Columbus School of Law where he served as the editor-in-chief of the *Catholic University's Journal of Law and Technology.* He received a B.A. in international studies from the American University's School of International Service and the University Honors Program.

Zoë Weaver-Lee is a program assistant at the Global Taiwan Institute. She graduated from Stetson University in 2019 with a Bachelor's Degree in Global Development and minors in Political Science and Asian Studies. During her time at Stetson, she spent two semesters in South Korea and Taiwan, after which she was awarded the Maris Prize for Undergraduate Research for her study regarding Taiwanese democratic development. Since her graduation, Zoë received the Huayu Enrichment Scholarship to study Mandarin in Taipei and has since returned to continue her research journey at GTI.

About GTI

GTI is a 501(c)(3) non-profit policy incubator dedicated to insightful, cutting-edge, and inclusive research on policy issues regarding Taiwan and the world. Our mission is to enhance the relationship between Taiwan and other countries, especially the United States, through policy research and programs that promote better public understanding about Taiwan and its people.

Acknowledgements

The views expressed in this paper are the authors' own and do not necessarily represent the positions of the Global Taiwan Institute. The author would like to thank Stephanie Adams, Marzia Borsoi-Kelly, Jack Liu, Margaux Garcia, and Jimmy Zhang for their thoughtful reviews of an earlier draft of the paper. An earlier version of this paper was presented at a conference in Taipei in 2017 hosted by Taiwan's Ministry of Justice Investigation Bureau.

Cover Photo Source: Shutterbean and Antonio Batinić.