2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level

Nikolas Ott*
Transnational Threats Department,
Co-ordination Cell
Organization for Security and
Co-operation in Europe (OSCE)
Vienna, Austria
nikolas.ott@osce.org

Anna-Maria Osula, PhD**
Guardtime / TalTech / Masaryk
University
Tallinn, Estonia
annamaria.osula@guardtime.com

Abstract: While States did not reach consensus on the 2017 report by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), the UN remains a core platform for diplomatic deliberations on international law, norms and principles for responsible state behaviour.

At the same time, regional organisations play an increasingly important role in stabilising State relations in cyberspace. Their relevance is also recognised in the new UN GGE mandate for 2019-2021. For the first time, the UN GGE negotiations include a formal way of embracing regional cyber expertise, knowledge and concerns, albeit they are ambivalent about how the envisaged input will be incorporated into the UN GGE process.

The paper argues that regional organisations should and are willing to increase their substantial input to the global debates on international cyber stability. Specifically, we analyse the benefits of the work of the Organization for Security and Co-operation in Europe (OSCE), the Organization of American States (OAS) and the Association of

* The opinions expressed in this article are those of the authors alone and are not representing the official policy of any organisation or other entity.

** Dr Anna-Maria Osula's contribution to this paper is based on research supported by Masaryk University project no. CZ.02.1.01/0.0/0.0/16_019/0000822 (C4E).

Southeast Asian Nations (ASEAN), undertaken in the context of Confidence-Building Measures (CBMs). In addition to global platforms, we see great potential in inter-regional collaboration.

Moreover, the paper points out a number of suggestions which would enhance the inclusion of regional organisations' efforts into UN GGE; and potentially, also into the Open-Ended Working Group (OEWG) negotiations. More effective norm development and CBM implementation can be achieved by carefully assessing the pros and cons of various venues and formats as well as taking advantage of existing synergies between UN initiatives and regional CBM and capacity-building initiatives. Regional organisations have better insights into national or regional priorities; while domestic implementation frameworks may be developed by regional organisations for faster CBM and norm implementation procedures, and possibly allow for additional funding for priority areas. Regional roadmaps should be developed for more effective norm and CBM development, while joint implementation efforts could foster the global uptake of norms. Furthermore, regional organisations may serve as incubators for new ideas and share valuable experience of lessons learned.

Keywords: *UN GGE, OSCE, OAS, ASEAN, regional organisations, cyber security, cyber security strategies, capacity-building, confidence-building measures, cyber norms*

1. INTRODUCTION[1]

The failure to reach consensus on the 2017 report by United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) reflects the widening gap between States' visions on how to achieve a secure and stable cyberspace. Simultaneously, recent incidents highlight how States are further developing and increasingly deploying destructive cyber capabilities. Combined with the ongoing dispute over norms, rules, and principles for responsible State behaviour, there is an increasing risk of unintended military escalation. Therefore, a new perspective toward stabilising cyberspace is necessary.

It may be argued that due to the cross-border nature of cyber threats, regional solutions become less relevant. However, this article posits quite the opposite: namely, that regional governmental organisations[2] play a crucial role in tackling

1 The authors are grateful to the anonymous reviewers for their comments. Special thanks also goes to Christoph Berlich, Ingmar Snabile, Henry Rõigas, Jessica Zucker and Kerry-Ann Barrett for their comments and feedback throughout the drafting process.

2 This paper focuses exclusively on regional (inter-)governmental organisations and therefore uses the term 'regional organisations' as a shorter substitute thereof.

concerns related to cyber security. Their active input on the international level has the potential to contribute to 1) more effective and targeted norm development by taking advantage of existing synergies between the UN and regional organisations; 2) faster implementation procedures on the regional and national level through targeted and customised support; 3) more coherent inter-regional co-ordination of agreed stability efforts through inter-regionally co-ordinated, but regionally implemented roadmaps and frameworks; and 4) capacity-building and awareness raising. Thus, further incorporation of regional voices in reaching a global agreement on the content, interpretation and implementation of the norms of State behaviour, confidence-building measures (CBMs) and capacity-building is essential.

However, their presence at global venues has so far been limited. This is mostly due to regional organisations having a specific mandate tailored toward activities within their respective regions. This limits the extent to which they may engage in other international fora and partly explains why regional organisations are rarely present at the international negotiating table.[3] In fact, the UN GGE 2019-2021 is the first UN entity venue which now includes a formal way of embracing regional cyber expertise, knowledge and concerns.[4] This development should be applauded and will hopefully mark a trend of further inclusion of regional organisations and their Member States' concerns and suggestions. However, besides mentioning the additional consultations with regional organisations in the resolution, it remains unclear how the envisaged regional organisations' input will be incorporated into the UN GGE negotiations. Furthermore, there is no indication on whether this consultation process will lead to a regular substantive exchange between the global and regional levels. There are also doubts regarding overcoming the different views which stalled progress on the previous UN GGE consensus report.

Against this background, the paper investigates mechanisms for further involving regional organisations in cyber security policy deliberations within the UN. The paper analyses selected regional organisations' activities and documents related to norm-building and CBMs. In order to narrow our scope, we focus on selected regional organisations' prominent role in agreeing upon and implementing CBMs and discuss how these initiatives could better support ongoing work on norm-building.

Our paper is structured as follows. After a brief introduction to the current UN GGE process and status quo, it analyses CBM-related developments undertaken at regional venues such as the Organization for Security and Co-operation in Europe (OSCE), the Organization of American States (OAS) and the Association of Southeast Asian Nations (ASEAN). We also reference some capacity-building efforts and norms

3 The European Union is an exception among regional organisations given its unique competencies and governance model. Therefore, the authors have decided to exclude the EU as a case study from this article.

4 United Nations, Advancing responsible State behaviour in cyberspace in the context of international security, Resolution adopted by the General Assembly on 22 December 2018, A/RES/73/266, p 4, available at: https://undocs.org/A/RES/73/266.

discussions when they relate to regional CBM activities in the respective regions. We then outline opportunities through regional organisations' efforts on CBMs as well as the increasing role and inter-connectedness of regional organisations. After that, cross-cutting benefits of inter-regional collaboration are discussed. Finally, we conclude by proposing practical options for further including representatives of regional organisations into global processes.

2. UN GGE STATUS QUO

The UN GGE is the most reputable platform for agreeing international norms for States in cyberspace. Since 1998, when the Russian Federation first introduced a draft resolution on information security in the First Committee of the UN General Assembly,[5] the UN Secretary-General has issued annual reports with the views of UN Member States to the General Assembly.[6] Additionally, UN GGEs have been formed in 2004/5, 2009/10, 2012/13, 2014/15, and 2016/17, with a total of three consensus reports (in 2010, 2013 and 2015) examining the existing and potential threats from cyberspace, and possible co-operative measures to address them.[7]

In the latest development, in November 2018, the UN First Committee (Disarmament and International Security) approved two separate proposals to create working groups which would develop rules for responsible State behaviour in cyberspace. These were later adopted by the UN General Assembly. The first initiative, proposed by the Russian Federation, was to form an open-ended working group (OEWG) in 2019, "acting on a consensus basis to further develop the rules, norms and principles of responsible behaviour of States".[8] The second suggestion, tabled by the United States (US), was to continue the previous UN GGE efforts in order to study "possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States".[9]

The tension between these two proposals is evident. On the one hand, the US claimed that the Russian proposal "imposes a list of unacceptable norms and language that

5 United Nations, Resolutions adopted by the General Assembly, 4 January 1999, A/RES/53/70.

6 United Nations Office for Disarmament Affairs, Developments in the field of information and telecommunications in the context of international security, available at: https://www.un.org/disarmament/topics/informationsecurity/.

7 The UN GGE convened in 2009 reached no consensus report. However, reports were published in 2010 (A/65/201), 2013 (A/68/98*) and 2015 (A/70/174). The UN GGE convened in 2016 did not reach a consensus report. UNODA fact sheet, available at: https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf.

8 United Nations, Developments in the field of information and telecommunications in the context of international security, Resolution adopted by the General Assembly on 5 December 2018, A/RES/73/27, available at: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27.

9 Footnote 4.

is broadly unacceptable to many States",[10] with other commentators adding that the text "departed from previous year's versions and included excerpts from the Group of Governmental Experts reports in a manner that distorted their meaning and transformed the draft resolution".[11] On the other hand, the Russian Federation argued that the working group proposed by the US would take the "international community backwards and result in a complete waste of resources, also being the product of extremely narrow interests of Western countries, especially the United States".[12]

One of the focal issues in this debate and a point of critique towards previous UN GGE processes is the selection of participating States. The number of countries involved in the UN GGE process has, over time, risen from 15 to 25, which reflects general aspirations of including a wider range of States, and eventually a hope for bigger buy-in to the agreed principles. At the same time, more members may also mean lengthier discussions and increased difficulties in reaching a consensus.

Both previously mentioned initiatives proposed to the UN General Assembly in 2018 touch upon including further stakeholders. The US proposal specifically requested the UN GGE meetings to be preceded by two two-day, open-ended, informal consultative meetings, so that all Member States could share their views, which the UN GGE Chair would then convey to the group of governmental experts for consideration.[13] In the same vein, the proposed OEWG has promised to take the negotiating process to a "higher level that is more inclusive, open and democratic"[14]; and has also asserted the possibility of holding inter-sessional consultative meetings with representatives of business, non-governmental organisations and academia, to share views on the issues within the group's mandate.[15]

3. UN GGE AND REGIONAL ORGANISATIONS

It is against this background that our article will look into the role of regional organisations in shaping the international norms for States in cyberspace. We will examine the UN GGE reports published in 2010, 2013 and 2015, to analyse how the role of regional organisations has developed.

Regional organisations and initiatives have always been an integral part of the reports. All three reports recognise the valuable work undertaken by regional entities;[16] we can

10 United Nations, First Committee approves 27 texts, including two proposing new groups to develop rules for States on responsible cyberspace conduct. Meeting coverage, GA/DIS/3619, 8 November 2018, available at: https://www.un.org/press/en/2018/gadis3619.doc.htm.
11 Id.
12 Id.
13 Footnote 4, p 5.
14 Footnote 10.
15 Footnote 8, p 5.
16 e.g. UN A/65/201 (2010) p 13; UN A/68/98* (2013) p 4, 14; UN A/70/174 (2015) p 35.

observe an increasingly substantial role being foreseen for the regional organisations.

This can be best seen in the UN GGE report of 2015, which finely outlined the areas where different actors should provide input in achieving international peace and security in cyberspace. The report established a detailed four-pillar system for guaranteeing cyber stability between States, made up of: a) the applicability of international law; b) norms, rules and principles for the responsible behaviour of States; c) CBMs; and d) capacity-building enhancing international co-operation.[17]

For example, similar to the conclusions adopted in 2013, the 2015 report recognised the importance of regional organisations in developing and implementing CBMs such as exchanging views and information, providing more transparency, enhancing common understandings and intensifying cooperation.[18] Equally relevant were regional efforts in capacity-building, such as securing ICT use and ICT infrastructures, strengthening national legal frameworks, law enforcement capabilities and strategies; combatting the use of ICTs for criminal and terrorist purposes, and assisting in the identification and dissemination of best practices.[19]

The 2015 report noted separately that the "development of regional approaches to capacity-building would be beneficial, as they could take into account specific cultural, geographic, political, economic or social aspects and allow a tailored approach".[20] Also, both the 2013 and 2015 reports clearly point out that the UN should encourage regional efforts,[21] and recommend regular dialogue through regional forums.[22] In 2015, the report puts specific focus on increased co-operation at regional and multilateral levels to "foster common understandings on the potential risks to international peace and security".[23]

The most significant development in engaging regional efforts within the UN GGE process was put forward through the US proposal for a new UN GGE in 2018. The Office for Disarmament Affairs of the Secretariat was invited to collaborate on behalf of UN GGE members and through existing resources and voluntary contributions, with relevant regional organisations, such as the African Union (AU), the European Union (EU), the OAS, the OSCE and the ASEAN, via a series of consultations: with the aim of sharing views on the issues within the group's mandate in advance of its sessions.[24]

17 For more information on the general purpose and conceptual underpinnings of CBMs as well as linkages between the four pillars, see Patrick Pawlak, "Confidence-Building Measures in Cyberspace: Current Debates and Trends", in *International Cyber Norms: Legal, Policy & Industry Perspectives*, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016.
18 e.g. UN A/68/98* (2013) 26a, 26b, 29; UN A/70/174 (2015) 16b-16d, 17, 18.
19 UN A/68/98* (2013) p 32a.
20 UN A/68/98* (2013) p 22.
21 e.g. UN A/68/98* (2013) p 13; UN A/70/174 (2015) p 35.
22 UN A/68/98* (2013) p 29; UN A/70/174 (2015) p 18.
23 UN A/70/174 (2015) p 30b.
24 Footnote 4, p 4.

This can be interpreted as an acknowledgment by States that the UN GGE process needs to be more inclusive and can benefit from stronger engagement of regional expertise. At the same time, the envisaged procedures are proof of the readiness of regional organisations to play a greater role in enhancing confidence between States as well as global norm- and national capacity-building. Indeed, as will be illustrated in the remainder of this article, there is a clear interest of regional organisations in contributing to enhanced trust and confidence among States, as well as reaching an understanding on acceptable and unacceptable State behaviour in cyberspace.

4. OPPORTUNITIES THROUGH REGIONAL ORGANISATIONS' EFFORTS ON CONFIDENCE-BUILDING MEASURES

The inter-connectedness of the four-pillar approach presented in the UN GGE 2015 report has provided the groundwork for increased involvement of regional organisations. These four pillars as a whole can be understood as cyber stability mechanisms which are only effective if they reinforce each other. For example, norms of responsible State behaviour require to be put into practice to ensure buy-in. CBMs serve exactly this purpose by translating broader legal concepts into more concrete, straightforward actions. As the following chapter will extensively outline, regional organisations are also uniquely equipped to develop and implement CBMs which are not directly linked to norms, rules and principles for responsible State behaviour; but instead are more pragmatic and practical by design, thereby developing the foundational groundwork for enhanced communication, transparency and collaboration. Moreover, CBMs only serve their purpose to the fullest extent if they are implemented, which requires the capacity to do so. The following paragraphs will outline how CBMs are connected to and reinforce the other pillars; and why this is important in securing the success of global agreements.

4.1. THE MUTUALLY REINFORCING ROLE OF CBMS IN GLOBAL NORM-BUILDING

While developing norms, rules and principles for the responsible behaviour of States is vital, States need to have confidence that others will adhere to the same rules. This might sound trivial, but it requires a high level of co-operation among States. Given their more practical and concrete design, CBMs serve as pragmatic mechanisms in crisis situations. They can therefore be employed as measures to address norms or rules violations. CBMs are thus critical components of any cyber stability mechanism. Nevertheless, it is important to note that even the most advanced set of CBMs will

not stop an intentional conflict; but they can stop an unintentional one by stopping or slowing down the spiral of escalation.

While norms and responsible State behaviour are discussed on the global level, CBMs tend to be developed on a regional or national level. This difference makes a lot of sense when reviewing the purpose of norms of responsible State behaviour and CBMs respectively. Ideally, norms of responsible State behaviour should not be subject to extensive interpretation, while CBMs leave more room for adjustment and allow for the inclusion of already existing regional or national procedures. This therefore allows for greater customisation and adjustment for regional needs. Regional organisations such as the OSCE, OAS and ASEAN Regional Forum (ARF) have engaged in this path and developed or are developing their respective sets of cyber/ICT security CBMs. In comparison with the EU, these three regional organisations bring together States that sometimes have difficult relations.[25] This is an important characteristic, as cyber stability needs to be built between non-like-minded States, not just geopolitical allies. Furthermore, in the context of the UN GGE process, if certain proposals are already supported or even initiated by regional organisations, there would automatically be a bigger buy-in during the UN GGE process in finding a consensus.

In addition to proposing and agreeing to norms, regional organisations benefit from their accumulated political capital in implementing practical measures. This aligns perfectly with the purpose of CBMs and helps drive their operationalisation forward. Third, regional organisations can consult, learn from and bridge different cultural and political approaches to cyber/ICT security. These three characteristics provide an excellent platform for regional organisations to address global cyber security challenges through explicitly regional means.

Additionally, there is a shared interest among nations in keeping the diplomatic process on cyber stability measures alive. Having multiple platforms across regions will help to test, for example, how States may practically implement norms. However, even though the cyber CBMs of the 21st century may share the same name as arms control CBMs of the Cold War era, their purpose and design is quite different;[26] 21st century CBMs are about "building areas of common understandings and practical cooperation among nations, including preparations for crisis management".[27] Large-scale cyber security incidents tend to spread fast, are normally trans-national; and most of the time, difficult to predict or anticipate. If States are to deal with such features, established practice, trust in each other and confidence that others will come to their support is needed.

25 OAS can be considered as the most 'like-minded' group among the three of them.

26 James A. Lewis, Confidence Building Measures in Cyberspace, Presentation to the Inter-American Committee Against Terrorism (CICTE) of the Organization of American States, Center for Strategic and International Studies, February 26, 2016, p 1, available at: https://www.oas.org/en/sms/cicte/Documents/2016/Speeches/JAMES%20LEWIS%20CSIS.pdf.

27 Id.

For this very reason, if one considers norms as means to establish and enhance trust and confidence amongst nations, it seems obvious that a discussion on norms needs to be complemented with practical considerations that foster an environment of collaboration and support amongst nations. This can be achieved by implementing agreed norms and CBMs into practical considerations that have a positive impact on nations' relations and interactions. Only through practice will nations eventually reach a level of trust and confidence, leading them to move negotiations on more delicate cyber security issues forward.

All three regional organisations discussed here have now adopted some CBMs and are currently discussing additional ones.[28] Member States have come a long way towards agreeing on these different sets of CBMs; but in order to put them in practice, national policy structures and capacities need to be in place. This process is commonly referred to as implementation and requires commitment from involved States, and support of external experts and consultants.

Given current emphasis on implementation across the regions, it is important to critically review how it can be most effective and achieve the desired results. A significant component of successful implementation involves proper guidance and assistance by a neutral actor with sufficient cyber security expertise, as well as knowledge about the respective nation. Given their long-standing engagement in the respective regions, the OSCE, the OAS and the ASEAN are uniquely equipped to provide customised support and guidance on the regional and sub-regional levels. Moreover, regional organisations have been a perfect platform for bridge-building exercises[29] like this for quite some time. However, targeted capacity-building needs to be provided on the national level to ensure proper engagement in CBMs. Workshops are one way of solving this issue; but raising the implementation rate of cyber CBMs requires a whole-of-government approach.

Capacity-building efforts on the working level might only have a small impact on the CBM implementation process due to the lack of awareness amongst high-level politicians and policymakers. While cyber security is widely covered in many media outlets these days, there still seems to be a certain degree of scepticism among high-level politicians and policymakers about the policy component of cyber security. Moreover, given that cyber security is a cross-cutting issue, normally addressed by several ministries, sometimes division of labour is unclear or not clearly defined. Most nations have national cyber security strategies or other strategy documents that explicitly address these issues. This is a starting point for any international effort to further enhance cyber stability, such as CBMs or norms of responsible State behaviour.

28 The OSCE is an exception here, as the set of 16 CBMs is already quite advanced there. Discussions on a third set are therefore not a priority at this point.

29 See following sub-chapter for a series of examples.

One way to facilitate enhanced implementation would therefore consist of its inclusion and clear reference in national strategy documents, such as cyber security strategies or defence strategies. This has the positive side-effect of helping nations better read each other, which already constitutes a confidence-building activity *per se*. Some regional organisations, such as the OAS, have been extensively involved in the development of national cyber security strategies. Synchronising such activities with the UN GGE process and other regional organisations would provide ample potential to further increase the impact of UN GGE reports, as well as harmonise national, regional and international efforts on cyber/ICT security.

The following sub-chapters will provide a summary of the OSCE, OAS and ASEAN/ARF CBM- and norm-related efforts, with a view to subsequently outlining how they connect to each other, as well as to the global discussion on the UN level.

4.2. ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE)

The OSCE has engaged in cyber/ICT security CBMs since 2013; and has passed two sets of CBMs, and two Ministerial Council Decisions[30] on cyber/ICT security. It continues to be a platform used by nations with significantly diverging interests due to its focus on practical measures rather than international policy or law components, which are traditionally covered by the UN. Thus, despite the ongoing political tensions between participating OSCE States, cyber/ICT security continues to be addressed by it, most recently through a series of sub-regional capacity-building and awareness raising workshops.[31] Just like the CBMs as a whole, these events are aimed at reducing tension between States by enhancing transparency, fostering collaboration and building trust.

As a first step, the OSCE set up an Informal Working Group in 2012.[32] This provided a platform to engage in structured, but still informal, discussions on CBMs. The first set of OSCE CBMs (2013) established official Points of Contact (PoC) and communication lines to prevent possible tensions resulting from cyber activities.[33] The second set (2016) focussed on further enhancing co-operation between

30 OSCE, Ministerial Council Decision No. 5/17 in 2017, available at: https://www.osce.org/chairmanship/361561 and Ministerial Council Decision No.5/16 in 2016 - available at: https://www.osce.org/cio/288086.

31 OSCE, Press release: OSCE organizes sub-regional training event on cyber/ICT security in Astana, 12 December 2017, available at https://www.osce.org/secretariat/362201; OSCE, Press release: OSCE co-organizes sub-regional training course in Bucharest on role of information and communication technologies in context of regional and international security, 28 June 2018, available at: https://www.osce.org/secretariat/386139; OSCE, Event discription: Sub-regional training on the role of ICTs in the context of regional and international security, available at: https://polis.osce.org/subregional-training-role-icts-context-regional-and-international-security.

32 OSCE, Permanent Council Decision No. 1039 in 2012, available at: https://www.osce.org/pc/90169.

33 OSCE, Permanent Council Decision No. 1106 in 2013, available at: https://www.osce.org/pc/109168.

participating States: including, for example, effective mitigation of cyber-attacks on critical infrastructure which could affect more than one participating State.[34] The 16 voluntary CBMs can be broadly categorised in three clusters: 1) *Posturing* CBMs, which allow States to "read" another State's posturing in cyberspace in order to make cyberspace more predictable; 2) *Communication* CBMs, which offer opportunities for timely communication and co-operation, including to defuse potential tensions; and 3) *Preparedness* CBMs, which promote national preparedness and due diligence to address cyber/ICT challenges.

Subsequently, the OSCE's focus has shifted from developing additional CBMs towards ensuring that all States properly implement the existing ones through practical support. This includes the use of the OSCE Communications Network "to address security of and in the use of information and communication technologies […] upon the identification of contact centres/points for cyber/ICT security-related communications within capitals".[35] Having two sets of CBMs and an extensive mandate to drive implementation forward, OSCE is focussing its efforts more than ever on making its CBMs operational through increased targeted support and capacity-building for OSCE participating States. This is highly connected to global discussions within the UN, as norms of responsible State behaviour need to be encouraged, supported and fostered through the increased implementation of the CBMs.

The OSCE has launched numerous projects to enhance CBMs. Several of these initiatives can be seen as complementing and taking forward the work being done at the UN GGE. Others may even generate ideas which have yet to be covered by UN GGE reports. For example, as a recent effort to increase ownership and targeted implementation, the OSCE launched an "adopt a CBM initiative" within the Informal Working Group in late 2017.[36] States that formally 'adopt' a CBM bring forward proposals on how to advance its respective implementation, use or impact within the OSCE community. Another development features scenario-based discussions, where government officials are exposed to the practical application of CBMs and norms of responsible State behaviour.[37]

Similarly, since 2017, the OSCE has organised sub-regional training for policymakers, technical experts and private sector representatives; and provided small-scale simulations for PoCs to review how much time participating States require to reply to a request for assistant and/or provide information to an issue at hand. There is

34 OSCE, Permanent Council Decision No. 1202 in 2016, available at: https://www.osce.org/pc/227281.

35 OSCE, FSC.DEC/5/17, Use of the OSCE Communications Network to Support Implementation of Permanent Council Decisions No. 1039, No. 1106 and No. 1202, 19 July 2017, FSC.DEC/5/17, available at: https://www.osce.org/forum-for-security-cooperation/331821?download=true.

36 Velimir Radicevic, Preventing cyberwar: the role of confidence-building measures and associated OSCE efforts, 3 December 2018, Presentation at the Institute for Higher National Defence Studies.

37 OSCE, Press release: New technological features, policy engagement and public-private partnerships as ways to lower risks of cyber conflicts in focus at Rome Conference, 28 September 2018, available at: https://www.osce.org/chairmanship/397853.

also a separate project to promote operationalisation of the network of policy and technical PoCs by enhancing its functioning, both as a crisis communication network and a platform for co-operation. For the purpose of creating more transparency, OSCE also organises, among other activities, a series of bilateral country visits for PoCs of non-like-minded States. The visits aim to help bridge the largest divides between States in the OSCE area in terms of trust, threat perceptions, approaches to cyber/ICT security, capacities and strategic priorities; and explore commonalities and avenues of co-operation.

Furthermore, with the purpose of promoting, assisting and fostering the implementation process of existing cyber/ICT CBMs, in 2016, the OSCE launched a project that aims to identify and prioritise national implementation challenges. Within this project, it facilitates the creation of national implementation roadmaps and customised capacity-building assistance plans in co-operation with partners such as the Global Forum on Cyber Expertise (GFCE). The latter will include mapping current capacity-building initiatives by other international entities, which could also address CBM implementation challenges on the national and regional levels and therefore complement pertinent OSCE activities.

4.3. ORGANIZATION FOR AMERICAN STATES (OAS)

The OAS uses its Inter-American Committee against Terrorism (CICTE) and the Cyber Security Program to drive its work on cyber security forward. The OAS's mission is to "build and strengthen cyber-security capacity in the Member States through technical assistance and training, policy roundtables, crisis management exercises, and the exchange of best practices related to information and communication technologies".[38] Among the main objectives of the Secretariat are to "establish national 'alert, watch, and warning' groups, also known as Computer Security Incident Response Teams (CSIRTs)".[39]

The OAS has always had a strong emphasis on capacity-building: for example, through supporting the development of cyber security strategies. It has facilitated more than 30 Cyber Maturity Model deployments by the Oxford University Global Cyber Security Capacity Centre among its Member States.[40] Recently, it has shifted its capacity-building efforts towards more specific topics. For example, similarly to the OSCE, the OAS has also engaged in a series of sub-regional workshops on industrial control systems and critical infrastructure in the electricity sector, on the protection of

38 OAS, Cyber Security, 2019, available at: https://www.oas.org/en/topics/cyber_security.asp.

39 Id. At the 2004 OAS General Assembly, the Member States approved Resolution AG / RES. 2004 (XXXIV-O/04), "A Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating A Culture of Cybersecurity".

40 Oxford Martin School, CMM Assessments Around the World, August 2018, available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-assessments-around-world.

critical infrastructures, cyber security and border protection;[41] as well as workshops on the applicability of international law cyber operations in the Americas.[42]

Moreover, having recognised the importance of regional implementation of the UN GGE reports through practical means, in 2017, the CICTE decided to establish a working group on co-operation and CBMs in cyberspace.[43] In 2018, a draft set of "Cyber CBMs for the Inter-American System"[44] was adopted by the CICTE and the OAS General Assembly with a proposed plan of action to establish additional measures.[45] Each OAS Member State will, as a first step, be asked to determine a national focal point, who will act as a first responder on the policy level should an incident concerning cyber security threaten relations between States. Moreover, going forward, OAS Member States will commence sharing information on national cyber policies, strategies and doctrines in a more formalised way.

4.4. ASSOCIATION OF SOUTHEAST ASIAN NATIONS (ASEAN) AND THE ASEAN REGIONAL FORUM

As the ASEAN's regional emphasis has been on economic progress and development, it launched its international cyber security efforts with an emphasis on international co-operation and harmonisation of policies, particularly with regard to cyber crime.[46] Given the increase in small and medium-sized enterprises (SMEs) which work mostly online, governments seem to have felt an increasing responsibility to secure their operational environment; hence the emphasis on cyber crime. Similarly, efforts undertaken to protect critical infrastructures can be understood as an attempt to protect the increasing amount of services provided online within the region.

41 OAS, Sub-Regional Workshop on Industrial Control Systems and Critical Infrastructure in the Electric Sector, 2017 available at: https://www.sites.oas.org/cyber/EN/Pages/Events/eventsdet.aspx?docid=102; OAS, Subregional Workshop on Protection of Critical Infrastructures: Cybersecurity and Border Protection, 2017, available at: https://www.sites.oas.org/cyber/EN/Pages/Events/eventsdet.aspx?docid=99.

42 The legal courses are jointly organised by the Secretariat of the CICTE and the Ministry of Foreign Affairs of the Netherlands. See OAS, The Hague Process: Courses on the International Law Applicable to Cyber Operations, 2017, available at: https://www.sites.oas.org/cyber/EN/Pages/Events/eventsdet.aspx?docid=90; Autoridad Nacional para la innovación gubermental, Panama, November 2018, available at: http://innovacion.gob.pa/noticia/3231.

43 OAS, Inter-American Committee against Terrorism, Establishment of a Working Group on Cooperation and Confidence-Building Measures in Cyberspace, OEA/Ser.L/X.2.17, CICTE/RES. 1/17, 10 April 2017, available at: http://scm.oas.org/doc_public/ENGLISH/HIST_17/CICTE01114E07.doc.

44 CICTE/GT/MFCC-7/17 rev.2, Inter-American Committee Against Terrorism (CICTE): Regional confidence-building measures (CBMs) to promote cooperation and trust in cyberspace, available at: http://scm.oas.org/doc_public/ENGLISH/HIST_18/CICTE01179E05.doc.

45 The proposed text was approved in May 2018 by the Inter-American Committee against Terrorism: CICTE/RES.1/18, Inter-American Committee Against Terrorism (CICTE): Regional confidence-building measures (CBMs), to promote cooperation and trust in cyberspace, OEA/Ser.L/X.2.18 and in June 2018 by the OAS General Assembly through Resolution AG/RES. 2925 (XLVIII-O/18): http://scm.oas.org/doc_public/ENGLISH/HIST_18/AG07745E03.doc.

46 NATO CCD COE, ASEAN Regional Forum Reaffirming the Commitment to Fight Cyber Crime, INCYDER, 20 July 2013, available at: https://ccdcoe.org/asean-regional-forum-reaffirming-commitment-fight-cyber-crime.html.

However, given the lack of agreement on the UN GGE 2017 report under its Singaporean Chairmanship, discussions within the ASEAN have increasingly looked at how it could move discussions on the four UN GGE pillars forward in its own region.[47] This also resembles a shift from compartmentalised cyber security efforts to a more strategic conversation on the challenges posed.

As a result, through a series of ministerial meetings, norms and CBMs rose to the top of the cyber security agenda, resulting in a formal endorsement of the 11 norms recommended by the UN GGE 2015 report during the ASEAN Ministerial Conference on Cybersecurity (AMCC) in September 2018.[48] As Elina Noor rightly points out, "The seeds of a more strategic conversation on positioning ASEAN within the norm-setting agenda in cyberspace have now finally been sown".[49] Shortly afterwards, ASEAN ministers formally affirmed the AMCC outcome and "noted the agreement by the relevant Ministers: (a) on the need for a formal ASEAN cybersecurity mechanism to coordinate cyber policy […]."[50] As a next step, the ASEAN Network Security Action Council will "prepare a proposal for a formal ASEAN cybersecurity coordination mechanism for consideration by relevant ASEAN sectoral bodies. [ASEAN Ministers] agreed that in the meanwhile, the AMCC should continue to serve as the interim and non-formal ASEAN platform for cybersecurity".[51]

These developments were accompanied by the Sydney Recommendations on Practical Futures for Cyber Confidence Building in the ASEAN region, which outlined how cyber confidence building can be moved forward.[52] At present, five CBMs are being discussed in the ASEAN-ARF Inter-sessional group and will probably resemble similar pathways taken by the OSCE and the OAS.[53]

4.5. INCREASING ROLE AND INTERCONNECTEDNESS OF REGIONAL ORGANISATIONS

Previous sub-chapters have outlined three regional organisations' efforts in shaping

47 Caitríona Heinl, Can ASEAN Continue to Improve Cybersecurity in the Region and Beyond? March 22, 2018, available at: https://www.cfr.org/blog/can-asean-continue-improve-cybersecurity-region-and-beyond.

48 CSA Singapore, Singapore International Cyber Week 2018 - Highlights and Testimonials, September 20, 2018, available at: https://www.csa.gov.sg/news/press-releases/sicw-2018---highlights-and-testimonials.

49 Elina Noor, ASEAN Takes a Bold Cybersecurity Step, *The Diplomat*, October 4 2018, available at: https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/.

50 ASEAN, Chairman's Statement of the 33rd ASEAN Summit, Singapore, November 2018, available at: https://asean.org/storage/2018/11/33rd_ASEAN_Summit_Chairman_s_Statement_Final.pdf.

51 Id.

52 Sydney Recommendations on Practical Futures for Cyber Confidence Building in the ASEAN region, September 2018, available at: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-09/Sydney%20recommendations_Cyber-ASEAN.pdf?kwrNP4FHCYxE9oGVhxzchUvF3rx11hoG.

53 ARF Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies and 1st ARF-ISM on ICTs Security: https://www.mofa.go.jp/press/release/press4e_002011.html.

the landscape of cyber security-related norms and practical CBMs. There are two main conclusions we can draw from this.

Firstly, the aforementioned regional organisations initially focused only on certain topics related to cyber security; and have thereby been keeping their work narrow and not as broad as the UN GGE reports. Recently, all have gradually expanded their scope into additional UN GGE pillars, recognising that one-sided emphasis only works for a limited amount of time. In fact, some regional organisations may have the mandate to focus on areas not covered by the UN GGE, such as Internet infrastructure, content management, freedom of expression, privacy protection, digital economy and introduction of new technologies. All in all, regional organisations eventually seem to have acknowledged that their initially limited efforts can become more substantiated if multiple, or ideally all four, pillars are addressed within each region. Since the OSCE, OAS and ASEAN are coming from different perspectives and originally had different foci, their comprehensive approach, covering most if not all four pillars, provides ample opportunity to support each other's efforts, as will be demonstrated in the next chapter.

Secondly, even though regional organisations have expressed their appreciation of the proposed norms, there appears to be some concern over the lack of consensus following the most recent UN GGE efforts. Commentators have suggested that regional organisations such as the ASEAN should not wait for the UN GGE to be reconvened: even if consensus will be achieved and additional norms agreed to, this will take time.[54] Instead, as detailed already, it has been proposed that the ASEAN should start working on implementing these norms and possibly shaping new ones "in ways that correspond to ASEAN Member States' needs and contexts, and can take the proactive role instead of waiting for larger States to dictate the rules of the road".[55] This clearly points to the interest as well as capacity to push towards more tailor-made solutions on the regional level. At the same time, it raises the question of whether the UN GGE is the most suitable global platform for regional organisations to harmonise their efforts and make themselves heard internationally.

Therefore, before concluding on how to better incorporate their views into global discussions, the following chapter will also look at how regional organisations may benefit from enhanced inter-regional activities.

54 Benjamin Ang, Next steps for cyber norms in ASEAN, 2018, https://www.rsis.edu.sg/wp-content/uploads/2018/10/CO18174.pdf.

55 Id.

5. CROSS-CUTTING BENEFITS OF INTER-REGIONAL AND GLOBAL OPPORTUNITIES

Instead of discussing possible new international platforms for developing cyber norms, focus should remain on maximising the impact of what is already agreed upon and established. In order to achieve that, national, regional and global efforts need to be linked in a coherent way and practical efforts focused on implementation should receive priority. Moreover, discussions need to become more nuanced, streamlined and channelled into the right structures. Only by doing so can States focus on implementing and operationalising agreed norms and CBMs.

Firstly, when discussing additional norms to be added to the framework of the already agreed UN GGE 2015 report, it would help to reflect on which topics are actually crucial for the maintenance of peace and stability among States at this point. Secondly, it is also key to parse out the vast number of topics within the cyber security umbrella and identify fitting fora for each issue. Global institutions like the UN, regional organisations like the OSCE, like-minded entities and fora that facilitate dialogue among non-like-minded States all have their value. Maximising the effect and impact of existing platforms by using the right platform for the respective topic at hand is key. When it comes to linking regional and global efforts, the UN, specifically the UN GGE but potentially the new OEWG too, provides room for such co-operation.

In the following sub-paragraphs, we will highlight elements of inter-regional and global platforms which we believe would benefit from the greater inclusion of regional organisations.

5.1. INTER-REGIONAL DEVELOPMENTS

As outlined above, the OSCE, OAS and ASEAN are the key actors worldwide to enhance international cyber stability through their cyber/ICT CBM catalogue, capacity-building efforts, international co-operation and dialogue. When applying a global lens, each of them is just one out of several regional organisations that are trying to foster regional co-operation and offer policy advice on cyber/ICT security-related issues within their area of operations. In order to better understand similarities, differences and room for additional collaboration, there is significant potential for an inter-regional initiative that aims at establishing knowledge and best practices exchange amongst regional organisations working on cyber/ICT security issues.

A sustainable network with other regional organisations developing cyber/ICT CBMs as well as capacity-building initiatives would be beneficial in several aspects. Such

an inter-regional approach would facilitate gaining specific insights into related cyber/ICT security initiatives by other international organisations, as well as identify common interests and maximise the impact of potential overlapping initiatives by collaborating or planning joint workshops, training, conferences etc. Developing working-level connections among the regional organisations working on cyber/ICT security CBMs would facilitate co-operation and communication. Exchanging best practices and specific knowledge about regional characteristics, governmental structures or policy challenges related to cyber/ICT security issues would provide good grounds for furthering trust and collaboration. Equally relevant would be to explore the possibilities of joint CBM implementation initiatives in States that are part of several regional organisations engaged in cyber/ICT security initiatives; and identify possibilities of further linking capacity-building initiatives with CBMs.

One option for such inter-regional cooperation would be the Global Forum on Cyber Expertise (GFCE). The launch of the GFCE was a result of the 2015 Global Conference on Cyber Security. Initially created by the Dutch government, the GFCE is now a "global platform for countries, international organisations and private companies to exchange best practices and expertise on cyber capacity building".[56] By its very design and mandate, the GFCE is an ideal platform for an international best practice exchange, collaboration and co-operation. In the mid- to-long run, this initiative could establish a sustainable hub for constructive exchange amongst regional organisations and facilitate resource and capacity sharing, information exchange and long-term co-operative projects and initiatives, while avoiding unnecessary duplication amongst regional organisations.

States of involved regional organisations would also benefit from this initiative since this platform is likely to reduce duplication and enhance global awareness of capacity needs across regions. Moreover, more effective inter-regional co-operation is likely to create improved distribution of resources amongst regional organisations and streamline cyber stability efforts across regions. Helping regional organisations better co-ordinate amongst themselves could also help States with their own international cyber/ICT policy initiatives, as most cyber/ICT security related initiatives are highly intertwined and connected across regions or even globally: and thus gain effectiveness from initiatives that are already harmonised between regional organisations. Equally, additional support from selected States through the GFCE could ensure political buy-in, increase the impact of this initiative and generate interest in operationalising this network for enhancing pertinent national capacities.

Such a platform could also support the effective implementation of the CBM catalogues of the OSCE, OAS and ASEAN by supplementing regional organisations'

56 GFCE, about page, available at: https://www.thegfce.com/about.

efforts with additional capacity-building and awareness-raising efforts among GFCE members.

Another promising inter-regional development was a workshop organised in Geneva in January 2019 by the Center for Security and International Studies, and the United Nations Institute for Disarmament Research, on "The Role of Regional Organizations in Strengthening Cybersecurity and Stability".[57] While this did not result in the establishment of a formal inter-regional body for exchange, the workshop itself was already a welcome development: for the first time, it provided representatives of regional organisations with the opportunity to constructively engage with UN officials, and discuss in concrete terms how regional contributions and expertise could best be integrated into UN-level discussions. As all regional organisations mentioned in the UN GGE mandate were present in the room, it also allowed them to discuss amongst themselves how they could best co-ordinate their input across regions.[58]

During the discussions, there seemed to be overall agreement amongst participants that regional organisations have been the enablers of capacity-building, awareness raising and CBM development. As a result, regional organisations have significant untapped potential to contribute to international cyber security policy negotiations. Such efforts would not seek to replace UN-level discussions, but to complement, support and incorporate regional perspectives into the discussions. It was reiterated that regional organisations have a unique advantage in launching certain activities, as they have a better grasp of regional developments and national preferences, which play a vital role in implementing norms and CBMs.

5.2. GLOBAL PLATFORMS

Global efforts such as the UN GGE are clearly interconnected with the work of regional organisations. When looking at the UN GGE 2015 report, many of the 11 norms and principles are already closely connected to existing capacity-building or CBM efforts. In fact, several studies have confirmed both the influence of the UN GGE on regional CBMs, and the potential of regional measures to complement the UN GGE measures.[59] However, what is missing is a clear structure and framework for enhancing the positive, mutually reinforcing impact. Clarifying how such parallel

57 See UNIDIR Press Release, The 2nd International Security Cyber Issues Workshop Series: The Role of Regional Organizations in Strengthening Cybersecurity and Stability, available at http://unidir.org/programmes/security-and-technology/the-2nd-international-security-cyber-issues-workshop-series-the-role-of-regional-organizations-in-strengthening-cybersecurity-and-stability.

58 Overview of the Group of Governmental Experts and Open-ended Working Group Processes, presentation by Gillian Goh, Political Affairs Officer and Cyber Team Leader, UN Office of Disarmament Affairs, available at: http://unidir.org/files/medias/pdfs/overview-of-the-group-of-governmental-experts-and-open-ended-working-group-processes-eng-0-786.pdf.

59 See, e.g., footnote 17, pp.129-153; DiploFoundation, Towards a secure cyberspace via regional co-operation, 2017, available at: https://www.diplomacy.edu/sites/default/files/Diplo%20-%20Towards%20a%20secure%20cyberspace%20-%20GGE.pdf.

efforts can be harmonised and brought together should be part of the discussions within the newly formed UN GGE and OEWG.

Even though traditionally the UN GGE process does not directly involve non-State actors, more formalised input from regional organisations could benefit the overall process by presenting a consolidated view of its members, support the implementation of the agreed principles and enforce capacity-building efforts and awareness raising. Despite the lack of an explicit reference to regional organisations in its mandate, the UN OEWG should also consider how to engage with regional organisations. Overall, when designing the processes for further including regional organisations' efforts at the UN level, we suggest keeping in mind the following proposals.

a) Choosing the Right Venue and Format

The two somewhat overlapping proposals for taking forward the norms-building process at the UN level (described in Chapter 2) pose a dilemma to all involved stakeholders, ranging from States to regional organisations, which have previously been directly or closely involved following UN GGE reports. Which of the two working groups should be given more attention? Which one develops more relevant information for regional organisations? While these questions cannot be answered yet, only the UN GGE mandate explicitly invites regional organisations for consultations. We therefore suggest embracing this invitation, while also clarifying how regional organisations can contribute to discussions within the OEWG. For the benefit of the complementarity of efforts and the potential for convergence, regional organisations, even if they are explicitly mentioned in the UN GGE mandate, should try to identify means to actively engage with both groups.

However, given that at this stage regional consultations are only foreseen with the UN GGE, most of the following recommendations are more applicable to regional collaboration with it. Overall, close collaboration with regional organisations, mentioned in the UN GGE mandate, seems more practical, as the new GGE proposal follows a concrete timeline and specifically incorporates consultations with regional organisations. We therefore argue that it makes most sense for regional organisations that were explicitly mentioned in the UN GGE mandate to engage without reservations. On the other hand, even though the OEWG format does not foresee a strictly defined timeline,[60] it promises a multi-stakeholder approach,[61] therefore leaving room for the potential inclusion of consultations with regional organisations as well.[62]

60 The OEWG's mandate asks for the submission of a report on the results of the study to the General Assembly at its 75th session, but leaves room for continued discussions after this deadline.

61 Alex Grigsby, The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased, 15 November 2018, available at: https://www.cfr.org/blog/un-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

62 Other entities which have not been invited to consultations with the UN GGE are facing an additional dilemma. They may be forced to focus their collaboration with the OEWG, as it addresses a wider range of stakeholders such as the private sector, non-governmental organisations and academia.

Moreover, the tentative meeting timeline[63] allows sufficient room for collaboration and information exchange between the UN GGE and the OEWG. This may be challenged by political differences, but could ideally result in a division of tasks or an assurance of avoiding overlap and/or contradiction between their respective reports.

b) Building on Existing Global-Regional Synergies

Our analysis of the ongoing efforts of regional organisations reveals a number of areas where there is a clear link between the UN GGE proposals and the work of regional organisations. For example, the limiting norm that "states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs" has clear connections to national capacities to address malicious or criminal use of ICT infrastructure, an area where ASEAN has been particularly active over recent years, as described in the previous chapter. Moreover, the norm that "states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure" neatly aligns with multiple critical infrastructure protection efforts, such as OSCE CBM 15 or the OAS's capacity-building workshops.

Another example is the limiting norm that "States should not conduct or knowingly support activity to harm the information systems of another State's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity", which directly relates to the OAS's capacity-building efforts; in particular, the development of CSIRTS among its members. Similar comparisons can be conducted for the good practices and positive duties included in the UN GGE's 2015 report.

These examples underline the large potential in systematically synchronising regional and global efforts. Building on already existing areas of collaboration will allow for more swift progress in the implementation of agreed UN GGE norms.

While previous CBMs agreed at UN level largely correspond to CBMs already agreed upon at regional level,[64] there is the possibility of additional CBMs being agreed in the UN. If the UN GGE or OEWG decide to propose additional CBMs, close collaboration with regional organisations would be beneficial for both sides, as mutually reinforcing efforts and regional expertise, needs and suggestions would most likely increase the impact, effectiveness and level of adoption of the UN-level CBMs.

63 Footnote 58, slide 3.

64 As Henry Rõigas and Tomáš Minárik outline: "The CBMs in the report largely correspond to those already adopted under the auspices of the OSCE in 2013. The key difference, however, is that, unlike the OSCE, the report does not establish or propose concrete cooperation channels". 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law, CCDCOE, available at: https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

c) Regional Organisations as Incubators for New Ideas

As outlined in the previous chapter, regional organisations have developed their own innovative ideas on how to address some of the most pertinent international cyber security policy challenges. These efforts have provided a positive contribution to international discussions on cyber security and remain a key component of effective implementation of globally accepted rules and norms. The OSCE's "adopt a CBM initiative" could be applied similarly to norms. Such targeted norm campaigns, driven by volunteer States, may provide new room for suggestions on how these norms can properly applied and implemented.

Also, unlike the OSCE, the UN GGE report does not "establish or propose concrete cooperation channels", since "the measures proposed in the report mainly relate to information exchange and developing international cooperation mechanisms between national entities dealing with ICT security".[65] Thus, the 2021 UN GGE report now has the potential to critically reflect on how existing co-operation channels can be made available for cyber security issues, or how the carefully constructed networks within different regions in the world could be connected.

d) Targeted Capacity-Building

As a positive example, the OAS's targeted capacity-building has helped its Member States to advance their national cyber security competencies significantly. While the OAS's efforts were constrained by its mandate, a dedicated UN capacity-building initiative, designed to help States that want to properly implement UN GGE reports but lack the resources to do so, would certainly contribute to a more coherent international cyber security policy landscape and eventually make cyberspace safer and more stable overall. With the OAS's existing expertise, the ASEAN Singapore Cybersecurity Centre of Excellence, the ASEAN Japan Cybersecurity Capacity Building Centre, and the OSCE's capacity-building workshop series, such a UN capacity-building initiative may be able to tap into regional areas of expertise and combine them in a way no regional organisation could by itself.

e) Not Re-Inventing the Wheel: Adding a Lessons Learned Instrument

When looking at potential focus areas for the newly created UN GGE, this paper argues that representatives should consider practical steps towards implementing previously agreed UN GGE reports. Especially after the lack of consensus for parts of the 2017 report, an initial focus on practical procedures could reduce the level of politically sensitive issues in the discussion while still making some meaningful progress on the issues at hand. Looking back at the overview of practical matters offered by regional organisations outlined in the previous chapter, this paper argues that global-regional collaboration within the UN GGE could easily include sharing lessons learned and

65 Id.

experience from regional organisations. Through the lessons learned process, norms can be further developed and gaps in the existing international frameworks identified.

f) Regional Roadmaps and Joint Implementation Efforts

Another component of global-regional collaboration within the new UN GGE could involve regional roadmaps on the agreed measures, norms and initiatives. Having regional organisations take part in the preparation of concrete implementation roadmaps could have several benefits when looking at the potential impact of the new report. Instead of publishing its new report with no concrete implementation follow-up procedure, the UN GGE could involve regional organisations early on, to develop a customised workplan for each region. This could significantly speed up the implementation process, increase the coherence of norm implementation, facilitate the use of regional capacities and improve linkages between existing regional efforts and newly developed norms and initiatives within the UN GGE report. This paper therefore suggests that such roadmaps should be a component of the UN GGE 2021 report.

g) Involve More Funding

Another potential benefit of increased global-regional cooperation lies in project-based work and funding. If a certain initiative is included into the UN GGE process without including regional organisations' considerations, it might prove difficult for regional organisations to follow up if their mandate does not overlap with the initiative at hand. Having regional organisations be part of the framing procedure would prove helpful in preparing regional follow-up projects and attracting external funding for the new initiative. Moreover, if new initiatives within the UN GGE report overlap with regional organisations' mandates, it is likely that regional implementation would be less controversial and therefore States would probably be less reluctant to provide funding.

h) Enhanced Timing and Priorities

Lastly, another potential benefit through greater global-regional exchange relates to a more structured norms discussion in terms of timing and priorities. Regional organisations, especially those with national offices or extensive national capacity-building efforts, have extensive insights into national concerns and can therefore evaluate whether the proposed UN GGE priorities line up with national ones. Such a procedure might also have a positive impact on the implementation of the norm in the respective region. Knowing which norm lines up with national or regional priorities might prove useful to the UN GGE and allow it to develop certain norm implementation pilot projects in the respective regions.

However, even if formally hearing out regional organisations sounds good on paper,

resolution A/C.1/73/L.37 leaves open how suggestions and concerns raised by regional organisations will be incorporated into the UN GGE deliberations. Besides this concern, we believe that our proposals should provide the stakeholder meetings, to be organised in 2019 by the United Nations Office of Disarmament Affairs, with sufficient concrete proposals on how to move the global-regional cooperation forward within the UN GGE.

6. CONCLUSION

This paper concludes by confirming that the UN GGE continues to have significant merit and is a much needed platform for enhancing international cyber stability negotiations. However, the deliberations and final report of the 2019-2021 negotiations could significantly benefit through increased collaboration with regional organisations. While the new UN OEWG provides room for private sector and NGO input, the new UN GGE mandate opens an entirely new opportunity for enhanced collaboration between the UN and regional organisations. This could lead to the development of a clear framework for enhancing the positive mutually reinforcing impact of global and regional efforts. This should also include a discussion on clarifying parallel efforts, which could be harmonised and brought together.

Another positive result of the increased exchange between the UN and regional organisations is that this opens up the possibility of expanding the scope of information, suggestions and expertise which is incorporated into UN GGE deliberations.

Furthermore, looking at the already agreed norms and principles, several areas of global-regional collaboration can be observed. There is large potential in systematically synchronising regional and global efforts. Regional organisations are already acting as an incubator for national implementation of UN GGE reports, and have developed their own innovative ideas on how to address some of the most pertinent international cyber security policy challenges.

Another potential benefit of increased global-regional cooperation lies in project-based work and funding. If a certain initiative is included in the UN GGE process without allowing for regional organisations' considerations, it might prove difficult for them to follow up if their mandate does not overlap with the initiative at hand. Having regional organisations be part of the framing procedure would prove helpful in preparing regional follow-up projects and attracting external funding for the new initiative.

When looking at the coherence between UN GGE reports and regional organisations'

activities, this paper argues that there is significant potential in lining them up through a joint workplan, which could be annexed to the new UN GGE report. Such a workplan would provide the drafting process of the 2021 UN GGE report with the opportunity to critically reflect on how existing co-operation channels can be made available for cyber security issues and how carefully constructed networks within different global regions could be connected. Moreover, such a workplan may include regional roadmaps on the agreed measures, norms and initiatives of the new report. Having regional organisations take part in the preparation of concrete implementation roadmaps could significantly improve the implementation process and overall impact of the new report.

Another potential benefit of customised regional roadmaps relates to a discussion of more structured norms in terms of timing and priorities. Regional organisations, especially those with national offices or national capacity-building efforts, have extensive insights into national concerns and can therefore evaluate whether the proposed UN GGE priorities line up with national ones. Knowing which norm lines up with national or regional priorities might prove useful to the UN GGE and allow them to develop certain norm implementation pilot projects in the region in question. These would also have a positive benefit for concrete and practical norms implementation. The UN GGE can profit from the many years of regional experience in capacity-building and norm implementation.

Lastly, a dedicated UN capacity-building initiative, jointly developed with regional organisations and aimed at helping those States that want to properly implement UN GGE reports but lack the resources to do so, would contribute towards a more coherent international cyber security policy landscape; and eventually make cyberspace safer and more stable overall.

While the new UN GGE provides regional organisations with the chance to make themselves heard, this paper also argues for enhanced inter-regional collaboration amongst the most active of them. The OSCE, the OAS and the ASEAN are among the key actors worldwide seeking to enhance international cyber stability through their cyber/ICT CBM catalogue, capacity-building efforts, international co-operation and dialogue. In order to better understand similarities, differences and room for potential collaboration, there is significant potential for an inter-regional initiative which aims at establishing knowledge and best-practices exchange amongst regional organisations working on cyber/ICT security issues.

Such an inter-regional approach would facilitate gaining specific insights into related cyber/ICT security initiatives by other international organisations, identifying common interests and maximising the impact of potentially overlapping initiatives

by collaborating or planning joint workshops, training, conferences, etc. Exchanging best practices and specific knowledge about regional characteristics, governmental structures or policy challenges related to cyber/ICT security issues would provide good grounds for furthering trust and collaboration.

Equally relevant would be to explore the possibilities of joint CBM implementation initiatives in States that are part of several regional organisations engaged in cyber/ICT security initiatives, and to identify possibilities of further linking capacity-building initiatives with CBMs.