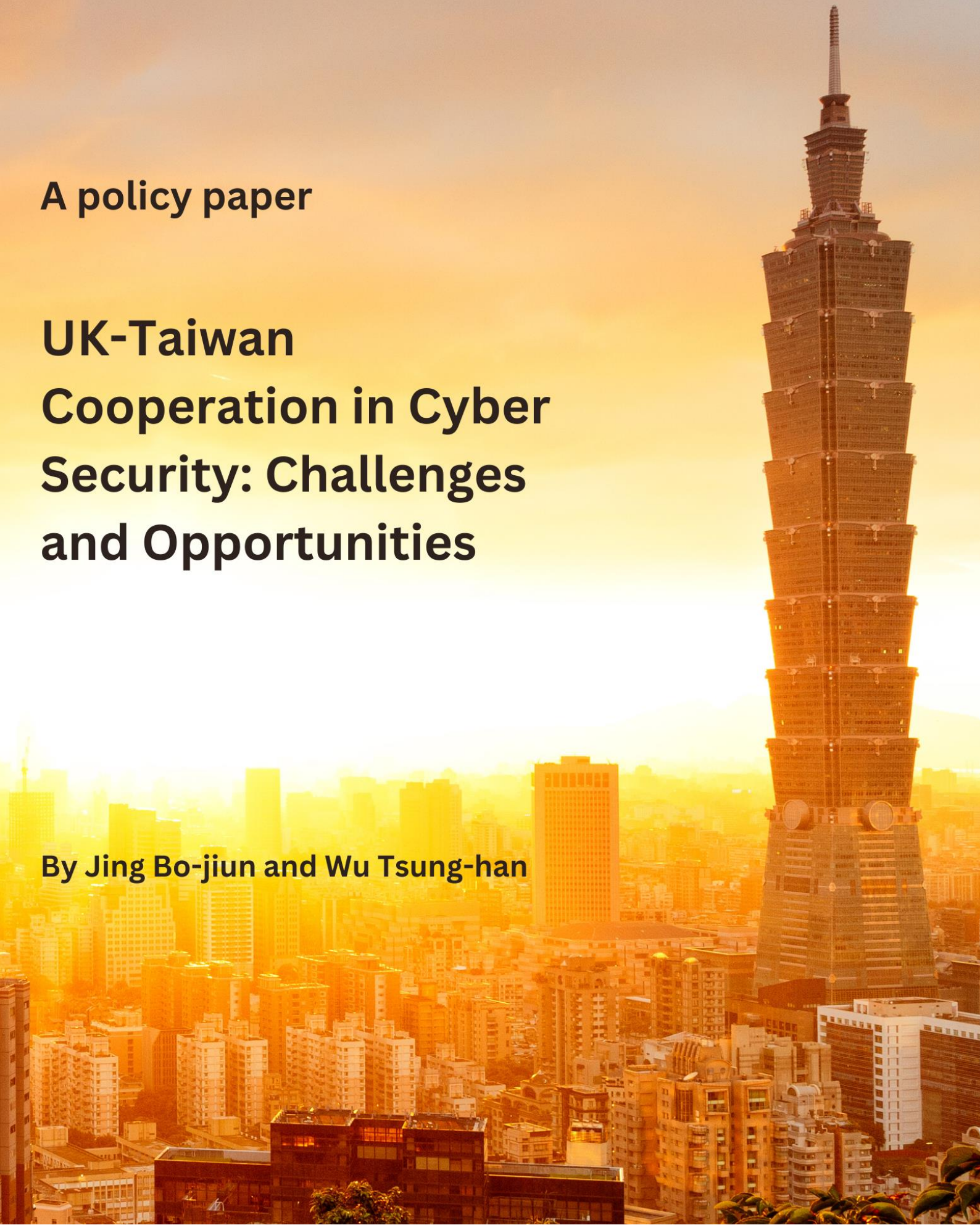
University of Nottingham
Taiwan Research Hub

A policy paper

# UK-Taiwan Cooperation in Cyber Security: Challenges and Opportunities



By Jing Bo-jiun and Wu Tsung-han

University of Nottingham
UK | CHINA | MALAYSIA

# UK-Taiwan Cooperation in Cyber Security: Challenges and Opportunities

*Jing Bo-jiun and Wu Tsung-han*

## Summary

Emerging technologies such as accelerated computing, artificial intelligence (AI), and the Internet of Things (IoT) have advanced rapidly in recent years, enhancing economic efficiency and convenience. However, their widespread adoption also introduces significant cyber security risks. While the UK and Taiwan have embraced AI and IoT, the interconnected nature and vast data proliferation of these technologies increase the potential for major cyber incidents. Furthermore, the growing threat of state-sponsored cyberattacks and espionage underscores the need for cooperation among like-minded states.

The UK and Taiwan have both made cyber security a top national security priority in response to growing digital threats. In 2021, the UK released its National Cyber Strategy 2022, reinforcing its goal to become a leading democratic cyber power. That same year, Taiwan published its second National Cyber Security Strategy Report, outlining its vision of building a resilient and trustworthy smart nation. Both countries had already developed comprehensive cyber strategies and roadmaps, focusing on strengthening cyber security frameworks and engaging the private sector in a whole-of-society approach.

This research examines UK and Taiwan cyber security strategies, assessing shared challenges and exploring opportunities for bilateral and multilateral cooperation to mitigate cyber risks and enhance resilience. The following policy recommendations are proposed:

- Given their shared democratic values and leadership in advanced technology, the UK and Taiwan should strengthen their cyber security frameworks through continuous policy development, implementation, and collaborative exchange.

- As both nations are top targets of nation-state threat activities and cyber criminals and given the rise of AI-enabled cyber capabilities among malicious actors, the UK and Taiwan should cooperate in talent development and implement measures to counter evolving cyber threats.

- UK-Taiwan cyber security cooperation should be further reinforced through satellite services, intergovernmental agreements, and multilateral platforms, ensuring a more resilient and secure digital landscape.

### Taiwan's Cyber Security Strategy

Taiwan's first National Cyber Security Strategy Report, titled 'Cyber Security is National Security,' was introduced in September 2018 by the National Security Council (NSC) under the Tsai Ing-wen administration.[1] Along with the Executive Yuan's National Cyber Security Programme (2017-2020), known as Phase 5, it shaped Tsai's cyber security strategy, aiming to build a safe and reliable digital nation.[2]

Tsai's cyber security strategy was built on a framework evolving since January 2001, when President Chen Shui-bian approved the Mechanism Programme of Security in Establishing National Information and Communication Infrastructure (2001-2004), or Phase 1. This initiative led to the creation of the National Information and Communication Security Taskforce

(NICST) under the Executive Yuan, a centralised interagency body overseeing cyber security governance. That same year, the National Centre for Cyber Security Technology (NCCST) was established to support NICST. [3] This framework continued under subsequent administrations, with one additional phase under Chen and two under President Ma Ying-jeou.[4] Major achievements included the creation of the National Security Operations Centre (N-SOC), the enactment of the Personal Data Protection Act (2012), and the formation of the Government Information Sharing and Analysis Centre (G-ISAC).[5]

During Tsai's first term, Phase 5 focused on strengthening legal and organisational structures. The Cyber Security Management Act, enacted in January 2019, empowered the Executive Yuan to enforce risk assessments, incident disclosures, and emergency response protocols for government agencies, affiliated enterprises, foundations, and critical infrastructure providers. Additionally, amendments to the National Security Act in June 2019 recognised cyberspace as part of Taiwan's defensible territory, establishing a legal basis for government and military cyber defence.[6]

Organisationally, Tsai upgraded the NICST's ad-hoc secretariat into the institutionalised Department of Cyber Security (DCS). She also established the National Communications and Cyber Security Centre (NCCSC) under the National Communications Commission (NCC) to protect critical infrastructure and enhance international cooperation. These reforms transformed Taiwan's cyber security regime into an 'Iron Triad' comprising the NSC, the DCS, and the NCCSC. On the military front, Tsai launched the Information, Communication, and Electronic Force Command (ICEF) in June 2017, creating the fourth branch of the Republic of China Armed Forces.[7]

During Tsai's second term, her administration released the 'Cyber Security is National Security 2.0' report in September 2021, aiming to build a 'resilient, secure, and trustworthy smart nation.'[8] In February 2021, the National Cyber Security Programme was renewed as Phase 6 (2021-2024).[9] In December 2022, the Ministry of Digital Affairs (MODA) was established, with the DCS transforming into the Administration for Cyber Security (ACS) under MODA. In January 2023, the NCCST was upgraded to the National Institute of Cyber Security (NICS). Under this structure, MODA sets national cyber security policy, ACS implements it, and NICS advises on R&D and talent development.

With MODA's creation, the Tsai administration expanded the 'Iron Triad' into a 'Six-pack' system, a Mandarin pun referring to a six-agency joint defence network comprising the NSC, National Security Bureau, ICEF, the Ministry of Justice's Investigation Bureau, the Ministry of the Interior's Criminal Investigation Bureau, and MODA. Meanwhile, the NCCSC continues to oversee critical infrastructure cyber security.

Since taking office in May 2024, the Lai Ching-te administration has been formulating the Phase 7 programme, set to launch in 2025. It will focus on public-private cooperation to enhance Taiwan's cyber security industry and strengthen cyber security resilience in critical infrastructure and society.[10]

## UK's Cyber Security Approach

In November 2011, the UK government under David Cameron published its first Cyber Security Strategy, titled 'Protecting and Promoting the UK in a Digital World'. It envisioned a secure and resilient cyberspace, driving economic and social prosperity while upholding key principles like liberty and fairness by 2015. [11] The subsequent National Cyber Security Programme (2011-2016) saw the establishment of the Centre for Cyber Assessment (CCA)

within GCHQ, the launch of CERT-UK for incident management, the creation of the National Cyber Crime Unit, and the operationalisation of the Joint Forces Cyber Group.[12]

In November 2016, Theresa May's government published the National Cyber Security Strategy 2016-2021, envisioning a 'secure and resilient UK, prosperous and confident in the digital world' by 2021. Centred on the 'defend, deter, and develop' objectives, the strategy aimed to protect against cyber threats, disrupt hostile actions, and expand the cyber security workforce. A key priority was strengthening the newly launched National Cyber Security Centre (NCSC), formed in October 2016 by merging CERT-UK, the CCA, the Centre for the Protection of National Infrastructure's (CNPI) cyber functions, and the Communications-Electronics Security Group (CESG) of GCHQ. The NCSC streamlined government operations, providing a unified source of cyber intelligence and national response.[13]

The 2016-2021 strategy also emphasised Active Cyber Defence (ACD), a proactive approach to strengthening networks and systems against cyber threats. In commercial settings, ACD involves identifying risks and implementing defensive measures, such as minimising phishing attacks and filtering malicious IP addresses. The UK government adopted this approach nationwide, leveraging its expertise to bolster cyber security resilience.[14] Building on this principle, the government established the National Cyber Force (NCF) in 2020, a defence and intelligence partnership aimed at disrupting, denying, degrading, and contesting cyber threats. The NCF enhances the UK's offensive cyber capabilities to safeguard national security and protect its allies.[15]

From this foundation, the UK government under Boris Johnson launched the National Cyber Strategy 2022, aiming to maintain the UK as a leading, responsible, and democratic cyber power by 2030, capable of protecting and advancing national interests in cyberspace. Under this strategy, the NCSC remains central to defending the UK's cyber landscape. Its key responsibilities include large-scale protection through digital services like ACD, managing major cyber incidents, and collaborating with the NCF to counter malicious cyber operations.[16]

Within this framework, the UK government introduced the Government Cyber Security Strategy 2022-2030 to ensure the resilience of core government functions, from public services to national security, while strengthening sovereignty and maintaining its position as a democratic cyber power. Key goals include hardening critical government functions against cyberattacks by 2025 and achieving full public sector resilience by 2030.[17] A central initiative is the Government Cyber Coordination Centre (GC3), a collaboration between the NCSC, the Government Security Group, and the Central Digital and Data Office. Under Prime Minister Keir Starmer, a new Cyber Security and Resilience Bill will be introduced in 2025 to regulate more digital services and supply chains, empower regulators, and mandate increased incident reporting to improve the response to cyberattacks.[18]

## Common Cyber Security Challenges Facing Taiwan and the UK

Both Taiwan and the UK recognise cyber security as a critical national security issue and have taken significant steps to strengthen their defences. Despite advancements, both governments continue to face persistent challenges in securing their digital landscapes. Two major obstacles stand out: the growing sophistication of cyber threats and the shortage of skilled cyber security professionals.

A key challenge is the increasingly sophisticated threats posed by malicious actors, from state-sponsored hackers to cybercriminals. These adversaries constantly refine their capabilities, exploiting vulnerabilities in government systems, critical infrastructure, and private enterprises.

Offensive cyber tools, such as ransomware-as-a-service (RaaS) and hacker-as-a-service (HaaS), have become commoditised, making cyberattacks more accessible and frequent.

The rise of AI-enabled cyber capabilities has further intensified this threat. AI-powered tools enable attackers to automate reconnaissance, phishing, and penetration efforts, increasing the efficiency and scale of cyber operations. As highlighted by the UK's NCSC, these advancements will likely escalate the global ransomware threat, with AI-driven attacks becoming more sophisticated and widespread.[19]

Beyond targeting government agencies and critical infrastructure, cyberattacks now extend to supply chains and personal data. According to the Microsoft Digital Defence Report 2024, Taiwan and the UK are among the most targeted nations for state-affiliated cyber operations. The UK ranks second in Europe and Central Asia, behind Ukraine, while Taiwan ranks first in South Asia, East Asia, and the Pacific, followed by South Korea. The report identifies Chinese state-backed actors as the primary perpetrators targeting Taiwan.[20] However, the anonymity of cyberspace makes attributing state-sponsored attacks highly challenging, and existing mechanisms for accountability remain inadequate.

Another major challenge is the shortage of skilled cyber security professionals. While this is a global issue, Taiwan and the UK face particularly acute challenges due to their critical roles in the global ICT and AI supply chains, which demand a larger pool of cyber security experts. In the public sector, both governments struggle with insufficient training and certification programmes, exacerbating the talent gap. Meanwhile, the private sector's higher salaries make it difficult for governments to attract and retain top talent, further weakening national cyber resilience. This shortage poses a serious risk to the security of critical public and private infrastructure, especially as both countries face the increasingly sophisticated cyber threats mentioned above.

Recognising the urgency of this issue, Taiwan and the UK have prioritised workforce development in their latest cyber security strategies. A key focus is strengthening partnerships between government, academia, and industry to expand training programmes and career pathways. In Taiwan, the NICS plays a leading role in developing cyber talent for both government and industry.[21] In the UK, the UK Cyber Security Council is responsible for establishing structured career pathways and expanding professional training.[22] Both institutions aim to create localised cyber security education and certification programmes, ensuring a steady pipeline of skilled professionals to support national and global cyber resilience.

## Opportunities for UK-Taiwan Collaboration

In recent years, UK-Taiwan digital cooperation has deepened, with more frequent interactions and higher-level engagements between public and private entities. This paper highlights three key areas for further collaboration: satellite services, intergovernmental agreements, and multilateral platforms.

### *Satellite Services*

Since 2023, Taiwan's collaboration with Eutelsat OneWeb has attracted significant attention. Formerly known as OneWeb, the company specialises in low-Earth orbit (LEO) satellites and merged with Eutelsat, a French geostationary-Earth orbit (GEO) satellite provider, in September 2023, forming the world's first GEO-LEO satellite operator.[23] Just two months after the merger, Eutelsat OneWeb signed an exclusive partnership with Taiwan's Chunghwa

Telecom, the island's largest integrated telecommunications provider.[24] This deal is expected to enhance Taiwan's digital resilience and deepen bilateral strategic ties.

Several factors drive this collaboration. First, Taiwanese manufacturers are already integrated into Eutelsat OneWeb's supply chain, producing satellite receiving terminals, ground station antennas, and communication components. As cooperation expands, European companies are increasingly interested in partnering with Taiwanese firms, particularly in R&D and semiconductor technology. Recognising Taiwan's crucial role in the global semiconductor industry – accounting for 60 per cent of mature-process chip production and over 90 per cent of advanced-process chip manufacturing – the UK has actively sought partnerships to ensure a stable semiconductor supply chain and a robust digital ecosystem.[25]

Another key driver of this cooperation is the Russia-Ukraine war, which has underscored the strategic importance of LEO satellites. Since February 2022, the battlefield has demonstrated how emerging technologies – including drones, AI, electronic warfare, and cyber warfare – are reshaping modern conflict. Before the war, Ukraine had already established multi-faceted cooperation with Western allies, including the US and UK, in intelligence sharing and cyber defence, helping to protect critical infrastructure and military bases from Russian cyberattacks. On the third day of the war, Ukraine sought assistance from SpaceX, and Starlink quickly responded, enabling the transmission of battlefield imagery and maintaining military command and control (C2) communications. The successful deployment of Starlink's LEO satellite constellation highlighted its crucial role in modern warfare.

Taiwan sees strong geopolitical parallels with Ukraine, driving efforts to enhance war preparedness and resilience. Ukraine's experience has reinforced Taiwan's need to anticipate potential invasion scenarios by the Chinese People's Liberation Army (PLA). Identifying likely combat zones and attack methods is crucial for effective defence planning. For years, Taiwan has faced China's grey zone warfare, including undersea cable disruptions.[26] In February 2023, two undersea cables connecting Taiwan's Matsu Islands were damaged by Chinese fishing vessels and freighters, severely disrupting telecom services for months. [27] These incidents have sparked discussions on the need for LEO satellites as a resilient backup system.

Despite Starlink's pivotal role in Ukraine, Taiwan has yet to partner with the programme, though the option remains open. Negotiations in 2019 stalled due to Taiwanese legal requirements and SpaceX's business policies. Taiwan mandates that telecommunications joint ventures must have at least 51 per cent Taiwanese ownership, conflicting with SpaceX's operational model. Additionally, concerns persist that Beijing could exert influence on SpaceX, given Elon Musk's business ties with China. With the threat of PLA aggression, Taiwan remains cautious about relying on a system potentially vulnerable to Chinese pressure.

As an alternative, Eutelsat OneWeb has emerged as a more suitable partner, aligning with Taiwan's security and operational preferences. In June 2023, Audrey Tang, Taiwan's former Minister of Digital Affairs, visited OneWeb's London headquarters to discuss potential collaboration on emergency satellite communications. Following the visit, Tang described the cooperation as a 'technological alliance' aimed at strengthening Taiwan's defensive capabilities.[28]

By November 2023, Eutelsat OneWeb and Chunghwa Telecom had formalised their agreement, securing LEO satellite services for Taiwan. The system was successfully tested in April 2024, enabling urgent communications after an earthquake in Hualien. By the end of 2024, Taiwan had achieved full satellite signal coverage, marking a major milestone in its digital and national security strategy.[29]

### *Intergovernmental Bilateral Agreements*

The UK and Taiwan should leverage their shared liberal democratic values to deepen economic cooperation in digital technology. Both countries possess strong ICT sectors that contribute to robust cyber security ecosystems. However, their commitment to the rule of law, intellectual property protection, and freedom of speech is equally – if not more – important in fostering trust and collaboration among stakeholders in digital innovation.

Building on this value alignment, the two governments have recently signed several agreements to enhance cooperation. In November 2022, Taiwan's Department of Industrial Technology (DoIT) under the Ministry of Economic Affairs signed a Memorandum of Understanding (MoU) with Innovate UK, part of UK Research and Innovation, during the 25th UK-Taiwan Trade Talks. This MoU aims to strengthen collaboration in applied research, experimental development, and innovation initiatives.[30] In April 2024, a new funding round commenced, with DoIT and Innovate UK jointly committing up to £5 million for projects in next-generation communication, semiconductor technology, space technology, IoT, Big Data, AI, 5G, and 6G.[31]

Further reinforcing this partnership, in November 2023, Taiwan and the UK, under the Conservative government, signed an Enhanced Trade Partnership (ETP) agreement, the UK's first ETP arrangement with another country.[32] This agreement aims to strengthen bilateral trade and investment, particularly in digital trade, by facilitating market access and addressing regulatory challenges businesses face in the digital economy. It also emphasises open markets, innovation, and regulatory cooperation to support international digital trade.

Despite some suspicions that the current Labour government's goal of forging more trade links with China could slow UK-Taiwan cooperation,[33] the UK government should not be overly concerned about the China factor nor restrict itself in strengthening economic relations with Taiwan. Given Taiwan's pivotal role in advanced technologies, such as semiconductors and AI, deeper trade and investment ties with the island could benefit the UK economy and strengthen its position in the Indo-Pacific. If the ETP succeeds in fostering two-way investment in digital technology, it could significantly advance cyber security, 5G, AI, and IoT capabilities in both Taiwan and the UK. This, in turn, would accelerate digital transformation across the public and private sectors, reinforcing the resilience and competitiveness of both economies in the global digital landscape.

### *Multilateral Platforms*

The UK and Taiwan have shown a strong commitment to multilateral cooperation in tackling cyber security challenges. In May 2024, the British Office Taipei, the American Institute in Taiwan, the Japan-Taiwan Exchange Association, the ROC Ministry of Foreign Affairs, and MODA jointly hosted an International Workshop on Resilience in Telecommunications and Cyber Security in Taipei under the Global Cooperation and Training Framework (GCTF). Several other de facto embassies, including the Australian Office Taipei, the Canadian Trade Office in Taipei, and the Netherlands Office Taipei, were also involved in organising the event. The workshop gathered 210 participants, including 43 international experts, scholars, and officials from 26 countries, to exchange insights on cyber security, telecom networks, and telecommunications resilience.[34]

The United States and Taiwan originally established the GCTF in June 2015 to leverage Taiwan's expertise in addressing global challenges. The initiative helps Indo-Pacific countries strengthen their capacity-building efforts through specialised training programmes while expanding Taiwan's multilateral cooperation in the region. Since its launch, the GCTF has

organised 76 international workshops on topics such as public health, women's empowerment, energy efficiency, e-commerce, cyber security, humanitarian assistance and disaster relief (HA/DR), and media literacy. More than 10,000 officials and experts from 133 countries have participated in these events.[35] Japan and Australia joined as full partners in 2019 and 2021, respectively.

The UK became actively involved in the GCTF in March 2021, when it co-hosted the Seminar on Building the Resilience of Nations and Communities to Disasters, marking its first direct engagement with the platform.[36] With its inaugural co-hosting role and continued participation – most recently in the 2024 cyber resilience workshop – the UK has become an integral part of the GCTF. It is expected to expand its collaboration with Taiwan in cyber security, AI, and related areas.

Outside the GCTF, the UK may find it challenging to include Taiwan in more official platforms, such as the 2023 AI Safety Summit, which was hosted by the UK and invited the EU and 27 countries, including China but not Taiwan, to discuss AI risks, resulting in the Bletchley Declaration on AI safety cooperation.[37] These diplomatic obstacles highlight the need for Taiwan to engage more actively with the UK through the GCTF. Likewise, the UK should consider becoming a full partner in the GCTF, which would further facilitate collaboration in cyber security, AI, and other strategic fields.

## Towards a Secure and Resilient Digital Future

Given their shared democratic values and technological strengths, the UK and Taiwan should deepen cooperation in digital resilience to address evolving cyber security challenges. This paper outlines key policy recommendations for enhanced collaboration.

First, the UK and Taiwan should strengthen intergovernmental communication and protect critical digital infrastructure. Leveraging bilateral and multilateral frameworks, such as the GCTF, can promote democratic cyber governance and enhance regional cyber security cooperation. Additionally, advancing digital resilience, particularly through Eutelsat OneWeb, can counter cyber threats from authoritarian regimes.

Second, joint research, technological innovation, and best practice sharing between governments, private sectors, and academia should be encouraged, particularly in next-generation communication and AI. Both nations should also invest in digital trade, industrial resilience, and supply chain security to build a robust digital ecosystem.

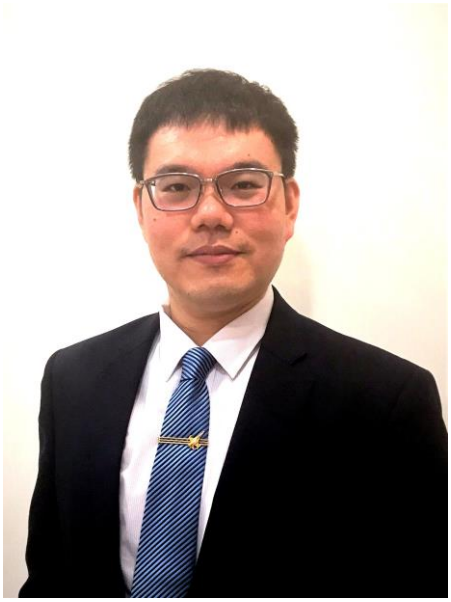
By expanding bilateral and multilateral cooperation, the UK and Taiwan can set a global precedent for cyber security partnerships in the Indo-Pacific, contributing to a more secure, stable, and resilient global cyber environment.

[1] National Security Council, ROC (Taiwan) (2018) *National Cybersecurity Strategy Report: Cyber Security is National Security*. https://www.president.gov.tw/Page/317/969
[2] Executive Yuan (2017) *National Cyber Security Program of Taiwan (2017-2020)*. https://www-api.moda.gov.tw/File/Get/acs/zh-tw/cYa9VkznxWRvmqR
[3] Executive Yuan (2002) *Mechanism Programme of Security in Establishing National Information and Communication Infrastructure (2001-2004)*. https://www-api.moda.gov.tw/File/Get/acs/zh-tw/YOHpUbnYmdF1fLZ
[4] Executive Yuan (2007) *Mechanism Programme of Security in Establishing National Information and Communication Infrastructure (2005-2008)*. https://www-api.moda.gov.tw/File/Get/acs/zh-tw/DNd72Azm6BVQaBE; Executive Yuan (2009) *National Information and Communication Security Development Programme (2009-2012)*. https://www-api.moda.gov.tw/File/Get/acs/zh-tw/lWZxf7FlHmlMBSh; and Executive Yuan (2016) *National Information and Communication Security Development Program (2013-2016)*. https://www-api.moda.gov.tw/File/Get/acs/zh-tw/nqiFsvrRUB3WWkX
[5] Jing, B. (2019) 'Cyber Security as a Sine Qua Non of Digital Economy: Turning Taiwan into a Reliable Digital Nation?', in Tatsumi, Y., Kennedy, P. and Li, J. (eds.) *Taiwan Security Brief: Disinformation, Cybersecurity, & Energy Challenges*. Washington, DC: Stimson Center, pp. 23-35.
[6] Ministry of Justice, ROC (Taiwan) (2022) *National Security Act*. https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030028
[7] Jing, B. (2021) 'Cybersecurity is National Security: Can Taiwan Have the Digital Cake and Eat it Too?', *Chinese (Taiwan) Yearbook of International Law and Affairs*, 38, pp. 120-137.
[8] National Security Council, ROC (Taiwan) (2021) *National Cyber Security Strategy Report: Cyber Security is National Security 2.0*.
[9] Executive Yuan (2023) *National Cyber Security Program of Taiwan (2021-2024)*. https://www-api.moda.gov.tw/File/Get/acs/zh-tw/x9U2Gtwj3y8EaXF
[10] Su. S. (2025) 'ACS Director-General Tsai Fu-longe Proposes Four Major Strategies to Strengthen Taiwan's Cyber Security Industry', *CNA*, 18 February. https://www.cna.com.tw/news/afe/202502180344.aspx
[11] HM Government (2011) *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf
[12] HM Government (2016) *The UK Cyber Security Strategy 2011-2016: Annual Report*. https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report
[13] HM Government (2016) *National Cyber Security Strategy 2016-2021*. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
[14] National Cyber Security Centre (NCSC) (2025) *Active Cyber Defence*. https://www.ncsc.gov.uk/section/active-cyber-defence/introduction
[15] National Cyber Force (NCF) (2021) *National Cyber Force Explainer*. https://assets.publishing.service.gov.uk/media/61b9f526d3bf7f05522e302e/Force_Explainer_20211213_FINAL__1_.pdf
[16] HM Government (2021) *National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK*. https://www.gov.uk/government/publications/national-cyber-strategy-2022
[17] HM Government (2022) *Government Cyber Security Strategy 2022-2030: Building a Cyber Resilient Public Sector*. https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030
[18] HM Government (2024) *Cyber Security and Resilience Bill*. https://www.gov.uk/government/collections/cyber-security-and-resilience-bill#when-will-the-bill-happen
[19] National Cyber Security Centre (NCSC) (2024) *The Near-term Impact of AI on the Cyber Threat*. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat
[20] Microsoft (2024) *Microsoft Digital Defense Report 2024*. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024
[21] National Institute of Cyber Security (NICS) (2024) *Scope of operation*. https://www.nics.nat.gov.tw/en/about/scope_of_operation/
[22] UK Cyber Security Council (2022) *Chartering a Cyber Future Strategy 2025*. https://www.ukcybersecuritycouncil.org.uk/news/news/chartering-a-cyber-future-strategy-2025/
[23] Browne, R. and Sheetz, M. (2023) 'Eutelsat and OneWeb Combine to Create European Satellite Giant as Musk's Starlink Pressures Sector', *CNBC*, 28 September. https://www.cnbc.com/2023/09/28/eutelsat-oneweb-merge-to-create-satellite-challenger-to-musks-starlink.html

[24] Chunghwa Telecom (2023) 'Chunghwa Telecom Selects Eutelsat OneWeb for Low Earth Orbit (LEO) Satellite Services', *Chunghwa Telecom*, 15 November. https://www.cht.com.tw/en/home/cht/messages/2023/1115-1530
[25] Jing, B., Lucenti, F., Sciorati, G., Luo, W. and Jie, Y. (2022) 'Taiwan Holds All the Chips in US-China Tech Showdown', *East Asia Forum*, 3 December. https://eastasiaforum.org/2022/12/03/taiwan-holds-all-the-chips-in-us-china-tech-showdown/
[26] Hinrix, F. (2024) 'Building Resilience in Taiwan's Internet Infrastructure from Geopolitical Threats', *The Henry M. Jackson School of International Studies*, 21 May. https://jsis.washington.edu/news/building-resilience-in-taiwans-internet-infrastructure-from-geopolitical-threats/
[27] Wu, H. and Lai, J. (2023) 'Taiwan Suspects Chinese Ships Cut Islands' Internet Cables', *AP News*, 8 April. https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70; Braw, E. (2023) 'China is Practicing How to Sever Taiwan's Internet', *Foreign Policy*, 21 February. https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/
[28] Su, S. (2023) 'Audrey Tang Visits the UK's Department for Science, Innovation and Technology to Exchange Views on Digital Signatures and Cloud Policy', *CNA*, 16 June. https://www.cna.com.tw/news/afe/202306160029.aspx
[29] Hsieh, A. (2024) 'Taiwan Showcases Satcom Prowess amidst Earthquake Crisis', *DigiTimes Asia*, 9 April. https://www.digitimes.com/news/a20240409PD202/communications-satellite-leo-satellite-network-communications-oneweb-satellite-communications.html; Shan, S. (2024) 'Satellites Touted in Quake Response', *Taipei Times*, 11 April. https://www.taipeitimes.com/News/taiwan/archives/2024/04/11/2003816266
[30] Ministry of Economic Affairs, ROC (Taiwan) (2022) 'The 25th UK-Taiwan Trade Talks Deepen Bilateral Economic Partnership', *Ministry of Economic Affairs*, 9 December. https://www.trade.gov.tw/Search2/Content.aspx?did=263193
[31] HM Government (2024) 'UK-Taiwan CRD 2024'. https://apply-for-innovation-funding.service.gov.uk/competition/1877/overview/ef8c4c48-2004-4a56-bc07-db349448bca4#summary.
[32] Chau, T. (2024) 'U.K. Making Constant Effort to Include Taiwan Globally: Departing Envoy', *Nikkei Asia*. https://asia.nikkei.com/Editor-s-Picks/Interview/U.K.-making-constant-effort-to-include-Taiwan-globally-departing-envoy
[33] Sergeant, G. (2024) 'Why is Labour So Scared to Talk about Taiwan?', *The Spectator*, 26 November. https://www.spectator.co.uk/article/why-is-labour-so-scared-to-talk-about-taiwan/
[34] American Institute in Taiwan (AIT) (2024) '2024 GCTF International Workshop on Resilience in Telecommunications and Cybersecurity', *AIT*, 4 June. https://www.ait.org.tw/2024-gctf-international-workshop-on-resilience-in-telecommunications-and-cybersecurity/
[35] GCTF (2025) *Mission*. https://www.gctf.tw/en/IdeaPurpose.htm
[36] GCTF (2021) 'Remarks by MOFA Minister Jaushieh Joseph Wu for GCTF Seminar on Building the Resilience of Nations and Communities to Disasters', *GCTF*, 10 March. https://www.gctf.tw/en/issues_detail28_0.htm
[37] HM Government (2023) *The Bletchley Declaration by Countries Attending the AI Safety Summit 2023*. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attendin

## About the Authors

Dr Jing Bo-jiun is a Senior Research Fellow in Taiwan Studies at the Oxford School of Global and Area Studies (OSGA), University of Oxford. His research and publications primarily focus on Taiwan-Southeast Asia relations, Taiwan's cybersecurity strategy, and the international relations of the Indo-Pacific region. Dr Jing is the author of the monograph Taiwan and Southeast Asia: Opportunities and Constraints of Continued Engagement (University of Maryland School of Law, 2016). He holds a PhD in International Political Economy from King's College London. Previously, he served as Head of the Taiwan Studies Project and as a Research Fellow at the Institute for Security and Development Policy (ISDP) in Sweden, 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.



Dr Wu Tsung-han is an Assistant Research Fellow at the Institute for National Defence and Security Research (INDSR) in Taiwan. His research interests focus on Chinese politics, cross-Strait relations, nationalism, cognitive warfare, and cybersecurity. Since the outbreak of the Russia-Ukraine war, he has co-hosted a project analysing the conflict's progression, extracting insights relevant to Taiwan's defence strategies, and examining the cooperation between Russia and the PRC. Dr Wu holds a PhD in Chinese Studies from the Lau China Institute, King's College London. Previously, he worked as a research project assistant in the Department of East Asian Studies at the University of Cambridge and served as the External Secretary for the British Postgraduate Network for Chinese Studies (BPCS). He has also been involved with Pushkin House in London and has served as a facilitator for the UK Parliament.