Asia Pacific Contributions to International Cyber Stability

Caitríona Heinl

INTERNATIONAL CYBER STABILITY

This article examines activities in the Asia Pacific related to normative proposals for restraining self-interested state activity in the field of cyber.[1] In the absence of a global agreement for international cybersecurity in the immediate future, this article outlines the potential for other multilateral efforts and regional activities in the Asia Pacific to promote common views, and universalise norms as stepping-stones to progress for an international governance framework. More research is needed now to address issues of stability and escalation control, which some scholars believe is arguably more important (or achievable) than seeking military superiority.[2]

While there did not seem to be consensus within the 2016-2017 United Nations Group of Governmental Experts (UN GGE) for new norms, nor does there seem to be an appetite for new norms in Asia Pacific discussions, new norms could potentially develop in other forums. In any case, this article is timely given the recent increase in attention on regional activities as a means to forge progress beyond the UN GGE.

Many states in the region recognise their self-interest in ensuring that cooperation in this field continues to support market interdependence, as well as regional economic and social growth. This is particularly the case where many

[1] The author explored similar questions surrounding the cyber-world order nexus for a panel session, "World disorder, cyber norms and grand strategy: the search for peaceful equilibrium", MIT-Harvard International Conference on Cyber Norms 5.0, March 2017. This article is adapted to focus on the Asia Pacific from the author's subsequent article: Caitríona Heinl, "Cyber dynamics and world order: Enhancing international cyber stability", Irish Studies in International Affairs, Royal Irish Academy, 2018.

[2] Jason Healey, "Triggering the New Forever War, in Cyberspace", The Cipher Brief, 1 April 2017, https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace, accessed 11 June 2018.

Asian countries' digital strategies consider the digital economy to be essential to their visions for future prosperity. Even where there are worries that international cybersecurity negotiations are currently stalling, economic-self interest that is often linked to the digital economy or smart city concepts (such as Singapore's "Smart Nation" ambitions) can sometimes explain why progress has already been made – and may continue to be made – in the field of cyber compared to other domains. Moreover, such delays can be part of the natural course of deliberations in a relatively new field where international discussions first began twenty years ago when Russia tabled a draft resolution in the First Committee of the UN General Assembly. It will continue to take time for this field to develop over the longer term. Indeed, the 2015 GGE consensus report specifies that the 11 voluntary non-binding norms' implementation may not be immediately possible.[3]

The need for political willingness, especially among the major powers, will continue to be a key factor in progressing with the development and implementation of norms of state behaviour and confidence-building measures (CBMs). A key concern raised following the 2016-2017 UN GGE is that the previous GGE meetings and work within regional bodies such as the Organisation for Security and Cooperation in Europe (OSCE) and ASEAN Regional Forum (ARF) took place in a more favourable international security environment. Many recent and ongoing geopolitical tensions do not bode well for such political willingness, and economic self-interest may not always outweigh such tensions. Nonetheless, leaders in countries like Singapore, while recognising this challenge, still advocate that although all 11 norms of the 2015 GGE are not ideal, they are practical and it is better to move forward by focusing upon their implementation.[4]

Given that state competition and self-interest can often have greater influence on state practice than norms, a number of trends such as intensifying major power rivalry, rising nationalism as well as challenges to the rule of law and international human rights obligations are making it even more difficult to find common ground on state behaviour in cyberspace. While these are trends that are being witnessed globally, many Asian countries such as Myanmar, Cambodia and the Philippines, among others, are now criticised for regressing. Asian countries can be significantly

[3] UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, 22 July 2015, pgh. 14, p. 8, http://undocs.org/A/70/174, accessed 12 June 2018.

[4] Author observations, United Nations Institute for Disarmament Research (UNIDIR) and CSIS, "International security cyber issues workshop: Preserving and Enhancing International Cyber Stability-Regional Realities and Approaches", September 2017. Experts, including the author, explored these questions in preparation for the workshop.

diverse in terms of cultural and political sentiments where, for instance, Japan, India, and Korea are rather different to China or Southeast Asia when it comes to openness and democracy. This difficulty is exacerbated by different conceptions of world order and conceptual understandings of cybersecurity and information security, including disruptive state behaviour in multilateral cyber efforts. China and Russia have been criticised for sometimes playing a disruptive role in multilateral cyber efforts on CBMs and transparency in forums like the UN GGE, ARF, and OSCE. Given calls at the highest levels in the Asia region for reform of the multilateral order and recognition of multi-polarity, scholars must therefore continue to consider the potential impact of these developments on cyber conflict and stability. This includes, for instance, the ambitions and need for more states in the region to become involved in shaping the agenda.

Given the palpable levels of dissatisfaction with the current post-World War Two order that is perceived by some Asian countries as Western-centric, states seem more willing to engage in cyber-enabled influence operations and low-level activity below the threshold of armed conflict to bring about change in the international security architecture. In other words, state parties and their proxies are more willing to pursue their ambitions to change the current order and undermine democracies with cyber-enabled tools without resorting to the use of military force, and without fear of major retaliatory consequences. While liberal democracies are particularly vulnerable to these types of activities, state espionage and political influencing will most likely continue, which means that states must develop more robust cyber defences and strengthen the resilience of their citizenry to these types of activities. The majority of attention is currently focused on Russian influence and information operations, yet rising global powers in the Asia region such as China also have ambitions in order building. Several national strategies delineate that cyber operations also include information operations – information security and hybrid conflict are aspects of national strategies in powers like China that have different conceptions of world order. This will then continue to have implications for the development of international cyber norms vis-à-vis liberal democracies' understanding of cybersecurity. This point is captured well in the following analysis of the recent 2018 election in Cambodia where "[j]ust as various countries in the developing world – including Cambodia – served as locations for proxy wars between the US and the Soviet Union and their respective allies during the Cold War,

Cambodia is once again functioning as the location for a new proxy war, this time with China leading the alternative to the US-led liberal world order."[5]

This article therefore argues that it is important to persist with ongoing endeavours at national and bilateral levels as well as among like-minded groupings, regional bodies, and informal mechanisms to create a regime for international cyber stability.

NATIONAL ENDEAVOURS

Regional policymakers' understanding of cyber-related issues has become far deeper and more nuanced in recent years. Not so long ago, many of these countries did not even hold national views on these questions. This means that current and future discussions on international security cyber issues will become more complex and require more time given that more experts, actors and agencies will be involved. Even in 2016, it was clear then that there is now a "new negotiating dynamic, driven by broader participation and by contending concepts of cybersecurity", which was considered likely to make reaching consensus in the 2016-2017 GGE more challenging.[6] Likewise, progress in forums such as the ARF and ASEAN will likely be affected by such broader participation. While this is likely to delay progress, it is also a positive indicator when more states continue to become involved in shaping the development and implementation of cyber norms and CBMs. For example, states such as Brunei and Singapore, which were not highly active previously in their international cyber engagement activities, submitted national views on how to implement norms to the UN Office for Disarmament Affairs (UNODA) in 2017.

Such endeavours thus provide opportunities for these states to take ownership of the agenda, especially where they may not have been members of previous GGEs. Prime Minister Modi earlier argued that the voices of many rather than the few should shape the agenda.[7] This type of thinking resonates in the cyber stability agenda where more countries should ideally become involved in this process of developing rules of responsible state behaviour. Even with an uptick in state sub-

[5] Alvin Cheng-Him Lim, "The Spiral Repetitions of Cambodia's 2018 General Election", Asia Dialogue, http://theasiadialogue.com/2018/08/09/the-spiral-repetitions-of-cambodias-2018-general-election/, 9 August 2018, accessed 10 August 2018.

[6] James Lewis and Kerstin Vignard, "Report of the International Security Cyber Issues Workshop Series", UNIDIR and CSIS, 2016, 11.

[7] Author observations, Raisina Dialogue, "The New Normal: Multilateralism with Multipolarity", Observer Research Foundation, New Delhi, 17-19 January 2017.

missions from the region (such as Singapore and Brunei) to UNODA, more states, including smaller states, can hopefully become more involved.

A number of countries in the Asia Pacific continue to make considerable efforts to champion aspects of the international cybersecurity. Malaysia was a member of two GGEs, and for many years it has advocated regionally for transparency as a means to contribute to confidence building as well as support for CBMs. It has done so through efforts such as co-hosting several ARF workshops on CBMs and capacity building, as well as publishing new cybersecurity strategies that outline how it intends to position itself internationally and regionally. Countries like Japan, the United States, Australia, and China, among others, are particularly active in terms of international engagement (although US diplomatic engagement in multilateral forums has lessened in the wake of the Trump administration). The United States and Australia have devoted much time to regional engagement through, for example, workshops on CBMs and capacity building endeavours. Once Japan organised itself nationally, it too has become highly active in international and regional engagement. In particular, the country has shown regional leadership in its work on technical capacity building, cyber capacity building and norms, including work with ASEAN members on capacity building. The Japan Computer Emergency Response Team (JPCERT) is also considered to be a leader in the region.

Indonesia and Korea have both been members of former GGEs on a number of occasions. Korea participated in the last four GGEs, and it hosted the Global Cyber Space Conference in 2015. The country continues its work in this space through initiatives such as driving regional awareness of the latest GGE proceedings in East Asia, and interregional workshops. Smaller states such as Singapore became highly active in their international engagement in recent years – launching, for example, a regional cyber capacity building programme in support of norms and CBMs implementation as well as leveraging regional institutional mechanisms like ASEAN for global influence.

Likewise, while India has become more engaged with broader global order issues in recent years, scholars note the country's ambitions to be a stabilising influence in the world system by being a rule-setter and security provider in contested spaces such as cyberspace and sensitive technologies.[8] It was, for instance, a member of the 2016-2017 GGE, and it hosted the 2017 iteration of the Global Conference on Cyber Space (GCCS). India also became a Co-Chair of the Global Forum on Cyber Expertise (GFCE). These types of activities are important given that countries like

[8] Ibid.

India and China have such large populations that they can have a significant effect on the global digital ecosystem.

Even with a swell of regional activities in this field in recent times, it is still the case, however, that cybersecurity and information security may not be a priority issue in other countries in the region such as Cambodia. There is a well-known regional developmental and digital divide, which means there is significant diversity in terms of cyber maturity (there is even an urban-rural digital divide within countries like India and China). This divide between countries like Cambodia, Myanmar, Laos and Vietnam and other Asian countries is particularly evident in regional institutional groupings like ASEAN and the ARF. Several Southeast Asia countries are still figuring out how to communicate effectively domestically (between government ministries and agencies) which can thus impact international cooperation. This situation is exacerbated by the ongoing need to continue coordinating national level policymaking and the integration of fast-developing technologies within those policies. These uneven levels of capacity could also affect the consensus required for future progress within regional institutional mechanisms such as ASEAN, thus affecting its collective ability to inform the global cyber norms discussion. Moreover, debates continue about the impact of such digital divides and lack of capacity to address attacks upon states' international obligations.

As it stands, Asian states' varying understanding of cybersecurity and what they perceive to actually constitute a cyber threat will continue to shape their domestic priorities (security interests also vary widely between countries in the region). This will continue to impact attempts to find common ground and different interpretations of norms. In addition, infrastructure needs, concerns about non-interference in internal affairs, geopolitical support, and regime changes are factors that can impact international and regional cybersecurity developments such as capacity building, or the consensus needed in forums like ASEAN. For instance, the Duterte regime seems more willing to realign towards China in exchange for infrastructure investment at the expense of America (even with the state's traditional alliance with the United States).[9] The Philippines has been Co-Chair of the ASEAN Defence Ministers' Meeting-Plus Expert Working Group on cyber, and there have been occasions where officials were not authorised to attend regional cyber events. This could impact regional efforts to enhance transparency and trust by building communities of interest through regular meetings and conferences. Indonesia, too, has been willing to receive infrastructure investment and diplomatic support from

[9] See "The Rise of Duterte: A Populist Revolt against Elite Democracy" by Richard Heydarian for more information about the impact of the rise of China.

China. In return for geopolitical support (such as Cambodia's advocacy in ASEAN for China's position on the South China Sea dispute) China has apparently provided aid and investment as well as support when Cambodia faced United States and European sanctions for human rights violations.[10] The country also apparently received from China "US$20 million worth of support for the 2018 election, 'including polling booths, laptops and computers.'"[11]

Furthermore, while concerns about terrorism and fake news have heightened globally in recent years, those regional states which understand cybersecurity as including risk to their political, military, social and cultural landscapes in addition to risk to infrastructure are particularly worried about social stability and Internet control. The heightened concerns about terrorism, and more recently fake news, have brought about an increase in the introduction of counter-terrorism and cyber legislation in the region. A key concern is whether this legislation could sometimes be introduced as a means for illegitimate content control. For example, Malaysia's introduction of a "fake news law" in 2017 just before the election is criticised as being designed to suppress criticism of former Prime Minister Najib and the ruling party at that time.[12] Another key question is how cyber capacity building should be conducted where values may not be compatible, particularly where there might be valid capacity building requests for assistance, including technical training and programmes to investigate in order to tackle violent extremism online, but a risk that these skills could be then used for surveillance.[13] Large democracies like India have the potential to provide a model for other countries where there are genuine concerns about countering violent extremism online and "fake news".

The ways in which states in Europe and the United States now choose to tackle these types of trends as well as nationalism, hate speech, freedom of expression and anti-democratic sentiments are watched closely by states in this region. Even where there is parliamentary oversight in liberal democracies to provide a system of checks and balances, they are sometimes accused of hypocrisy. This situation is not helped by the current United States administration, which is so far less attentive to democracy and human rights matters. This is leaving – has already left – a vacuum in the region (even where many countries effectively share, albeit to varying degrees, similar Confucian internal stability and social harmony concerns).

---

10 Cheng-Him Lim, "The Spiral Repetitions of Cambodia's 2018 General Election".

11 Ibid.

12 Austin Ramzy, "Hopes for New Era of Malaysia Free Speech Are High, but Pending", New York Times, 18 June 2018.

13 OSCE and Ministry of Foreign Affairs Republic of Korea, "Inter-regional Conference on Cyber/ICT Security", Background note, Seoul, 2 March 2017.

Others explain that, for now, the Chinese government seems content to quietly push its arguments on cyber sovereignty to receptive leaders, although there is some evidence that this lobbying is becoming more active given the general US retreat across a range of multilateral forums.[14] In other words, there is a perceived risk that China could provide other countries with an attractive example of a successful economic model that continues to align with its own cultural values and conception of world order. China is willing to support capacity building that aligns with its cultural and political values, and Singaporean cyber capacity building programmes also continue to reflect the country's own positions on these subjects. This article concludes that such differences between states on Internet sovereignty and information control are not likely to change in the near future.

BILATERAL AND LIKE-MINDED EFFORTS

Many endeavours at bilateral level and among like-minded groupings such as multilateral memorandums of understanding (MOUs) enable the opportunity to make progress by sharing experience, finding common ground, implementing norms that could extend to larger groups, and capacity building to support OSCE/ARF CBMs. However, such endeavours should ultimately aim to complement global efforts to support international cyber stability (and not add further uncertainty and fragmentation).

Many bilateral MOUs, such as the Singapore-Thailand MOU of 2016 to share experience, have been agreed in recent years. Joint statements such as the United States-Singapore statement in August 2016 were also successful in affirming these states' commitment to the applicability of international law to state conduct in cyberspace and commitments to promote voluntary norms of responsible state behaviour in cyberspace. Bilateral efforts can often be easier for states to make progress where, for example, countries like the Republic of Korea may have found it easier to deal with other states bilaterally rather than regionally due to its difficulties with North Korea.

Similarly, regional countries sometimes find like-minded initiatives useful where progress on cyber issues within regional and international mechanisms such as the ARF and GGE are not seen to work effectively. In addition, steps have been taken to push the international security cyber agenda within like-minded forums

[14] Scott Shackelford and Frank Alexander, "China's cyber sovereignty: paper tiger or rising dragon?", Asia & the Pacific Policy Society, 12 January 2018, available at https://www.policyforum.net/chinas-cyber-sovereignty, accessed 11 June 2018.

such as the G7 and G20. Multilateral MOUs have also been agreed such as the Unites States-Japan-Australia-India MOU, as well as joint ministerial statements by Japan, the United States and Australia committing to coordinate in international forums like the UN GGE and ARF.[15] Singapore, too, initiated a Forum of Small States meeting on the sidelines of the previous GGE in 2017. More recently, the coordinated joint United States-United Kingdom statement regarding Russian malicious cyber activities affords an opportunity for other states to join with the goal that a large enough group of nations that feel and act the same way about acceptable and unacceptable behaviour can use that coalition to put pressure on those who are not behaving the way they should.[16] The recent coordination of international attribution is both an example of like-minded groups sending a deterrent message, while also affording other states the opportunity to join them in agreeing upon acceptable state behaviour. Likewise, there are regional calls to bring groups of developing countries together on key issues given the apparent need for a more equitable dispersal of power – this may become even more apparent in the field of cyber where countries like China cite concerns about developing countries in cyber negotiations.

These types of activities further provide an example of broader world order trends identified by intelligence communities whereby a future international environment of competition and cooperation among major powers will probably result in "ad-hoc approaches to global challenges that undermine existing international institutions".[17] Nonetheless, this article finds that while like-minded initiatives can help to make progress in this field, states should ideally work to ensure that these endeavours do not cause further uncertainty and fragmentation that is "insulting to global norms".[18]

---

[15] Office of the Spokesperson, "Joint Statement of the Japan-United States-Australia Trilateral Strategic Dialogue", United States Department of State, 25 July 2016.

[16] Levi Maxey, "Russia Hacks Its Way to the High Ground of the Internet", The Cipher Brief, 16 April 2018, available at https://www.thecipherbrief.com/article/tech/u-s-uk-blame-russia-probing-internet-routers-globally?utm_source=Join+the+Community+Subscribers&utm_campaign=83d511a588-EMAIL_CAMPAIGN_2018_04_17&utm_medium=email&utm_term=0_02cbee778d-83d511a588-122471557&mc_cid=83d511a588&mc_eid=c1f2be183c, accessed 12 June 2018.

[17] United States Office of the Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community", Senate Armed Services Committee, James R. Clapper, Director of National Intelligence, 9 February 2016, available at https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf, accessed 8 June 2018, p. 16.

[18] Healey, "Triggering the New Forever War, in Cyberspace".

REGIONAL SECURITY ARCHITECTURE

The regional level is sometimes considered to be more suited to implementation of norms and CBMs whereas the global level is more suited to agreements and norms. A robust regional security architecture supported by activities in groupings such as ASEAN, the ARF, East Asia Summit (EAS), ASEAN Defence Ministers' Meeting (ADMM), Shanghai Cooperation Organisation (SCO) and BRICS are often considered important for international and regional stability. The OSCE, Organization of American States (OAS), and ARF have already made some progress in building common understanding and identifying cyber CBMs for regional application – for example, the OSCE's 16 CBMs and the ARF Workplan which aim to operationalise international cybersecurity norms (the ARF has particular strategic importance given the membership of major powers such as the United States, China, Russia, India and Japan, even where this diverse membership could make it more difficult to find common ground).

The Heads of State or Government of the ten ASEAN members and the United States also agreed the Sunnylands Declaration in early 2016 where they committed to promote security and stability in cyberspace consistent with norms of responsible state behaviour. The 2017 ASEAN Cybersecurity Cooperation Strategy was later agreed under Singapore's vice-chairmanship of the ASEAN Network Security Action Council to focus on norms and a cooperation and capacity building framework. The strategy's aim to coordinate cyber policies across the many forums in ASEAN's political-security, economic, and socio-cultural community pillars is significant insofar as it will hopefully support international cooperation. However, it is expected that strategy and international cooperation matters will be examined through the Telecommunications and IT Ministers Meeting (TELMIN). This may not be the best forum to make progress on strategic and security issues, like norms development, especially where the TELMIN and political-security communities can often differ in their understanding of, and approach to, cybersecurity issues. For similar reasons, the ARF Inter-Sessional Meeting (ISM) on cybersecurity was recently established. By continuing to hold these cyber discussions under the ISM on counterterrorism and transnational crime, it could potentially affect how norms and strategy would develop.

Developing and implementing CBMs is considered urgent over the short to medium term in this field to reduce near-term risk by dealing with issues related to misperception and miscalculation. This should ideally reduce the potential for conflict by providing de-escalation mechanisms, especially where it is difficult to assess

or count cyber capabilities.[19] There is an identified need for better communication and coordination between states (as well as across national governments), and a real necessity to move beyond awareness-raising on CBMs to actual implementation and follow-up after meetings.[20] Much awareness-raising has taken place in ARF and ASEAN meetings in recent years, but little progress on concrete implementation. This is particularly important where CBMs and capacity building can assist states to find common understanding of their normative commitments.

Regular meetings and practical exercises (such as the table-top exercises previously held in ARF, OSCE and ASEAN meetings) can continue to assist this process of building capacity and confidence.[21] In terms of capacity building, many states in the region are still challenged by the speed of technological changes, they often lack technical capacity and gaps in the law persist, which is hindering international cooperation and exchange of good practice. GGE experts agree that capacity building is essential for both cooperation and confidence building.[22] Singapore's ASEAN Cyber Capacity Programme has thus included a number of regional workshops on CBMs, capacity building and norms, including the first formal ASEAN workshop on norms in May 2017. The goal is to provide resources, expertise and training to enable ASEAN members to more proactively participate in the international cybersecurity agenda. The country also launched the annual ASEAN Ministerial Meeting on Cybersecurity in 2016 to identify ways to increase cooperation and continue the development of norms in ASEAN states. These initiatives seem to have helped to pave the way for Singapore to present ASEAN's perspectives at the global level through the ASEAN statement to the UN at the end of 2017, thus contributing to the international cyber stability agenda.

Some of the OSCE and OAS work on CBMs could also provide good practices for other regional bodies such as the ARF, while successful ARF confidence building table-top exercises were introduced within OSCE meetings. There is space to further increase such examples of cross-regional exchange of good practices and interregional cooperation (although the work within these regional forums is far from done). Interregional cooperation can work towards ensuring complementarity

---

[19] Author observations, "ASEAN Cyber Norms Workshop", Singapore Cyber Security Agency, 8-9 May 2017.

[20] Ibid.

[21] Author observations, "Australia-Singapore Cyber Risk Reduction Workshop", Singapore Cyber Security Agency and Australian Department of Foreign Affairs, 6-7 December 2017.

[22] UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, Summary.

globally so that measures within regional bodies like the ARF and ASEAN do not evolve in such different directions that they cause further fragmentation. Some recent examples of efforts to identify and promote synergies between different regional efforts in order to promote global cyber stability include the joint OSCE and Ministry of Foreign Affairs of the Republic of Korea Inter-regional Conference on Cyber/ICT Security in 2017, where Korea and Thailand offered to be bridges between the OSCE and Asia region.

Such interregional efforts (and even bilateral capacity building) could be hampered by incompatible state views on cyberspace governance though, particularly where ASEAN states often hold different perspectives on internal stability, content control and sovereignty. It is unlikely that such views would affect intra-ASEAN cooperation or engagements with countries like China, which continues to promote its notions of cyber sovereignty. Rather, such views could impede capacity building efforts with the EU, for example, or bilaterally with countries like Australia.

Lastly, informal regional mechanisms such as academia, research institutes and Track 1.5/Track 2 diplomatic mechanisms have played a fruitful role to date in forging progress in the region. These informal mechanisms can continue to enable progress where formal international and regional mechanisms such as the GGE or ARF may not be successful or are slow to make progress. Such initiatives can sometimes provide the space for policymakers to increase their understanding of key questions, and it can help to build networks and communities of interest in an informal environment. Findings within academia and informal deliberations can often inform the Track 1 decision-making process further down the line. There is still room for more independent insights and fresh ideas that can be produced through papers, and informal roundtables or workshops with concrete scientific questions about ways to transition to the next phase of international and regional security discussions. However, governments should avoid politicising institutes and analysts in order to avoid the criticism of the previous GGE where experts were described as proxies for negotiations rather than expert consultations. In short, as Richard Haass surmises, in order to forge further progress in this field currently, smaller consultations with critical governments, companies and NGOs are likely to achieve more than large formal gatherings of countries.[23]

[23] Richard Haass, *A World in Disarray: American Foreign Policy and the Crisis of the Old Order,* (New York, New York 2016), 247.

CONCLUSION

This article examines the contribution of Asia Pacific states to a regime for international cyber stability, including promoting common views and implementation of norms of responsible state behaviour in cyberspace, CBMs and capacity building. It argues that it is important to persevere with ongoing endeavours at national and bilateral levels as well as among like-minded groupings, regional bodies, and informal mechanisms. Recognising, however, that this process will take time. This is particularly the case since more state actors and experts are now involved, differences about the very understanding of cybersecurity persist, and high geopolitical tensions are slowing progress.

Even though regional states are fully cognisant of their economic self-interest in cooperating, ongoing geopolitical tensions are detracting from the political willingness needed to make progress. Both globally and regionally, major power rivalry, rising nationalism as well as challenges to the rule of law and international human rights obligations are making it even more difficult to find common ground on state behaviour in cyberspace. Within the Asia region itself, countries vary in terms of cultural and political values, including different conceptual understandings of world order and cybersecurity. These dynamics will continue to impact international cybersecurity issues. Moreover, there is clear dissatisfaction with the current order and rising powers like China also have ambitions in order building, evidenced by states' willingness to use cyber-enabled influence operations and engage in low-level activities without resorting to the use of military force and without fear of significant retaliation.

The article finds that, although it may lead to delays, it is better that more states in the region are becoming, and continue to become, involved in shaping the regional and global agenda. Several countries are continuing their efforts to create an international regime for cyber stability, and countries such as India and China can have a significant impact on the global ecosystem. Nevertheless, there is a developmental and digital divide, and several countries do not even consider cyber-related issues to be a national priority. Such diverse levels of cyber maturity can make international and regional cooperation more difficult. This is exacerbated by a situation whereby infrastructure needs, concerns about interference in internal affairs, geopolitical support and regime changes further impact the ability to make progress or forge the consensus that is often needed in regional institutional mechanisms like ASEAN.

Moreover, global concerns about terrorism and fake news mean that regional states are also introducing initiatives to address their social stability and Internet

control worries. Even where this has led to concerns about excessive (and illegitimate) content control, the ways in which the United States and European states are dealing with these problems as well as nationalism, hate speech, freedom of expression and anti-democratic sentiments are watched closely for examples of hypocrisy. Although many countries share similar social harmony concerns, the inattentiveness of the current United States administration to democracy and human rights is leaving a vacuum in the region. That said, this article finds that Internet sovereignty and information control differences will likely persist.

Numerous bilateral initiatives such as MOUs and like-minded efforts are helping to make progress where regional and international mechanisms like the GGE and ARF are sometimes ineffective by finding common ground, exchanging experience, and implementing norms that can extend to larger groups. Ideally, these efforts should aim to support global initiatives and avoid causing further fragmentation by creating ad-hoc approaches that undermine existing international institutions.

Given the importance of a strong regional security architecture for international and regional stability, continuing with the ARF and OSCE initiatives to build common understanding and implement cyber CBMs regionally is essential. As is the more recent push in ASEAN for better coordination and greater attention to norms, CBMs and capacity building, which should hopefully also contribute to international cyber stability. A lot of awareness raising has been conducted already, however, with fewer examples of concrete implementation of CBMs and meeting agreements. While these regional forums still have a long way to go, there is also room for more cross-regional exchange of good practices. This can help to avoid a situation where regional bodies evolve in very different directions and thus add more uncertainty and instability (although interregional and bilateral initiatives may be hindered by incompatible state and regional views on issues such as internal stability). Lastly, informal diplomatic mechanisms and academic initiatives can continue to help make progress by examining ways to transition to the next phase of regional and international security discussions.

Caitríona Heinl is Lead Strategist for Asia Pacific at EXEDEC. She was previously responsible for policy under the NTU Cyber Risk Management project, having transferred from the S. Rajaratnam School of International Studies (RSIS) Centre of Excellence for National Security at NTU Singapore where she worked as Research Fellow on international cybersecurity issues from 2012 to 2018.