Towards open and secure digital connectivity

Europe's and Taiwan's paths after the world's first digital pandemic

Brigitte Dekker
Xiaoxue Martin
Maaike Okano-Heijmans

Clingendael Report

Clingendael
Netherlands Institute of International Relations

Clingendael

Netherlands Institute of International Relations

Towards open and secure digital connectivity

Europe's and Taiwan's paths after the world's first digital pandemic

Brigitte Dekker
Xiaoxue Martin
Maaike Okano-Heijmans

Clingendael Report
April 2021

April 2021

About the authors

Brigitte Dekker is a Junior Researcher at the Netherlands Institute of International Relations 'Clingendael' in The Hague. Her research focuses on various dimensions of EU–Asia relations, with a specific interest in South-East Asia and China. Her research revolves around the nexus between trade, technology and geopolitics.

Xiaoxue Martin is a Junior Researcher at the Clingendael China Centre and the EU & Global Affairs Unit. Her work focuses on the contemporary politics and international relations of Greater China, in particular Hong Kong and Taiwan affairs, and China's relations with the US and the EU.

Maaike Okano-Heijmans is a Senior Research Fellow at the Netherlands Institute of International Relations 'Clingendael' in The Hague and a visiting lecturer at the University of Leiden. Her main research interests are in connectivity, economic diplomacy and international relations in EU-Asia relations, with a special focus on China and Japan.

The Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Follow us on social media
@clingendaelorg
The Clingendael Institute
The Clingendael Institute

Email: info@clingendael.org
Website: www.clingendael.org

Contents

Executive summary

Surveillance capitalism and digital authoritarianism have become facts of life in recent years. Set against the US–China trade–tech–data standoff, the European Union (EU) and its member states are navigating their course of open strategic autonomy, assessing how to position themselves in the digital age. Synergies and coordination with like-minded partners – including the United States (US) and countries in the Indo-Pacific – seem inevitable.

This raises the question of to what extent Taiwan can be a partner for closer cooperation on digital matters. Can the EU, and specifically the Netherlands, and Taiwan move beyond diverging priorities, and **promote a human-centred approach to the digital domain by leveraging their economic, scientific and cultural ties**?

In answering this question, this Clingendael Report examines the approaches of both sides to strengthening resilient societies, so-called 'Big Tech' regulation and digital development assistance. Findings suggest that while the underlying strategic interests and goals of Taiwan and Europe on digital connectivity align, priorities and strengths diverge. China's growing influence and assertive behaviour pose a substantial challenge to both sides' open, inclusive democracies, economic competitiveness and standard-setting power. As Europe and Taiwan improve policies domestically, as well as in and with third countries, especially in the Indo-Pacific region, they can benefit from each other's **complementary skills in specific digitalisation and digital connectivity domains**.

In recent years, the Taiwanese government made great efforts to create a **digital democracy and resilient society** and to engage citizens actively in such processes through digital means. This is a product of Taiwan's recent history and the tumultuous cross-strait relationship. The g0v movement stands out as a leaderless hacker collective that works with and for the government to promote the transparency of government information. It is committed to developing information platforms and tools for citizens to participate in society, blending technology and hackerdom with politics to create a new form of decision-making. The EU and its member states can benefit from Taiwan's experience by exchanging best practices on e-government, blending technology and politics, and insourcing the experts needed to guide governments through their digital transformation.

Regarding **Big Tech regulation**, the priorities and approaches of the EU and Taiwan diverge, but their ultimate objectives align, as both share a human-centred focus and hold national security concerns at the core. The Netherlands, EU and Taiwan could

benefit from mutual exchanges, with Taiwan having experience and a proven track record in countering disinformation, while the EU has been a front-runner of Big Tech regulation and privacy protection through its data regulation. Enhanced awareness among Taiwanese companies and citizens about the collective benefits of regulation in the digital field can promote understanding and address companies' concerns that EU regulations hinder their business in Europe.

In addition to improving digitalisation efforts at home and acting jointly on digital governance, **digital Official Development Assistance** (ODA) is emerging as an instrument for Taiwan and European countries to improve digital connectivity in and with third countries. Taiwanese efforts include e-health initiatives in East and Southeast Asia, while Dutch efforts focus on cybersecurity and primarily target African countries. More coordinated action in these fields may inspire efforts in other domains as well. Ultimately, it will help deliver inclusive and sustainable growth in the Indo-Pacific region, while also serving the economic and strategic interests of Taiwan and Europe – that is, economic competitiveness, secure connectivity, and an open and inclusive digital domain.

1 Introduction

The COVID-19 pandemic has amplified the trend towards digitalisation of our societies, as well as efforts to improve the rules, standards and policies that shape these changes. For Europe and Taiwan, as like-minded partners, economic competitiveness, secure connectivity, and an open and inclusive digital domain are central in these efforts.

Digital instruments vastly improve global connections and are an important tool for development. Ensuring that they uphold rather than undermine our democracies remains a challenge, however. Countries like China, Cambodia and Myanmar are turning towards digital instruments to implement widespread digital surveillance and firewalls in an attempt to control the internet.[1] Yet the challenge goes beyond digital authoritarianism, as evidenced by the January 2021 riots on Washington DC's Capitol Hill. Both the riots, as such, and the subsequent regulatory actions by US so-called 'Big Tech' companies – including banning then US President Trump from Twitter and expelling right-wing social-networking service Parler from the Apple App Store and Google Play Store – brought home the undue power of influence and regulation of Big Tech over democratic societies.

Confronted with these challenges and each equipped with strengths of their own, Taiwan and the European Union (EU) and its member states – including the Netherlands – stand to benefit from mutual learning and greater coordination on digital policies at home and abroad – that is, digital connectivity. This requires improved mutual understanding of each other's digital strategies and actions.

This Clingendael Report seeks to contribute to this aim by unveiling convergences and divergences in the domestic and foreign policies of the Netherlands, the EU and Taiwan in the digital field, and by highlighting opportunities for mutual learning and deepened coordination and cooperation between the two sides more broadly. Three domains are discussed as promising areas for collaboration: (1) creating resilient societies; (2) dealing with foreign Big Tech; and (3) engaging third countries by way of digital official development assistance (ODA), including in the e-health and cybersecurity domains.[2]

1 Mahtani, S., 2021. 'First came political crimes. Now, a digital crackdown descends on Hong Kong,' *Washington Post*, 12 January, Asia & Pacific section.

2 These three focus areas emerged from the authors' interviews with policy-makers and experts in Taiwan and Europe/the Netherlands for the purposes of this research, held between October 2020 and February 2021. Among others, the authors wish to thank representatives of the National Development Council (NDC), the Ministry of Foreign Affairs, the Department of Cyber Security of the Executive Yuan, the International Cooperation and Development Fund (ICDF), the Chung-Hua Institute for Economic Research (CIER), the Prospect Foundation and DoubleThink Lab in Taiwan; and representatives of the Ministry of Foreign Affairs, Parliament and the private sector in the Netherlands.

Each section details the interests and concerns, as well as the fundamental norms and standards underpinning Dutch and Taiwanese action. Divergences in prioritisation and approach in the three domains are discussed in order to highlight challenges to broadened coordination and cooperation. Overcoming these will be a crucial step for Taiwan and the Netherlands – and Europe, more broadly – to equip themselves better for the digital age and to strengthen the impact of their digital connectivity activities abroad.

Forging digital connectivity partnerships

The COVID-19 pandemic aroused agitation on a global scale and is considered the first digital pandemic,[3] both in its origin – as the Chinese government's restrictions on the digital dissemination of information created momentum for the virus to spread unnoticed – and in its effect. Governments are resorting to digital instruments to combat the virus and populations are more active in the digital sphere than ever because of widespread lockdowns. These responses and shifts call attention to the need for improved, multilateral action on challenges of digital sovereignty and digital rights. The EU and its member states (henceforward, Europe) – and the Netherlands specifically – have much to gain from closer cooperation with countries that share their interests in the digital sphere. When it comes to digital authoritarianism,[4] referring to governments' use of digital tools including the internet to increase social and political control and/or undermine civil liberties, European governments tend to look at India, Japan, Singapore, South Korea and the United States as partners with shared concerns.[5] Often overlooked, Taiwan also stands out as a promising like-minded partner for closer cooperation on digital matters, as this Clingendael Report will demonstrate.

Both Taiwan and Europe adhere to a human-centred approach that puts users first and emphasises data privacy and digital rights. This contrasts with the primarily business-oriented approach of the US government – which is evolving now under the Biden administration – and with the state-security focus of the Chinese Communist Party and the Chinese government.

EU member states and Taiwan are repositioning themselves to increase their economic competitiveness and normative influence in the digital age, against a context of intensifying Sino–American rivalry that is profoundly reshaping the global technology

3 Okano-Heijmans, M., 2020. 'Coronavirus: the world's first digital pandemic,' The Hague, the Clingendael Institute.

4 As Erol Yayboke and Samual Brennen point out in a CSIS Brief, digital authoritarianism presents overlapping and expanding challenges: (1) within autocracies; (2) as tools to undermine adversaries; (3) via export to like-minded regimes; and (4) within and by democracies themselves.

5 Dekker, B., and Okano-Heijmans, M., 2020. 'Europe's Digital Decade? Navigating the global battle for digital supremacy,' The Hague, the Clingendael Institute.

landscape and governance. Unilaterally as well as in issue-based coalitions,[6] steps are being taken to protect consumers and strengthen democracies' investments in strategic sectors and intrusive Big Tech, and to reorganise critical supply chains – including of chips, rare earths and vaccines – to reduce reliance on China.

For the EU countries, cooperation and synergies with like-minded partners are a necessity to strengthen their leverage globally in the digital domain. In the words of Member of the European Parliament Reinhard Bütikofer[7]: 'The increasingly connected world calls for proactive action from the EU and its member states in order to enhance cooperation with its partners in the digital domain and all related fields, such as health and a green transition'.

Responses of EU member states, including the Netherlands, to digital matters specifically in the Indo-Pacific are shaped by developments in two parallel – and partly overlapping – domains: the EU–Asia Connectivity Strategy[8] of 2018; and the EU Digital Strategy[9] published in February 2020. As of March 2021, the EU and its member states are consolidating their focus on the Indo-Pacific region. France, Germany and the Netherlands have published their vision or guidelines on the Indo-Pacific region, and an overarching EU approach is expected before summer 2021. Digital connectivity will certainly feature herein, holding promises for strengthened cooperation in numerous domains.

Within the Indo-Pacific region, Taiwan has been an example of modernisation and digitalisation. The country has grown into an important partner for Dutch and other European high-tech companies, especially on semi-conductors. Taiwan aspires to continue to serve as a hub for a new generation of knowledge-based industries, products and services, but also as a service-specific hub in the cybersecurity sector. Efforts are being made to deepen ties between the US private sector and innovation hubs in Taiwan.

As the digital sphere becomes increasingly contested, more coordinated efforts by Taiwan and Europe can serve to better promote shared approaches and norms on digital connectivity. For example, greater synergies with Taiwanese action could help to improve sustainable and secure digital connectivity in the region, an objective

6 Dekker, B., and Okano-Heijmans, M., 2020. 'Dealing with China on high-tech issues: views from the US, EU and like-minded countries in a changing geopolitical landscape,' The Hague, the Clingendael Institute.

7 Committee on Foreign Affairs, rapporteur: Butikofer, R., 2020. 'Report on connectivity and EU-Asia relations (2020/2115(INI)),' European Parliament, 17 December.

8 European External Action Service, 'Connecting Europe & Asia: the EU strategy,' 2019. 26 September.

9 European Commission, 'The European Digital Strategy', 2020.

explicitly mentioned in the Indo-Pacific Guidelines[10] that the Netherlands published in December 2020.

The 2nd Taiwan–EU Dialogue on Digital Economy (DDE), which was held in December 2020, illustrates that efforts to strengthen ties and increase cooperation in the digital area are already ongoing. In the Dialogue, the two sides discussed the influence of COVID-19 on the digital and data economy, the importance of establishing public–private partnerships in the green and digital transition, and major topics such as research and technology cooperation, artificial intelligence (AI), cybersecurity certification and digital connectivity between Europe and Asia. Both sides acknowledge that the DDE can serve as a platform for cooperation on the digital economy.[11]

The exchange of information and ideas to complement each other's digital endeavours is still limited, however.[12] This could be ascribed to diverging priorities and approaches, notwithstanding commonalities in the standards and norms that underpin policies. Even if the EU and Taiwan do not align on all aspects of the digital domain, both sides acknowledge that there is much to gain from digital cooperation and knowledge exchange. As will be detailed in the following sections, opportunities for this are particularly apparent in three domains: creating resilient societies; dealing with foreign Big Tech; and supporting and steering policies in third countries by way of digital ODA.

10 The Netherlands Ministry of Foreign Affairs, 'Indo-Pacific: guidelines for strengthening Dutch and EU cooperation with partners in Asia,' 2020. 13 November.

11 National Development Council (NDC), 'The 2nd Taiwan-EU Dialogue on Digital Economy (DDE) successfully concluded,' 2020. 8 December.

12 Dekker, B., and Okano-Heijmans, M., 2020. 'In between giants: how a EU-Taiwan Partnership could ensure digital benefits for all,' *Taiwan Insight*, 29 July.

2 Resilient societies

Both the Netherlands and Taiwan have implemented domestic measures to make their systems and people more resilient and to protect citizens, businesses and the government against interference[13] from foreign states and non-state actors. They aim for resilient societies that are able to deal with non-traditional, hybrid threats that have arisen with increased digitalisation of society, such as cyber espionage and attacks, disinformation and election interference through online means.[14] More than most other countries, the Taiwanese government – in cooperation with key stakeholders – has successfully leveraged the opportunities of digital instruments to enhance e-government and societal resilience.

2.1 Taiwan's e-government

In recent years, the Taiwanese government has made great efforts to digitise democratic processes and to engage citizens actively in such processes. Today's renowned e-governance architecture is a result of these efforts, which were shaped by the desire to protect the relatively young Taiwanese democratic system. Unwanted foreign interference – largely from China – is a particular concern and led to the inclusion of an effective digital method to counter disinformation campaigns and cyberattacks from China.

Citizen engagement in political processes is a product of Taiwan's recent history. The activist Sunflower movement that emerged during spring 2014 in opposition to the Cross-Strait Service Trade Agreement (CSSTA) with China, set off a wave of political innovation and digitalisation in Taiwanese politics.[15] Taiwan's government turned to civic hackers for assistance in its efforts to bring more transparency to government decisions, as a way of addressing broadly shared concerns about Chinese influence in Taiwan's society. Interestingly, the debate in Taiwan then revolved around 4G telecommunications infrastructure – similar to current ongoing debates in European countries about 5G networks.

13 Sie Dhian Ho, M., Bruijne, de, K., Houtkamp, C., 2020. 'Zorgen over buitenlandse inmenging,' The Hague, the Clingendael Institute.

14 AIVD, MIVD, and NCTV, 'Dreigingsbeeld statelijke actoren,' 2021, 3 februari.

15 Ho, M., 2019. 'The activist legacy of Taiwan's sunflower movement,' Washington, Carnegie Endownment for International Peace.

The leaderless hacker collective g0v[16] (pronounced gov-zero, as it aims to rethink the government 'from zero') paved the way for Taiwan's 'shadow' digital democracy.[17] G0v promotes the transparency of government information and is committed to developing information platforms and tools for citizens to participate in society, blending technology and hackerdom with politics to create a new form of decision-making. In 2016, former g0v member Audrey Tang became Taiwan's first Digital Minister, demonstrating the importance that Taiwan's government attaches to digital governance.[18]

One project that aims to increase government transparency through technology is vTaiwan.[19] This platform serves as an online–offline consultation process that aims to connect a broad array of stakeholders and to organise hackathons along with the consultation process. vTaiwan has enabled so-called regulatory sandboxes – spaces where existing rules are relaxed to introduce new services and tools for the consumer market before deciding whether to amend regulations thereafter.[20] Specific sectors include autonomous vehicles, the platform economy, fintech and the 5G spectrum.[21] In Europe, sandboxes primarily focus on the fintech sector (that is, when businesses use technology to automate financial services) and are solely conducted on a national scale.[22] Connecting sandboxes, and in particular companies involved in sandboxes, could unlock opportunities to discuss synergies and convergences between projects and create awareness concerning cross-border possibilities for a project in the future.

G0v and vTaiwan may be understood as bottom–up digital instruments that help to strengthen democracy by using technology in the interest of the public good, including the engagement of citizens. Additionally, instruments to create resilient societies by exposing possible threats serve the same goal. DoubleThink Lab, for example, aims to expose disinformation from China, thereby countering digital authoritarianism.[23] Founded in 2019, this non-governmental organisation (NGO) seeks to map the online information operation mechanisms, as well as the export of surveillance technology.

16 G0V, 'Ask not why nobody is doing this, you are the nobody,' n.d.

17 Miller, C., 2020. 'How Taiwan's 'civic hackers' helped find a new way to run the country,' *The Guardian*, 27 September.

18 Generation Internet Policy Lab. 'Interview with Audrey Tang,' 2019, 28 February.

19 vTaiwan,. 'Where do we go as a society?,' n.d.

20 Open GOV, 'Expanding Taiwan's digital economy through the government's 8-year DIGI+ plan,' 2017. 27 October.

21 Generation Internet Policy Lab, 'Interview with Audrey Tang,' 2019, 28 February.

22 Parenti, R., 2020. 'Regulatory Sandboxes and Innovation Hubs for FinTech,' *European Parliament DG Internal Policies*, September.

23 Doublethink Lab, 'About Us,' 2019, September.

As such, it seeks to defend not just Taiwan's democracy, but also to assist Southeast Asian countries in doing so – an effort in which the Netherlands and Taiwan could join forces. Especially since COVID-19, Taiwan has been an important node in the transmission of Chinese-language disinformation to Southeast Asian countries.[24]

2.2 Dutch efforts towards digital democracy

Whereas Taiwanese domestic digital efforts are grounded in a firm desire to protect Taiwan's digital sovereignty and democratic processes, the Dutch government's domestic digitalisation approach seems generally driven by economic efficiency considerations. It has been left largely to the private sector – with the Dutch government primarily focused on creating an enabling environment for citizens and businesses to develop digital initiatives. This is evident from the Dutch government's 'Digitalisation Strategy' of 2018[25], the first whole-of-government approach that set out ambitions and objectives for a digital transition.[26] The strategy includes a Cybersecurity Agenda, a Digital Trust Centre to assist companies to operate safely online, an action plan for small and medium-sized companies, and a plan for digital inclusiveness.[27] The subsequent Agenda for a Digital Government[28] (NL DIGIbeter) mentions the need for far-reaching collaboration by government, academia and the private sector to protect fundamental rights and public values. It does not, however, mention the need for the Dutch government itself to invest in digital instruments and know-how.

In 2019, engagement between government and citizens was pushed higher on the agenda by the Dutch House of Representatives. A temporary Committee on the Digital Future was installed to get a firmer grip on developments in digitalisation.[29] This temporary committee concluded that the House of Representatives should establish a standing parliamentary committee for Digital Affairs, after the Dutch Parliamentary elections in March 2021. Furthermore, it recommended, among other things, that the House should draw up a digitalisation agenda and place additional focus on EU legislation and how it is shaped. Separately, a widely supported motion[30]

24 Ke, H., and Min Chen Lee, L., 2020. 'How China's infodemic spreads to Taiwan and Southeast Asia', Taipei, Doublethink Lab.

25 Government of the Netherlands, 'Nederlandse Digitaliseringsstrategie: Nederland digitaal – hier kan het. Hier gebeurt het,' 2019. June.

26 Government of the Netherlands, 'Resultaten en opbrengsten Conferentie Nederland Digitaal 2019,' 2019. March.

27 Ministry of Economic Affairs and Climate, 'Digital Trust Center', n.d.

28 Government of the Netherlands, 'NL DIGIbeter: Agenda Digitale Overheid', n.d.

29 Dutch Parliament, 'Temporary Committee Digital Future', 2020. May.

30 Van Kooten-Arissen, 2019. 'Motie van het Lid van Kooten-Arissen', *Dutch Parliament*, October.

that was inspired by Estonian practices led to an extensive report on how to strengthen the link between citizens and politics in the Netherlands through digital means.[31]

Differences in approaches to creating a resilient society and a digital democratic architecture by Taiwan and the Netherlands can be explained by diverging underlying interests and priorities. Taiwan has always calculated its steps in the context of a looming threat from the People's Republic of China, and its citizens are acutely aware of (possible) Chinese influence on Taiwanese politics and society. Domestic e-governance initiatives are therefore normatively motivated and seek to strengthen society from the bottom–up. By contrast, e-governance initiatives in the Netherlands did not emerge from an existential threat, and development and implementation have largely been left to the private sector.

2.3 The future is digital (democracy)

In recent years, the interests and concerns of Taiwan and the Netherlands are starting to converge, even if Chinese influence (attempts) and awareness thereof among the public are still far lower in the Netherlands compared to Taiwan. The shift in Europe is triggered in particular by the 5G debate, hybrid operations – by state-owned enterprises and academic exchanges – and China's so-called 'wolf warrior diplomacy' during the COVID-19 pandemic. That said, a public debate on geopolitics and digitalisation – and the combination thereof – remains lacking in the Netherlands.

Creating awareness and enhancing the public debate with fact-based knowledge could create momentum for initiatives to better connect citizens and politicians through safe and secure digital means. This should not only further increased awareness of the impact of digitalisation on daily lives, but also build trust and political engagement while the Dutch democracy is digitally transforming. Improved e-governance at the European level could also bring 'Brussels' and EU citizens closer, thereby enhancing trust in the EU processes and European democracy. Currently, only town twinning – that is, networks of towns and civil-society projects – encourages democratic participation at the EU level.[32] These projects bring together citizens at local and EU levels to discuss issues on the European political agenda and create mutual understanding on those topics. Grassroots and national initiatives to enhance digital EU democracy are, however, not yet supported.[33] In addition, the EU could focus on scaling up digital participation. E-participation and e-voting are on the rise in Europe. 'Have your say' is an example of

31 Rathenau Instituut (2020). Initiatieven voor digitale democratie op nationaal niveau – Een internationale vergelijking. Den Haag (auteurs: Jong, R. de, J. Jansen, P. Faasse & P. Diederen)

32 European Commission, 'The Europe for citizens programme', n.d.

33 Lironi, E. 2018. 'Harnessing Digital Tools to Revitalize European Democracy,' *Washington*, Carnegie Europe.

a European online consultation platform for citizens, who can share views on (aspects of) EU laws and policies on this website before the Commission finalises proposals.[34] However, this website's possibilities have not yet reached their full potential, especially with regard to publicity and reach. In order to develop an accessible user environment, scale up the platform and enhance confidence in the system, EU experts can engage with Taiwanese experts who already have a strong and proven track record on these issues. Public–private partnerships and more informal grassroots initiatives are important steps on this trajectory.

Taiwan's push for closer digital connections between the government and its citizens is the outcome of a bottom–up historical path, rather than a swift top–down transformation. In the Netherlands, such a bottom–up transformation – to the extent that it exists – is hampered by the neo-liberal economic mindset wherein digitalisation efforts are largely outsourced to the private sector, rather than an in-house effort that empowers the government for the long haul. This has resulted in a significant gap in knowledge, as well as capabilities, between the Dutch government and (consultancy) businesses, which hampers the swift introduction of digital innovations when needed – such as the COVID app. A more capable and actively engaged government is crucial to ensure that investments are also made in digital innovations that have long-term public benefits but that may generate less profit in the short term, such as digital feedback tools on government policies or government budget visualisations to provide citizens with insights and to increase transparency.

The instalment of a permanent Commission for Digital Affairs in the Dutch House of Representatives following the March 2021 parliamentary elections is an important step towards enhancing awareness among politicians of challenges and opportunities in the digital domain. Beyond the Dutch Parliament, a significant shift is needed in Dutch policy-making and society more broadly. After all, the cross-cutting digital domain impacts practically every policy area, and not all ministries are aware of the increased importance of digital matters. Creating a constructive dialogue with Taiwanese government officials and NGOs may inspire Dutch ministries to attract more in-house knowledge on digitalisation issues and serve as an example of how to create a (digital) connection with society.

Lastly, at the European level, the Taiwan–EU Dialogue on Digital Economy holds great promise, but e-governance and the dimension of digital democracy are yet to be included. Democratic engagement and civic participation in EU decision-making are still lacking. Digital tools can be of assistance to foster European citizenship and improve concrete civic participation in the EU policy-making process.

34 European Commission, 'Welcome to Have your say', n.d.

3 Dealing with foreign technology companies

While Taiwan is clearly a frontrunner in digital government, the EU has come to be the global referee in attempting to rein in the power of so-called Big Tech companies – for now, mostly from the United States. Despite the convergence of norms with the EU, regulating Big Tech has not been on the agenda of the Taiwanese government. Its efforts in this regard are mostly within the framework of the Asia–Pacific Economic Cooperation (APEC) and in tune with the United States. One Taiwanese expert explains succinctly why this is the case: 'because we have a bigger enemy to deal with'. Clearly, Big Tech regulation – which may antagonise the United States – is a lesser priority in Taiwan, because of the continued threat from China.

As Washington also turned towards regulating Big Tech in late 2020, now is a good time to engage Taiwanese players on digital regulation with European characteristics. Cooperation between Taiwanese and European actors may help to raise the human-centred approach, not only in their own jurisdictions, but also in third countries.

3.1 The EU: regulating Big Tech data

In December 2020, the European Commission proposed its long-awaited legislation to curb the power of Big Tech companies as part of the EU's Digital Strategy: the Digital Services Act (DSA); and the Digital Markets Act (DMA).[35] These acts encompass new rules and aim to create an open digital space, with European values at the core of the legislation. The DMA establishes obligations for dominant online platforms that act as 'gatekeepers' in the digital market in order to create a fairer business environment and a level playing field for innovators and start-ups, and aims to create a wider array of platforms for consumers. The DSA aims to better protect consumers' rights, establish transparency and a clear accountability framework for platforms, and foster innovation. To tackle disinformation, the proposal sets out a co-regulatory backstop, to which Facebook, Twitter and Google have already signed up,[36] in order to provide platforms with codes of conduct to address the negative impacts of information.[37]

35 European Commission, 'The Digital Services Act Package,' 2021. March.

36 Stolton, S. and Grüll, P., 2021. 'Lawmakers call for tougher EU disinformation laws in wake of US riots,' *EURactiv*, 8 January.

37 European Commission, 'Digital Services Act – Questions and Answers,' 2020. December.

In addition, a revised Code of Practice aims to counter online disinformation under the legal framework of the DSA. Some Members of the European Parliament, however, argue that guidelines will not be enough to counter disinformation, as they rely on the platforms' goodwill.

This new legislation has been the product of years of legal battles between the European Commission and US Big Tech companies Google, Apple, Facebook and Amazon (known collectively as GAFA).[38] European Commissioner for Competition Margrethe Vestager, who is also the Executive Vice-President of the European Commission for A Europe Fit for the Digital Age, has led most of these high-profile investigations, but these never resulted in concrete change in the behaviour of these companies.

In addition to the newly proposed DSA and DMA, discussions on digital taxation, privacy, the bounds of free expression and accountability of platforms are areas of concern, but the EU is moving closer to addressing all these matters in the context of the European Digital Strategy. In particular, the European White Paper on AI and the General Data Protection Regulation (GDPR) that preceded the DSA and DMA proposals demonstrated the standard-setting power of the EU, even beyond its own borders.

The new regulation comes at a delicate time, as it will primarily affect the big US technology platforms, which have become 'too big to care', in the words of EU Commissioner for the Internal Market Thierry Breton.[39] As the EU and US under President Joe Biden try to revive the damaged transatlantic relationship, Big Tech regulation poses one hurdle to improved ties. US actors are especially unsettled by the EU focus on regulating GAFA companies – instead of its Chinese equivalents Baidu, Alibaba, Tencent and Xiaomi (collectively known as BATX) – because of their larger EU market share.[40] Underpinning this debate is strong divergence between the EU's economic security approach and normative arguments for digital regulation, in particular privacy protection and a digital level playing field, and the US national security approach, which aims to counter Chinese Big Tech. Indeed, it is not so clear that the EU regulatory efforts today look beyond US Big Tech companies and incorporate in today's discussion the challenges that greater European market share by Chinese companies are likely to bring. After all, as illustrated also by the recent rethink of investment screening, companies that may seek not just economic but also political/strategic goals need to be governed in different ways than traditional private-sector

38 Amaro, S., 2020. 'The EU is about to announce new rules for Big Tech – and there's not much they can do about it,' *CNBC*, 5 November.

39 Espinoza, J. and Fleming, S., 2020. 'EU seeks new power to penalize tech giants', *Financial Times*, 20 September.

40 Dekker, B., and Okano-Heijmans, M., 2020. 'Dealing with China on high-tech issues: views from the US, EU and like-minded countries in a changing geopolitical landscape,' The Hague, the Clingendael Institute.

companies – specifically, by also considering national security grounds and public order as reasons for government intervention.

In 2018, the divergence between the United States and Europe on the responsibilities and ethical implications of Big Tech concerning data usage seemed to decline when Facebook was summoned by the US Senate after the Cambridge Analytica scandal.[41] However, the ethical and normative debate receded in subsequent years, as the US–China trade–tech war and the consequent national security focus took centre stage. The Capitol Hill riots and subsequent Twitter ban of Trump, however, seem to have resurrected the debate concerning Big Tech regulation within the United States, which will likely bring the US and EU closer together in the coming years.

3.2 Taiwan: citizen awareness and bottom–up push

While the digital policies of the EU and its member states mostly focus on privacy protection and Big Tech regulation, Taiwanese policies are shaped by Taiwan's deep distrust in Chinese undertakings. In the digital age, this distrust is amplified by the constant flow of cyberattacks and reflected in the low number of Taiwanese citizens using applications or technology developed by Chinese companies.

Chinese telecommunications company Huawei has been at the centre of the 5G discussions globally, but was already barred from 4G networks in Taiwan. Moreover, popular Chinese applications such as TikTok and WeChat did not make any headway in Taiwan, with even the younger generations aware of the potential (information) security risks. A key difference with US Big Tech companies, as highlighted by Taiwanese experts, is that TikTok allows Chinese government-sponsored accounts. This means that the Chinese government can covertly communicate political messages and state propaganda to TikTok users, which poses national security concerns for the Taiwanese democracy. This is a different argument than that put forward by the United States under President Trump, which tried to ban TikTok on the grounds of national security, as the data collected by TikTok could be used for blackmail or espionage.[42]

In a way, the Taiwanese approach to Big Tech is closer to the US than to the EU and its member states, as both focus on national security issues rather than on the ethics of data-gathering and the (mis)use of data by third parties – the EU's main focus area. Taiwan does have data regulation in place, however. The collection, process and use of

41 Perticone, J., 2018. 'Another congressional panel just summoned Mark Zuckerberg – and it could be the tip of the iceberg,' *Business Insider*, 23 March.

42 Gertz, G., 2020. 'Why is the Trump administration banning TikTok and WeChat?,' *Brookings*, 7 August.

personal data are subject to the Personal Information Protection Act (PIPA) of 2015[43] and the Enforcement Rules of the Personal Data Protection Act.[44] With the international effect of the GDPR being more extensive than ever imagined, the Taiwanese government held several public hearings to solicit public opinion on the PIPA and the possibility of changing the regulation to comply with the EU's standards.[45] Companies, in particular, consider the GDPR as a potential obstacle and barrier for Taiwanese companies' commercial interests in the EU, and there is still a lack of awareness among Taiwanese civil society about the consumer side of data protection.

Related to concerns about implicitly communicated political messages from the Chinese government to Taiwanese citizens are concerns about misinformation, as Taiwan faces continuous cyberattacks from China. The objectives of these attacks are manifold, from undermining Taiwanese President Tsai Ing-wen's leadership, to sowing doubts on liberal democracy as a government system and promoting China's authoritarian government as superior. Information is distorted or framed to feed these narratives. Despite the differences between Taiwan's and China's use of Mandarin characters – traditional and simplified, respectively – shared language is an important element for the success of Chinese disinformation campaigns in Taiwan. With the diversity of threats, Taiwan's government has developed a nationwide strategy to counter disinformation by engaging Taiwanese citizens. Especially the Cofacts system and 'Dr Message', chatbots that can be added as contacts on mobile phones, are unique in reducing disinformation. Citizens can simply flag the disinformation by forwarding it to the chatbot and the Cofacts employees will check whether follow-up action is needed.[46] This initiative has been successful and the Taiwan Fact Checking Center partners with Cofacts to conduct a more in-depth fact check or an investigation into a specific rumour to limit the spread of disinformation and fake news.[47]

Through the DSA, the EU is also considering ways to limit the spread of illegal and harmful messages, including misinformation and fake news. Looking into the methods used by the Taiwanese government and companies to create a holistic and effective approach to counter misinformation can serve as input for the intended development of a co-regulatory framework.

43 Dataguidance, 'Personal Data Protection Act 2010 (as amended in 2015),' 2015.

44 Dataguidance, 'Enforcement Rules of the Personal Data Protection Act (2 March 2016),' 2016.

45 Dataguidance, 'Taiwan - Data Protection Overview,' 2020. July.

46 Tseng, E., 2020. 'Rumors vs. Reality: Dr. Message and Cofacts Combat Misinformation,' Taipei, TaiwanNGO.

47 Taiwan FactCheck Centre, 'About Us', n.d.

3.3 Regulation of the platform economy: not so different after all?

While the underlying incentives when it comes to Big Tech regulation thus diverge between the EU and Taiwan, their ultimate aim may not be too different after all, as both – although to different extents – share a human-centred focus and hold national security concerns at the core. The EU and Taiwan are both concerned by the increased regulatory power that Big Tech platforms acquire and the market disruptions these companies can constitute by either limiting start-up potential or forcing traditional players, such as taxi drivers, out of the market. Countering disinformation has been one of the main controlling measures for social media platforms in Taiwan, with an effective government strategy. In the EU, the focus has been mainly on the broader regulation of Big Tech platforms. Rather than governments countering disinformation, the platforms are held accountable and the consumer is protected through extensive EU legislation. Hence, the aim is similar, but the approaches and priorities differ. Notwithstanding the differences, cooperation in the field of broader platform regulation, countering misinformation and consumer protection are feasible areas to increase cooperation between the EU and its member states and Taiwan.

The window of opportunity to influence platform regulation effectively on a multilateral level is closing rapidly, especially now that the US seems to be taking steps to regulate US Big Tech by summoning GAFA to court.[48] In a 499-page report in October 2020, the US Congress stated that the GAFA companies had abused their monopoly power, and called for changes to anti-trust laws in the US to restore competition. While concrete action may still be a long way off, Taiwan and the EU may want to share best practices and refine their strategies to stand their ground effectively once the US turns to its allies to respond effectively to upcoming issues concerning platform regulation.

A path forward could be to include platform regulation into the Taiwan–EU Dialogue on Digital Economy (DDE)[49]. The EU has taken its first steps to regulating Big Tech with the publication of the DSA and DMA, in addition to the GDPR. Discussing these with Taiwanese experts and government officials may not only be a useful exercise to determine the (unintended) extra-territorial effects of the EU's digital platform governance efforts, but also to identify upcoming difficulties in platform regulation. First, this could involve an exchange of views on disputes between like-minded governments and Big Tech companies, such as the 2021 dispute between Facebook and the Australian government about proposed legislation that would force technology

48 Kang, C. and McCabe, D., 2020. 'House Lawmakers comdemn Big Tech's 'monopoly power' and urge their breakups', *The New York Times*, 6 October.

49 National Development Council (NDC), 'The 2nd Taiwan-EU Dialogue on Digital Economy (DDE) successfully concluded,' 2020. 8 December.

platforms such as Facebook to pay local and international news publishers for content.[50] Facebook barred Australian users for a few days in late February 2021 from finding or sharing news on their timelines as a reaction to the proposed legislation, thus concerning citizens that Facebook may be too powerful to handle for the government.

Second, while Taiwan's situation is unique – in the sense that it is a bigger target of cyberattacks from China than any other government – the Taiwanese government's approach to online disinformation can serve as an inspiration to European governments. Disinformation and fake news concerning COVID-19 vaccines and elections are of particular concern for EU member states such as the Netherlands and Germany, both with elections in 2021. The International Institute for Democracy and Electoral Assistance (IDEA) developed a code of conduct to increase the transparency of political advertisements on social media platforms and the Dutch government launched a website to address disinformation during election times.[51] The Taiwanese government has experience in countering disinformation. Encouraging joint research and projects between European and Taiwanese companies and think tanks may refine the Dutch – and other EU member states' – approaches to countering disinformation in areas beyond the elections and political advertisements.

Third, the economic recovery from the COVID-19 pandemic will largely be focused on the digital transformation of companies, showing the need for cross-border cooperation with partnerships between the public and private sectors. Notwithstanding the shared privacy goals, Taiwan is not necessarily a firm supporter of stronger data protection regulation such as the EU's GDPR. However, the EU could step up its efforts through the EU–Taiwan DDE, by including a structural dialogue on the benefits of the GDPR and possibilities to connect the EU and Taiwanese digital markets through an adequacy decision. Thereafter, there could be more convergence between Taiwan's DIGI+ plan (which aims to promote digital development and hasten Taiwan's transformation into a smart-tech nation), promoting six core strategic industries, and Europe's Digital Strategy, which aims to ensure Europe's leading position in global digital developments. The sharing of best practices, but also concrete joint projects in fields such as micro-electronics, smart systems, AI, blockchain and cybersecurity have to be at the core of any EU–Taiwanese cooperation.

50 Flynn, K., 2021. 'Facbeook bans news in Australia as fight with government escalates', *CNN Business*, 19 February.

51 The Netherlands Ministry of the interior and Kingdom relations, 'Minister Ollongren bevordert transparantie politieke advertenties met gedragscode', 2021. February.

4 Digital official development assistance

In addition to improving digitalisation efforts at home and jointly in the international realm, digital official development assistance (ODA) is an important instrument for Taiwan and European countries to improve digital connectivity and promote standards in third countries. By way of its Digital Silk Road, China already responds to the need in developing countries for increased digital assistance.[52] The EU is enhancing its efforts to create offers of its own, in particular in Africa, to provide alternatives to the Chinese assistance. Taiwanese ODA, for its part, has been focused on the Southeast Asian region. Greater synergies and improved complementarities are an important way to deliver better results on shared interests.

Within Europe, the Digital4Development (D4D) policy of 2017 has mainstreamed digital technologies and services into EU development policy.[53] The Cyber4D project, for example, seeks to promote and sustain a secure and safe digital environment in developing countries.[54] As a practical extension of the Netherlands Digitalisation Strategy of 2018[55], the Digital Agenda for Foreign Trade and Development Cooperation of 2019 (in Dutch, BHOS) aims to map possibilities and risks of digital technology to improve ongoing ODA initiatives and enhance future interventions, employing the (internationally agreed) Principles for Digital Development.[56] Furthermore, the BHOS seeks new international coalitions with like-minded partners to foster digitalisation. Supporting developing countries in the digital economy and trade, cybersecurity and capacity-building, as well as promoting responsible use of digital technology and data, including digital rights, are central to Dutch efforts. 'Learning from others' experiences' is explicitly mentioned in the BHOS.

52 Dekker, B. and Okano-Heijmans, M., 2020. 'Unpacking China's digital silk road,' The Hague, the Clingendael Institute.

53 European Commission, 'The EU Digital for Development policy,' 2017. May.

54 European External Action Service, 'Launching of the EU Cyber-Resilience for development Cyber4D programme in Mauritius', 2019. February.

55 Government of the Netherlands, 'Nederlandse Digitaliseringsstrategie: Nederland digitaal – hier kan het. Hier gebeurt het,' 2019. June.

56 Government of the Netherlands, 'Digitale agenda voor buitenlandse handel en ontwikkelings-samenwerking,' 2019. June.

Overall, Dutch efforts in digital ODA aim to enhance digital inclusion and create resilient societies against digital threats, thereby enabling specific groups, such as women, the elderly and rural citizens, to take advantage of the digital revolution.[57] Digital inclusion and enhanced digital resilience, however, can only be achieved with the availability of hard infrastructure, which remains a basic need in many Indo-Pacific countries. Telecommunications networks are the backbone of digitalisation, while mobile phones and data packages can bring more citizens online. This remains a blind spot in the agendas of both Taiwan and Europe. China has been responding to this basic need in the developing world, providing beneficiary countries with the necessary digital infrastructure. This benefits China, as Chinese companies effectively export the technical standards underpinning their technologies to recipient countries. The EU and the Netherlands have so far neglected this basic element, which requires more investments in infrastructure, education, literacy and communications. E-economies that are largely built on Chinese infrastructure will, however, complicate ODA efforts that seek to compel Asian governments to make digital inclusion central to their future development trajectories.

Taiwanese efforts to improve digital connectivity abroad focus on e-governance, capacity-building by sharing experiences in coding and enhancing policy abilities, and jointly developing information and communication technology (ICT) solutions towards development in a diversity of areas, such as healthcare and agriculture.[58] Already in 2009, the Taiwanese Ministry of Foreign Affairs in its White Paper on Foreign Aid Policy highlighted the importance of collaborating with the private sector in third countries to make new technologies available.[59]

Taiwan's dispute with China puts real constraints on its assistance to and cooperation with third countries. Taiwanese actors are careful to position their activities as complementary to, rather than in competition with, China's Digital Silk Road and other Chinese mainland initiatives.[60] Projects are framed as connected to the United Nations' Sustainable Development Goals (SDGs), as these are perceived as more neutral and less politically sensitive, and avoid putting the recipient country in an awkward position. One specific project carried out by the Taiwanese government is the Taiwan Digital Opportunity Center (TDOC).[61] As part of the New Southbound Policy, the TDOC focuses

57 Government of the Netherlands, 'Begroting Digitaliseringsagenda BHOS,' 2021.

58 International Cooperation and Development Fund, 'Information and Communications Technology,' n.d.

59 Ministry of Foreign Affairs Republic of China (Taiwan), 'progressive partnerships and sustainable development: white paper on Foreign Aid Policy', 2009. May.

60 Choi, K., 2020. 'Weapons Brushed By the Enemy: The Bounded Autonomy of Taiwan's Middle Power Foreign Policy' *The Korean Journal of International Studies*, April, 18(1), 87-122.

61 Ministry of Foreign Affairs Republic of China (Taiwan), 'Taiwan Digital Opportunity Center (TDOC) Project,' 2016. January.

on improving countries' ICT capabilities and reducing digital divides in the region.[62] Moreover, Taiwan shares its expertise with partners around the world by way of the Global Cooperation and Training Framework (GCTF), which is administered by the US, Taiwan and the Japan–Taiwan Exchange Association.[63] Through this initiative, Taiwanese experts engage with practitioners from around the world in a wide variety of fields – including public health, the digital economy, cybersecurity and good governance – even if many international institutions do not allow Taiwan to participate.

4.1 Towards greater synergies and coordination

Coordination between Taiwan and European actors, including the Netherlands, in the provision of digital ODA to third countries is very limited at present, although Taiwanese interlocutors indicate an interest in exploring this area. As the EU and its member states pivot to the Indo-Pacific, partnering with Taiwan on digital ODA can bring mutual benefits, as Taiwan is an experienced actor in the region on digital connectivity, while the EU can bring scale to efforts. Two potentially fruitful areas for synergies and coordination are e-health innovation – in which Taiwan is a frontrunner – and cybersecurity – in which the Netherlands has gained significant experience over the last decade.

4.2 Case study: Taiwan's e-health innovation

E-health was a focus area of Taiwanese digital ODA even before the COVID-19 pandemic, promoted under President Tsai's New Southbound Policy. Agencies like the International Cooperation and Development Fund (ICDF) assist other countries in developing ICT solutions for practical issues similar to those Taiwan itself faces, such as maternal healthcare in rural areas. The United States acknowledged Taiwan as a valuable partner in the Memorandum of Understanding (MoU) signed by the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO) in August 2020.[64] In November 2020, an MoU was signed between the same partners to create a US–Taiwan Economic Prosperity Partnership Dialogue in which global health security, including pandemic preparedness

62 Office of Trade Negotiations, Executive Yuan, 'An introductory guide to Taiwan's New Southbound Policy,' 2017. September.
The New Southbound countries include Australia, New Zealand, Singapore, Malaysia, Brunei, Thailand, the Philippines, Cambodia, Indonesia, Laos, Myanmar, Vietnam, India, Bhutan, Sri Lanka, Bangladesh, Nepal and Pakistan.

63 American Institute in Taiwan, 'Global Cooperation and Training Framework (GCTF) Programs,' 2020.

64 American Institute in Taiwan, 'AIT and TECRO Sign MOU on Health Cooperation,' 2020. August.

and response, will be a continued topic of discussion.[65] In order to increase Dutch and Taiwanese efforts abroad in the field of digital ODA, a similar framework is worth exploring.

Taiwan plays to its strengths in the provision of digital assistance to friendly countries, focusing on areas where it can export its own development experiences to deepen regional integration. E-health is a prime example of this. As a country that has been extremely successful in containing the spread of COVID-19 within its borders with the help of digital technology, Taiwan has branded itself as a reliable partner and 'a force for good in the international community' in international efforts to fight the virus.[66] Using the slogan 'Taiwan Can Help', the Taiwanese government kicked off a campaign of providing medical resources and sharing its methods to aid others in containing the pandemic.[67] It also uses its success story as a platform to lobby for increased participation in international organisations from which it is currently barred, such as the World Health Organisation (WHO) and the United Nations (UN).

One example of Dutch activities in e-health ODA, the Dutch government has been part of a joint project with PharmAccess and CarePay, which launched the online platform 'M-Tiba' in 2015.[68] This platform connects patients, insurance companies and healthcare institutions for the financing and delivery of high-quality care through text, telephone or internet services. In Nigeria and Kenya, this platform enjoys wide support from local governments.

Hence, the proven track records of Taiwan and the Netherlands in the field of digital assistance complement each other in Southeast Asia and Africa, respectively.
As the EU and its member states prepare to deepen their engagement in and with the Indo-Pacific – most likely also in the field of digital ODA – they would do well to coordinate their actions with democratic countries in the region, including Taiwan. After all, they share concerns about creeping digital authoritarianism in countries ranging from China, Myanmar and Cambodia, and can build on each other's experiences. Coordinated efforts that also engage the relevant private-sector players will lead to better overall results and more effective allocation of limited funds.

65 American Institute in Taiwan, 'MOU between AIT and TECRO on establishing an US-Taiwan Economic Prosperity Partnership Dialogue,' 2020. November.

66 Ministry of Foreign Affairs Republic of China (Taiwan), 'Taiwan can help, and Taiwan is helping!,' 2020.

67 Taiwancanhelp.us, 'WHO can help? Taiwan', 2020.

68 Government of the Netherlands, 'Digitale agenda voor buitenlandse handel en ontwikkelings-samenwerking,' 2019. June.

4.3 Case study: the Netherlands and cybersecurity

Cybersecurity is an important precondition for the digital economy and society to function. As digitalisation accelerates, cyber threats have been on the rise. The Netherlands and Taiwan have a cooperation track record on cybersecurity, as exemplified by the Taiwan–Israel–Netherlands Forum of Cybersecurity in Smart Cities in 2018.[69] In addition, a Taiwanese cybersecurity start-up delegation visited the 'One Conference' in 2019, the largest international cybersecurity conference in the Netherlands; and Taiwan participated as an observer in the 2020 annual meeting of the Global Forum on Cyber Expertise (GFCE), initiated by the Netherlands and established at the 2015 Global Conference on Cyberspace in The Hague.[70]

Internationally, the Netherlands focuses on enabling developing countries to enhance their digital security and increase freedom online.[71] In 2013, the Dutch government established The Hague Security Delta, encompassing a multi-stakeholder network to exchange knowledge and create joint research projects in the area of (cyber)security.[72] Subsequently, Dutch digital ODA strategy has focused on cybersecurity capacity-building in developing countries, as this may contribute to those countries' digital resilience. The integrated International Security Strategy of 2018–2022 emphasises, among other things, the importance of strengthened Dutch cyber diplomacy and the connection between the Netherlands' unique position regarding international law and order and the Dutch push to improve cybersecurity on a global level.[73] Bilateral dialogues are also part of Dutch cyber diplomacy efforts to push cybersecurity higher on the international agenda.[74] In January 2021, the Indonesian–Dutch Dialogue on International Cybersecurity was organised virtually to reaffirm the close cooperation between partners in the field of normative international frameworks, capacity-building and disinformation in the digital domain.[75]

Taiwan's activities in the cybersecurity domain have largely been driven by the continuous threat of cyberattacks from China. The Taiwanese National Cybersecurity Strategy is therefore mainly concerned with developing and strengthening Taiwan's

69 Netherlands Ministry of Foreign Affairs, 'Research of cybersecurity industry in Taiwan,' 2020. June.

70 The GFCE, 'Strenghtening cyber capacity and expertise globally through international collaboration,' 2018.

71 Government of the Netherlands, 'Digitale agenda voor buitenlandse handel en ontwikkelings-samenwerking,' 2019. June.

72 The Hague Security Delta, 'Together we secure the future,' n.d.

73 Netherlands Ministry of Foreign Affairs, 'Wereldwijd voor een veilig Nederland: geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022,' 2018. March.

74 Netherlands MInistry of Foreign Affairs, 'Factsheet: Cyberdiplomatie,' 2019. July.

75 Goverment of the Netherlands, 'Eerste Indonesië-Nederland-Dialoog over internationaal cyberbeleid: gezamenlijke verklaring,' 2021. January.

cybersecurity to protect domestic infrastructure, companies and citizens.[76] Representatives from Taiwan's National Development Council (NDC) and the Taiwanese Ministry of Foreign Affairs detailed that the 2019 focus had been on the exchange of talent, research and development and international cybersecurity cooperation. An enhanced cybersecurity dialogue through a multi-stakeholder platform to connect Dutch and Taiwanese policy-makers, businesses and academia is therefore a natural way forward. The Taiwanese government has shown a willingness to share its database on cyberspace and cyberattacks, which entails regional information and insights into Chinese cyberattacks. This could be specifically interesting for the Netherlands, as it would provide Dutch intelligence services with greater knowledge and patterns that could enhance the Netherlands' cybersecurity strategy towards China, as noted in the May 2019 policy paper 'The Netherlands and China: a new balance'.[77] Within the domain of digital ODA, bilateral cooperation between the Netherlands and Taiwan could enhance Dutch cybersecurity diplomacy and enable both governments to promote the development of cybersecurity projects effectively in third countries.

Another specific opportunity for coordination could be increased information-sharing on the Taiwanese 'hardware root of trust' (for details, see Box 1). In response to the ongoing flow of cyberattacks from China, the Taiwanese government established a large network of government officials, industry representatives and academics to create a resilient Taiwanese ecosystem. Related to Taiwan's cybersecurity expertise are the efforts of the Taiwanese government to advocate for international cyber standards, specifically in the field of the Internet of Things (IoT). In order to establish this for IoT products that are manufactured in Taiwan, the Taiwanese government is now providing necessary security advice and security certificates to companies. This market shortcoming is caused by the use of open-source networks to develop products, a useful tool for innovation but often lacking the necessary cybersecurity expertise/safeguards. By introducing this new programme, the Taiwanese government aims to create secure IoT applications, assist high-tech companies with meeting international cybersecurity standards and to gain consumers' confidence, all translating into annual profits for the Taiwanese companies.

Regarding digital ODA, Dutch and Taiwanese counterparts can assist the implementation of cybersecurity systems in third countries, provide training and encourage capacity-building. Currently, however, the Dutch and Taiwanese efforts are not yet aligned, so building synergies and coordination could strengthen and complement the efforts of both governments in third countries.

76 National Center for Cyber Security Technology, 'About NCCST', n.d.

77 Government of the Netherlands, 'The Netherlands & China: a new balance', 2019. May.

Box 1 The hardware root of trust

The Taiwanese government is currently implementing a programme that advocates for a *hardware root of trust* and a (supply) *chain of trust*. The hardware root of trust[78] is the foundation on which all secure operations of a computing system depend. This is mostly done in a programmable hardware root of trust, so it can be updated and versatile. Additionally, the (supply) chain of trust refers to the validation of each individual component within a supply chain of a specific 'Internet of Things' (IoT) product, ensuring the sole use of trusted hardware and software.

In short, IoT encompasses a network of physical objects that can be connected through a network, thereby enabling the devices to collect and share data to create an optimal user experience.[79] The IoT industry is skyrocketing, with numerous traditional goods, such as door locks, fridges and streetlights, being updated with IoT advancements. This raises questions about the security of the full IoT product supply chain, and the possible threat that software updates may pose to the IoT goods.

A specific initiative that builds on the concept of the chain of trust is the Clean Network Program.[80] Initiated by the Trump administration, the Clean Network Program ensures a safe telecommunications network by only engaging with trusted partners in the full telecommunication spectrum (applications, app stores, cloud services, undersea cables and telecommunication operators). Taiwan is a member of the clean 5G network, as it has been 'clean' since the introduction of 4G.

In another initiative, President Biden signed an executive order on 24 February 2021 for 'resilient, diverse, and secure supply chains'.[81] This includes a 100-day review of supply chain risks for four vital products, including semi-conductors. Although not explicitly stated, the effort is aimed at reducing the United States' reliance on China, where Taiwan is, again, positioned as a logical partner.

78 Rambus, 'Hardware Root of Trust: Everything you need to know,' 2021. February.
79 IBM, 'What is the Internet of Things (IoT),' 2016. November.
80 U.S. Department of State, 'The Clean Network,' 2020. December.
81 The White House, 'Executive Order on America's Supply Chains,' 2021. February.

5 Conclusion

Although both the EU and Taiwan acknowledge the importance of digital connectivity, their approaches and priorities are not yet aligned. Taiwan primarily seeks to fend off disinformation and cyberattacks from mainland China and e-health is a key element of its assistance to neighbouring countries. For their part, efforts by the EU and its member states in the field of digital connectivity focus on digital regulation and strengthening cybersecurity efforts. The EU's and Dutch digital ODA still primarily targets African countries and hardly reaches the Indo-Pacific region. While the EU is taking real steps to regulate Big Tech to protect data privacy and break monopolies, Taiwan takes a free-market approach that focuses on increasing digital literacy/skills rather than market intervention. EU regulations in the digital field are viewed as obstacles for Taiwanese companies seeking to work with European partners and in the European market.

In Taiwan, the main priority has been, and continues to be, the creation of a resilient society that can counter Chinese interference and uphold democratic structures. As such, the Taiwanese government has prioritised the cybersecurity challenge from China, seeking to empower government and citizens to deal with this threat. In Europe, cybersecurity has largely been left to the private sector. Today, this leaves the continent with an outdated framework that is unfit to deal with the hybrid security threat emerging from China.

EU member states have only recently come to see China as a 'systemic rival' promoting alternative models of governance.[82] They are still at the start of the long-term process of rebalancing geo-economic opportunities and threats arising from China. In recent years, the EU's focus in the digital domain has been on reigning in Big Tech. As such, the EU has prioritised the economic challenge that for now comes from the United States, embarking on a long trajectory of top–down digital regulation. Put simply, Taiwan has bigger worries than US Big Tech.

Differences in historical experiences, priorities and approach notwithstanding, the strategic interests and goals of Taiwan and Europe have converged in recent years. Most importantly, both the EU and its member states and Taiwan can be characterised as favouring a human-centred approach to the digital domain. China's growing influence and assertive behaviour pose a substantial challenge for Taiwan's and Europe's open, inclusive democracies, economic competitiveness and standard-setting power.

82 European Commission, 'European Commission and HR/VP contribution to the European Council: EU-China – A strategic outlook,' 2019. March.

As they seek to promote sustainable and secure digital societies at home and digital connectivity in and with other countries, Taiwan and Europe stand to benefit from each other's complementary skills. Ample opportunities exist to leverage their economic, scientific and cultural ties to this objective. As this Clingendael Report lays out, synergies, coordination and cooperation between the EU and its member states – the Netherlands specifically – and Taiwan are particularly evident in the following domains:

- **Resilient societies:** the EU and its member states can learn from Taiwan by exchanging best practices on blending technology and politics, and insourcing the experts needed to guide governments through their digital transformation. Increased cooperation with Taiwan in this field will be highly valuable for European governments.

- **Big Tech regulation:** the Netherlands, EU and Taiwan would benefit from mutual exchanges, with Taiwan having experience and a proven track record in countering disinformation, while the EU has been stepping up its game to regulate Big Tech and address consumers' privacy concerns through the GDPR. Creating awareness among Taiwanese companies and citizens about the collective benefits of the GDPR could increase understanding and awareness, and dispel any doubts from Taiwanese companies.

- **Digital ODA:** The Netherlands and Taiwan can create synergies between their efforts in third countries. Taiwan focuses most of its e-health initiatives on East and Southeast Asia, while Dutch efforts primarily target African countries. Creating synergies in capacity-building efforts and training on cybersecurity could deliver greater benefits overall and inspire action in other fields as well.

Moving forwards, various challenges remain. In Europe, policies and instruments to deal with China's growing geopolitical and political clout are still in an early phase. Particularly in Big Tech cooperation, the EU needs to look beyond US Big Tech companies and incorporate into today's discussion the challenges that greater European market share by Chinese companies will bring. At the same time, the Chinese government's pressure on Europe – in the economic, political and/or security domain – creates difficulties in the EU–Taiwanese relationship beyond pure economic cooperation. Utilising the EU–Taiwan Dialogue on the Digital Economy (DDE) as an established platform, and expanding the topics addressed in the DDE, are important steps to nourish synergies and coordination in the digital domain between Taiwan and the EU and its member states.