STUDY

Making Cyber CBMs Work

Identifying Enablers and Challenges to Strengthen Effective Implementation

Helene Pleil

October 29, 2026

Tech analysis and policy ideas for Europe

interface

Table of Contents

1. Executive summary 4

2. Introduction: cyber stability in an era of decreasing trust 7

3. Defining success: what makes a process effective 10

4. From commitment to practice: enablers and challenges 13
- 4.1. Factor 1: Geopolitical Environment 13
- 4.2. Factor 2: Political Will 14
- 4.3. Factor 3: Timing 15
- 4.4. Factor 4: Prior CBM Experience 17
- 4.5. Factor 5: Participation 19
- 4.6. Factor 6: Institutional Design 21
- 4.7. Factor 7: Consensus Building 22
- 4.8. Factor 8: Dedicated Secretariat 23
- 4.9. Factor 9: Financial and Human Resources 25
- 4.10. Factor 10: Capacity, Knowledge and Cyber Maturity 27
- 4.11. Factor 11: Ownership 28
- 4.12. Factor 12: Operationalisation 29
- 4.13. Factor 13: Understanding of Each CBM 31
- 4.14. Factor 14: Measurability 32
- 4.15. Factor 15: Non-Abuse 33

5. Key findings: patterns across enablers and challenges 34
- 5.1. Cyber CBMs: unique or just another multilateral policy process? 35
- 5.2. Implementation as a continuous process 36

6. Making cyber CBMs work: bridging the implementation 37

gap
6.1. Strengthen a shared vision 37
6.2. Strengthen implementation mapping efforts 38
6.3. Strengthen ownership 40
6.4. Strengthen and leverage capacities in a sustainable manner 41
6.5. Strengthen cross-regional learning 42

7. Acknowledgement 43

Executive summary

Cyber confidence-building measures (CBMs) are mutually agreed-upon sets of actions between states that, while not obligatory nor legally binding, carry political weight. They aim to strengthen trust, increase transparency and predictability, maintain communication between states and reduce the risk of misunderstandings and unintended escalation – which becomes especially crucial when there are growing geopolitical tensions and rapid technological progress.

Over the past decade, cyber CBMs have become an established element of international cyber diplomacy, with such measures having been adopted within several regional organisations, including the Organization for Security and Co-operation in Europe (OSCE), the Organization of American States (OAS), the Association of Southeast Asian Nations Regional Forum (ARF), the Conference on Interaction and Confidence-Building Measures in Asia (CICA) and the Economic Community of West African States (ECOWAS), as well as at the global level through the United Nations (UN). The African Union (AU) is also considering developing cyber CBMs, which further underscores the continued relevance of these measures. Examples of such multilateral cyber CBMs include establishing directories of national Points of Contact (PoCs), sharing cybersecurity strategies, exchanging national views on threats or on the application of international law in cyberspace, conducting joint workshops, building national capacities or setting up crisis communication mechanisms.

However, achieving consensus regarding cyber CBMs is only the first step. Their contribution to international peace and security ultimately depends on whether they are implemented and used in practice. While a considerable portion of the research has been devoted to negotiating and formulating cyber CBMs, their implementation has received far less attention. Thus, building on previous interface research that mapped implementation across organisations, this study examines the aspects that influence multilateral cyber CBM processes based on 15 factors (an overview of these factors is presented in the figure below) and translates these findings into practical recommendations.

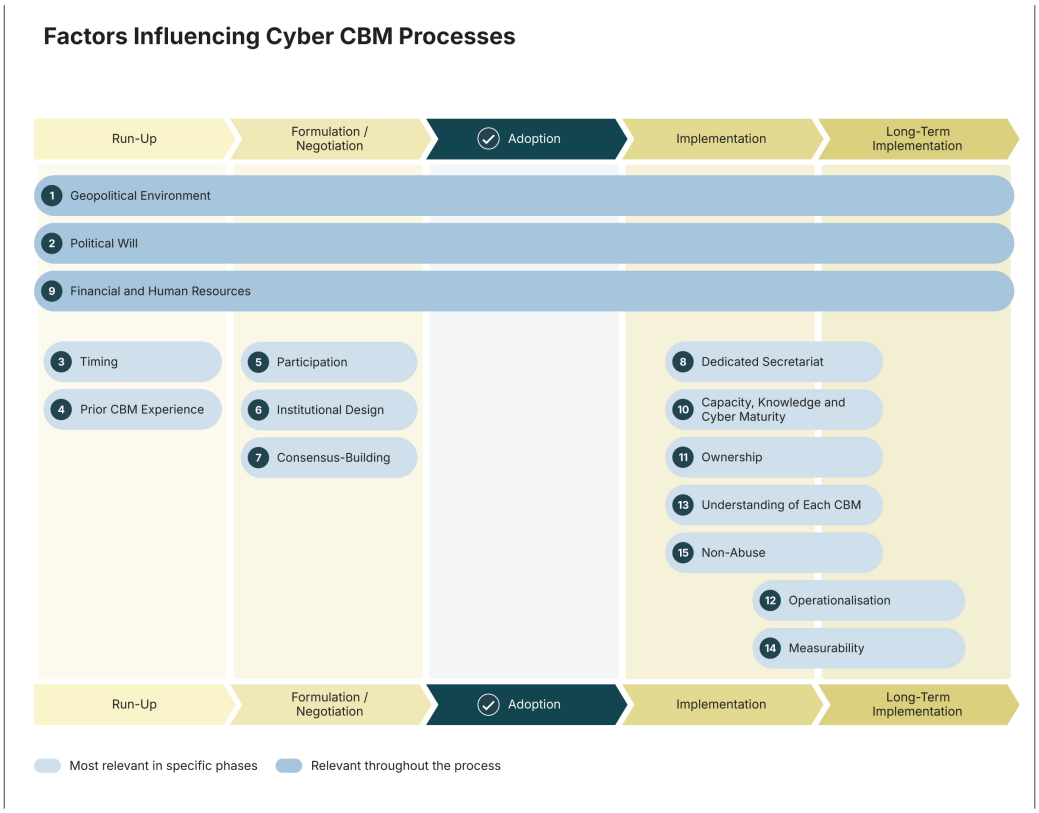
Assessing implementation success requires a broad perspective. Since cyber CBMs are a preventive instrument, their principal objective – the avoidance of conflict and unintended escalation – cannot be directly evaluated. Instead, the effectiveness of such practices needs to be assessed through a combination of indicators, including adoption and participation, institutionalisation, implementation activities, practical use and operationalisation, good faith and non-abuse as well as the overall security environment. Success may also be reflected by more sweeping developments, such as strengthened cyber capacity, closer regional cooperation, increased policy coordination, the diffusion

of norms and increased integration of cybersecurity into foreign and security policies.

As the success of such a process primarily depends on sustained political commitment, political will emerges as the most relevant factor. However, political will is not sufficient on its own. Effective implementation is also enabled by dedicated secretariats, clear ownership, a shared understanding of the CBMs and, most importantly, adequate financial and human resources. Conversely, implementation is often constrained by limited cyber capacity, competing political priorities and lack of trust among parties, insufficient awareness, high staff turnover, differing interpretations of broadly formulated CBMs and the voluntary nature of the measures themselves.

The identified factors should not be considered in isolation, as they are highly interconnected and often reinforce one another. It is apparent that some factors are more relevant during the run-up of such a process, such as the geopolitical environment or timing, or the formulation phase, such as participation or consensus building, whilst others – including ownership, dedicated secretariats or the understanding of each CBM – are particularly relevant in relation to ongoing CBM implementation. In contrast, political will and resources are crucial at almost every stage of the process.

Factors influencing Cyber CBM Processes



Overview of the factors that influence cyber CBM processes, arranged in a loose chronological order according to the stage at which they are the most relevant.

Overall, this analysis identifies more factors that can hinder implementation than those that actively facilitate it. Moreover, enabling and challenging factors are often two sides of the same coin: reducing challenges such as insufficient political will or limited resources may be more important in many cases than introducing or leveraging entirely new enabling measures. Certain driving factors can be actively created and strengthened, including institutional design choices, the strategic use of political windows of opportunity and the promotion of ownership of measures and their implementation.

This study also underlines that there is no universal model when it comes to regional cyber CBMs. The importance attributed to individual factors hindering or enabling a process, the nature of the factor itself or the starting point or way to proceed differ across organisations depending on political dynamics, institutional design, prior CBM experience, cyber maturity and available resources. Nevertheless, common patterns emerge across all processes, allowing the lessons learnt to be transferred while respecting regional specificities.

Based on these findings, the study identifies six priorities for future efforts:

- **Develop a shared understanding of implementation and success among relevant actors**, including clear expectations regarding what the successful implementation of individual CBMs and possible steps to achieve that should look like in practice while taking into account differing regional contexts and perspectives.
- **Strengthen transparency and implementation reviews** through voluntary reporting, implementation mapping and regular exchanges of information about good practices and implementation challenges by drawing on standardised processes and existing resources.
- **Promote ownership and institutional responsibility** by encouraging states to actively champion individual CBMs and sustain implementation over time instead of relying on individual persons or states to drive the process forward.
- **Invest in sustainable capacity-building and resources**, ensuring that implementation support is closely linked to practical CBM requirements to be thoughtful of limited resources.
- **Maintain political momentum for implementation** by keeping cyber CBMs on the agenda of relevant international and regional fora beyond the negotiation and adoption phases and using windows of political opportunity to frame discussions around concrete implementation steps, share experiences and sustain follow-up in relevant negotiation and implementation processes.
- **Expand cross-regional learning**, enabling global and regional organisations that have cyber CBM processes in place, or are considering putting them in place, to exchange implementation experiences, identify opportunities for interoperability and mutual reinforcement and build on existing efforts where appropriate while accounting for differing regional contexts.

As the framework for responsible state behaviour in cyberspace continues to mature, this study argues that the contribution of cyber CBMs to international peace and security will depend less on negotiating additional commitments and more on ensuring that existing measures are effectively translated into practice – at least within the multilateral organisations that already have cyber CBMs in place.

Introduction: cyber stability in an era of decreasing trust

Rapid advances in digital technologies are reshaping the cyber threat landscape. The growing development and diffusion of artificial intelligence (AI), including its potential to automate various aspects of cyber operations, may increase the speed, scale and accessibility of malicious activities.[1] Simultaneously, cybercrime and state-linked cyber operations continue to pose challenges to international security.[2] These technological developments are unfolding against a backdrop of intensifying strategic competition,[3] ongoing armed conflicts[4] and growing strain in relations between states and within security partnerships.[5] As political relations become increasingly adversarial and consensus becomes harder to achieve in multilateral diplomacy, practical mechanisms that preserve dialogue and reduce uncertainty become increasingly valuable.

Decreasing trust between states is also a challenge in the cyber domain, where limited transparency and difficulty attributing malicious activities[6] create persistent risks of misunderstanding. For example, a representative from South Korea highlighted this assessment at the United Nations (UN), saying that "the borderless, anonymous nature of the cyberspace and the speed at which malicious actors conduct illegal destabilising cyber activities, means that confidence among states, or lack thereof, is becoming an ever more important factor of international security".[7]

Based on almost two decades of work,[8] cyber confidence-building measures (CBMs) have emerged as a key instrument of international cyber diplomacy. They are part of a broader framework for responsible state behaviour in cyberspace, alongside discussions of threats, voluntary norms of responsible state behaviour, the application of international law and capacity-building. This is reflected in the UN's newly established, permanent Global Mechanism on Information and Communication Technologies (ICTs) in the

1 Read more on this for example in the report Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards.

2 See for example in the report on the ENISA threat landscape 2026.

3 Read more on the Trump administration views China for example in the current US defense strategy.

4 UN GA (2026): Economic and social repercussions of the Israeli occupation on the living conditions of the Palestinian people in the Occupied Palestinian Territory, including East Jerusalem, and of the Arab population in the occupied Syrian Golan. A/81/11-E/2026/77. See for example here and here focusing on conflict escalation between Israel and Lebanon, here on recent strikes from the US and Saudi-Arabia on Iran backed militias in Iraq, as well as here giving a more detailed overview on the war between Israel, the US, and Iran, and more detail on the current situation in Sudan. Find more information on Russia's war on Ukraine here.

5 See for example here and here regarding tariffs. See for example here and here focusing on tensions within NATO, or a more detailed analysis of current EU-U.S. relations here.

6 Kwiatkowski, Ivan, Kazakova, Anastasiya, Ryng, Julia, Chan, Kendrick (2022): 'Unpacking' technical attribution and challenges for ensuring stability in cyberspace.

7 South Korea' s Representative (2021): (8th Meeting) Open-ended working group on Information and Communication Technology (ICT) - First Substantive Session (13-17 December 2021).

8 The GGE Report 2010 was the first to set out recommendations for potential cyber CBMs.

Context of International Security, created following 25 years of temporary discussions. These complementary areas address different dimensions of international cyber stability – from understanding threats and clarifying expectations of state conduct to strengthening national capabilities and fostering trust and cooperation.

What are (cyber) CBMs?

CBMs are structured agreements that are negotiated and implemented between states.[9] While not obligatory[10] nor legally binding, they carry political weight.[11] They aim to strengthen trust, increase transparency and predictability and reduce the risk of conflict arising from misperceptions or a lack of communication between the states. Consequently, cyber CBMs have become an established tool of **collective problem-solving** within the international cyber diplomacy framework, linking technical cooperation with diplomatic dialogue.

Over the last 15 years, states have increasingly adopted cyber CBMs[12] in bilateral, regional and multilateral settings, such as in

- the Organization for Security and Co-operation in Europe (OSCE; since 2012),[13]
- the Organization of American States (OAS; since 2017),[14]
- the ASEAN Regional Forum (ARF; since 2015,[15] implementation starting in 2018),
- the UN (since 2023),[16]
- the Economic Community of West African States (ECOWAS; since 2024)[17]
- and the multilateral forum Conference on Interaction and Confidence Building Measures in Asia (CICA; since 2021).[18]

In practice, the cyber CBMs developed within multilateral organisations have generally proven to be among the most durable approaches.[19] Such organisations have played an important role in advancing these measures, as they can build on existing initiatives and their close ties to national authorities and tailor initiatives to different levels of cyber maturity, political priorities and regional contexts while addressing shared threat perceptions. Further, the UN provides a global foundation for cyber CBMs, ensuring that confidence-building efforts can extend to all states, including those not covered by regional frameworks. Regional and

9 Healey, Jason, Mallery, John C., Jordan, Klara Tothova, Youd, Nathaniel V. (2014): Confidence-

10 United Nations General Assembly (1996): A compilation of all texts of principles, guidelines or recommendations on subject items adopted unanimously by the Disarmament Commission. Note by the Secretary-General (A/51/182).

11 Zielkowski, Katharina (2013): Confidence Building Measures for Cyberspace. In: Katharina Zielkowski (Ed.): Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy.

12 For the sake of consistency, this paper uses the term cyber CBMs, even though the OSCE, for example, uses the term cyber/ICT security CBMs.

13 OSCE (2012): Permanent Council Decision No. 1039. Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.

14 OAS CICTE (2017): CICTE/RES.1/17. Establishment of a Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

15 ARF (2015): ASEAN Regional Forum Working Plan on Security of and in the use of information and communications technologies (ICTs).

16 Annex A of the second APR - UN General Assembly (2023): Developments in the field of information and telecommunications in the context of international security. (A/78/265).

17 ECOWAS (2024): Directive C/DIR.2/12/12 on Cyber/ICT Confidence Building Measures.

18 Find them here.

19 cf. Pawlak, Patryk (2016): Confidence-Building Measures in Cyberspace: Current Debates and Trends. In: Anna-Maria Osula and Rõigas, Henry (Eds.): International cyber norms. Legal, policy & industry perspectives. NATO Cooperative Cyber Defence Centre of Excellence. // Ott, Nikolas, and Osula, Anna-Maria (2019): The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level. In: 2019 11th International Conference on Cyber Conflict. // UNIDIR (2019): The Role of Regional Organizations in Strengthening Cybersecurity and Stability: Experiences and Opportunities Report of the 2nd International Security Cyber Workshop Series.

global approaches are, therefore, complementary.

Multilateral cyber CBMs broadly focus on exchanging information, enhancing communication, building up capacity and strengthening cooperation. Examples include establishing directories of national Points of Contact (PoCs), sharing cybersecurity strategies, exchanging national views on threats or the application of international law in cyberspace, conducting joint workshops, building national capacities and setting up crisis communication mechanisms (see a full overview of multilateral cyber CBMs here).

The main objective behind engaging in cyber CBM processes is related to international peace and security: reducing risks, increasing predictability and preventing unintended escalation in the cyber domain. For example, numerous statements by states within the UN processes emphasise these goals.

Participation in cyber CBMs may also be motivated by strategic, reputational, capacity-building or domestic considerations. Engagement can provide access to expertise, strengthen partnerships, demonstrate commitment to responsible behaviour and enable states to shape emerging norms and governance processes. In addition to these substantive motivations, the design of CBMs makes participation more accessible than other policy processes. As CBMs are voluntary and non-binding, they are relatively inexpensive to adopt and serve as instruments for international cooperation that allow states to build mutual trust without legal pressure.[20]

While cyber CBMs have become an established element of the international cyber diplomacy framework, the associated scholarly and policy discussions have primarily focused on developing, negotiating and adopting these measures. Relatively little attention has been given to what happens once consensus has been reached and how the effectiveness of the measures is assessed. However, the implementation is ultimately what determines whether cyber CBMs contribute to the realisation of their objectives. Therefore, as the international framework for responsible state behaviour in cyberspace continues to mature, the central challenge is increasingly shifting from agreeing on cyber CBMs to making them work in practice.[21]

Previous interface research mapped the implementation status of cyber CBMs across different multilateral organisations by tracing observable implementation activities and state practice and found significant variation in this regard across organisations, participating states and individual measures. While some cyber CBMs have been actively

20 Mason, Simon J. A. and Siegfried, Matthias (2013): Confidence Building Measures (CBMs) in Peace Processes. In: Managing Peace Processes. Process related questions. A handbook for AU practitioners.

21 Toth, Szilvia (2025): Regional Organisations and Confidence-Building Measures. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James (Eds.): A Handbook for the Practice of Cyber Diplomacy. EU Institute for Security Studies.

implemented and institutionalised, others have seen limited practical uptake. These findings suggest that the successful implementation of cyber CBMs depends on a range of enabling and hindering factors that remain insufficiently understood.

Examining these factors can help clarify the conditions under which CBM implementation is more likely to succeed while demonstrating that their relevance may vary across political and regional contexts and that putting them into practice ultimately depends on states' willingness and capacity to act. Such insights can provide a useful foundation for strengthening existing implementation efforts and serve as a resource for regions considering developing their own cyber CBM processes.

Defining success: what makes a process effective

Unlike reactive instruments, such as sanctions – which seek to levy costs in response to undesirable state behaviour – and legally binding arms control agreements – which impose formal constraints on state conduct – existing multilateral cyber CBMs are primarily preventive and voluntary in nature. Their greatest benefit may manifest as events that never occur: crises that get defused instead of intensifying, misunderstandings that get clarified before they can develop into political disputes or cyber incidents that do not trigger wider or cross-domain escalation.

As a result, assessing the contribution of cyber CBMs to their ultimate objectives is challenging. It is difficult to observe prevented crises and instances of de-escalation and attribute these to specific measures, and evidence of how cyber CBMs function in actual crisis situations remains limited. Nevertheless, the difficulty of measuring their ultimate impact does not preclude a more practical assessment of their implementation and potential effectiveness. By examining observable indicators of state practice and implementation activities, it is possible to identify patterns that may suggest whether and how cyber CBMs contribute to their intended objectives even if their direct impact on crisis prevention cannot be conclusively established.

Accordingly, the successful implementation of cyber CBMs should be understood as a multilayered concept. Rather than seeking to measure every dimension of effectiveness or establish a direct causal link between individual measures and international stability, this approach identifies a range of indicators that provide insights into the different aspects of implementation, namely participation, institutionalisation, implementation activities, practical use, responsible conduct and the broader security landscape, which are distinct but interrelated dimensions.

1. **Adoption and Participation:** Have CBMs been adopted? How many CBMs have been

formally adopted, and how many states are involved in the process?
The formulation of CBMs and their adoption constitute the basis of subsequent implementation. While their very existence is often considered an initial indicator of success, it represents a necessary starting point instead: without agreed-upon measures, there can be no implementation of those commitments. The extent of state participation provides the first indication of the political support for a CBM process. Broad participation may signal a shared interest in the process and its objectives, but it may not necessarily translate into effective implementation.

2. **Institutionalisation:** Have structures and processes been established to support implementation?
Institutionalisation is related to the extent to which cyber CBMs as well as the steps contributing to their implementation and overall objectives are embedded in the structures, responsibilities and processes of the associated multilateral organisation and the participating states. Institutionalisation helps ensure that implementation does not depend solely on individual officials or temporary political momentum and can be sustained over time.
Cyber CBMs are instruments of state-to-state diplomacy, and their formulation and adoption are primarily driven by diplomatic processes. However, implementation often depends on national authorities beyond foreign ministries, including cybersecurity agencies, other relevant governmental bodies and – depending on the measure – non-governmental actors that may also contribute to implementation. Therefore, institutionalisation also requires appropriate responsibility assignment and coordination efforts across the actors involved.

3. **Implementation Activities:** Are states taking steps to put CBMs into practice?
Implementation activities provide an indication of whether states are acting on their commitments, and these can often be observed via publicly accessible information and documented state practices.
In some cases, implementation can be measured relatively clearly. For example, implementation can be assessed by examining whether the meetings that a particular cyber CBM calls for have taken place, which states have nominated PoCs under relevant regional and UN frameworks, which states have established a national cyber incident severity schema as, for instance, recommended in OAS CBM 11 or whether relevant trainings or tabletop exercises have been carried out and which states took part in the same.
In other cases, implementation is less explicit, as some CBMs express broader commitments that may be advanced through national policy processes or activities not explicitly undertaken to fulfil a particular measure. For instance, developing a national cybersecurity strategy may contribute to the objectives of a CBM even if it was executed because of a wider policy process, i.e. CBM implementation was not its motivation or framing.

4. **Practical Use and Operationalisation:** Are CBMs used to manage incidents, misunderstandings or tensions in practice?
The implementation of a CBM does not necessarily imply that it is used in practice. Hence, a distinction must be made between what has been described above with regard to establishing a mechanism or carrying out activities to support it and relying on it when a relevant situation arises. For example, a PoC directory may be established and communication channels tested through regular communication checks. These activities indicate implementation, but they do not establish whether states rely on the directory and its associated channels during actual cyber incidents, misunderstandings or periods of heightened tension. States may opt for alternative communication channels instead. Thus, assessing the practical use of CBMs requires examining – where evidence is available – whether states use them when relevant and whether they are considered suitable for the purpose.[22]

5. **Good Faith and Non-Abuse:** Are the CBMs being used in good faith and not being abused?
The effectiveness of CBMs depends on them being used in good faith.[23] The potential

22 OSCE Secretariat (2020): OSCE Cyber Security Awareness Month.

misuse of CBM mechanisms poses a significant risk to trust and undermines the overall process.[24] Such risks can be assessed, to a limited extent, through documented concerns, statements by participating states and reported instances of alleged misuse. For example, in the case of the UN PoC Directory, states have expressed concerns that repeated or unfounded requests could be used to overwhelm national cybersecurity agencies, thereby reducing the mechanism's effectiveness and eroding confidence in both the tool itself and the broader diplomatic process.[25]

6. **Broader Security Environment:** Have cyber conflicts in the region led to escalation? Finally, the broader security environment should also be considered when assessing CBM success. Cyber CBMs are ultimately designed to reduce risks and prevent escalation. Therefore, the absence of significant cyber-related escalation within a region may serve as a potential indicator that the broader framework of trust, cooperation and communication that cyber CBM processes are building contributes positively to regional stability. However, such conclusions must be drawn with great caution, as many factors influence interstate relations, and it is rarely possible to establish a direct causal link between the broader framework that CBM processes have contributed to building in a given region and the absence of conflict.

The extent to which each of these dimensions can be assessed varies: some – such as implementation activities – produce identifiable outputs that can be tracked through press statements, social media posts, reports or documented state practice. Others – particularly practical use and its relation with the broader security environment – are more difficult to observe and attribute because information about the use of diplomatic communication channels during sensitive incidents may not be publicly available. Accordingly, the absence of documented use should not be interpreted as evidence that a CBM has not been used.

Based on this understanding, the next question that arises is about how such outcomes can be achieved. The following section examines the factors that enable or impede the effectiveness of multilateral cyber CBMs processes across different organisational contexts.

---

23 Kavanagh, Camino & Crespo, Laura (2019): Confidence Building Measures and ICT'. European Foreign Affairs Review 24 (2), p. 187–202.

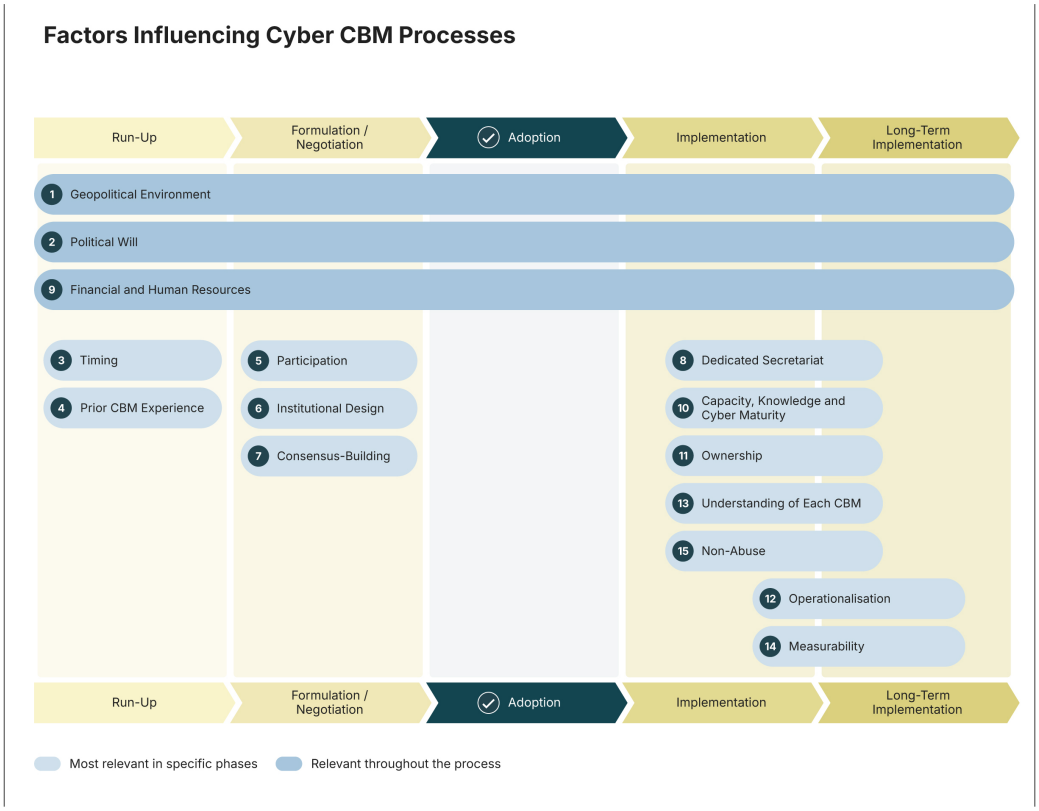
24 Lewis, Kevin N.; Lorell, Mark A. (1984): The Utility of Confidence-building Measures in Crisis Situations: Some Case Studies. RAND Corporation. // Mason, Simon J. A.; Siegfried, Matthias (2013): Confidence Building Measures (CBMs) in Peace Processes. In: Managing Peace Processes. Process related questions. A handbook for AU practitioners. // France's Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024). // Germany's Representative (2025): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025).

25 See for example the statement of France's Representative (2024): "(...) France, at the same time, wishes to reiterate its call to not exploit this tool, to not overuse the tool, at the risk of making it inoperable (...)" as well as Germany's Representative (2025) in a joint statement with France: "(...) It is not sensible to continue sending identical requests when a clear avenue to seek remedies to an alleged malicious cyber activity has been provided on numerous occasions. Such actions seem to be aiming at spamming our cybersecurity agencies, which are committed to responding to such queries in good faith. Such practices bear the risk to undermine, in the eye of the practitioners, the credibility of our diplomatic work here at the UN. And this contradicts the purpose of the future mechanism to bridge the gap between the technical and the diplomatic communities. Taken together, in our view, such activities undercut the meaningful objective of the global POC directory (...)." Meanwhile the Russia's Representative (2026) claimed the following: "I'll give you some statistics about the Russian POCs for last year. There were 2 ,576 inquiries. Out of those, around 48 % of them were responded to. That's due to a number of reasons. (...) Obviously, we also encounter cases where certain capitals simply ignore our requests for political reasons. Incidentally, that applies specifically to those countries that make unsubstantiated accusations regarding the supposed involvement of other states in various computer attacks." This suggests where a lot of inquiries came from.

From commitment to practice: enablers and challenges

Based on the indicators described above, this study identifies 15 factors that influence the effectiveness of cyber CBM processes. These factors are discussed in the following sections and have been organised in a loose chronological order. While some factors span several stages or influence the process throughout its development, others are particularly relevant only at a certain stage of the process (see figure below).

Factors influencing Cyber CBM Processes



Overview of the factors that influence cyber CBM processes, arranged in a loose chronological order according to the stage at which they are the most relevant

Factor 1: Geopolitical Environment

Cyber CBM processes are **shaped by the geopolitical environment** in which states negotiate, adopt and implement them. Geopolitical tensions can either constrain or incentivise confidence-building. When strategic competition intensifies and states increasingly question each other's intentions, trust in shared commitments may erode.

Governments may become less willing to exchange sensitive information, rely on communication channels with geopolitical rivals or invest political capital in multilateral cooperation. This could limit the objective of the mutually agreed-upon CBMs and complicate their implementation.

At the same time, deteriorating international relations can increase the need for mechanisms that help states manage tensions and reduce the risk of misinterpretations. Maintaining communication channels, clarifying intentions and establishing procedures for handling incidents may become more important precisely when trust is limited. Geopolitical competition can, therefore, provide an impetus for developing or strengthening CBMs even if broader political disagreements remain unresolved.

These dynamics are also shaped by broader technological developments. For example, advances in AI may accelerate vulnerability discovery and cyber operations, potentially shortening response times and complicating assessments of intent and state responsibility. Such developments may require existing mechanisms to be reviewed.

Factor 2: Political Will

A crucial cross-cutting factor throughout all stages of a CBM process – from initiation and adoption to long-term implementation – is **political will**. It influences whether states engage in CBM processes, the commitments they are willing to make and their continued support for implementation – even during periods of heightened geopolitical competition and when multilateral cooperation is under greater strain than normal. This requires continuous political prioritisation at the relevant levels of government, confidence in the value of the process and a willingness to cooperate with other participants.[26]

When it comes to the cyber domain, generating such buy-in at the national level can be challenging, where responsibilities are often distributed across multiple actors who may not be accustomed to international cooperation.[27] Moreover, cybersecurity is not always a political priority, with the attention given to it often increasing only in response to major cyber incidents – i.e. when new awareness of the risks of cyber insecurity has been forced upon governmental decision-makers.[28] Globally, incidents such as Stuxnet (2010),[29] WannaCry (2017)[30] and NotPetya (2017)[31] fundamentally shaped political

26 At the same time, willingness to implement commitments must be distinguished from the ability to do so: even where political support exists, limited financial, technical, or human resources may constrain implementation.

27 See for example the German cybersecurity architecture here.

28 Kavanagh, Camino & Crespo, Laura (2019): Confidence Building Measures and ICT. European Foreign Affairs Review 24 (2), p. 187–202.

29 Stuxnet, discovered in 2010, targeted Iran's Natanz uranium enrichment facility, sabotaging centrifuge operation by exploiting four zero-day vulnerabilities in Siemens' underlying Windows operating system. Infection happened via USB flash drives or open network shares, afterwards the infected system could be controlled by the perpetrator giving them full control, even including a command and control function via two servers. Widely attributed to the United States and Israel, it is considered the first publicly known cyber operation to cause physical damage to critical infrastructure and fundamentally shaped international debates on the military use of cyber capabilities

perceptions of cyber threats and the need for enhanced cybersecurity governance. Similarly, country-specific incidents, including Russia's cyber campaign against Estonia in 2007,[32] the destructive cyber operation targeting Costa Rica in 2022[33] and Iran's cyber operation against Albania in 2022,[34] triggered significant national and international policy responses. Such incidents have also been featured in states' statements and policy discussions to underline the importance of international cooperation and confidence-building in cyberspace.[35]

Factor 3: Timing

Another factor is **political momentum and the availability of windows of opportunity**. Like other policy processes, cyber CBM initiatives also partly depend on when political attention, shared interests and willingness to cooperate converge. Such windows may emerge from international negotiations, shifts in political priorities or heightened attention to cybersecurity. Recognising and using these opportunities can help initiate new processes, secure consensus regarding measures or advance implementation.

Periods of heightened tension can also create incentives for confidence-building. CBMs are particularly relevant when relations between states are strained, as they provide practical tools for managing risks and preventing unintended escalation. The Cold War origins of confidence-building illustrate this dynamic: despite profound political and military rivalry, states recognised the value of transparency and communication with regard to reducing uncertainty.[36]

(find more on it here).

30 WannaCry was a global ransomware campaign that spread – independently like a worm – rapidly in May 2017, it exploited the "EternalBlue" vulnerability in Microsoft Windows, which was initially developed by the NSA. The campaign affected more than 230.000 computers in 150 countries and severely disrupted hospitals, businesses, and government services. The total damage was estimated at around four billion U.S. dollars. Several governments later attributed the operation to North Korean state-linked actors, specifically the Lazarus Group (find more on it here).

31 NotPetya (2017) was disguised as ransomware but functioned as a destructive wiper malware causing permanent data loss for those affected. NotPetya was deployed through a supply chain compromise in an Ukrainian tax software update (MeDoc) and exploited the "EternalBlue" vulnerability in Microsoft Windows, which was initially developed by the NSA. Once in the system the malware spread autonomously. Though initially appearing as a financially motivated criminal operation, it was later attributed to Russian military intelligence GRU (Sandworm/APT44) as part of broader hybrid operations aiming to destroy Ukrainian targets. However, the malware quickly spread beyond Ukraine, affecting 65 countries worldwide and around 49,000 systems from multinational corporations as well as the healthcare sector, with estimated damages exceeding 10 billion dollars (find more on it here).

32 In 2007, Estonia experienced a series of distributed denial-of-service (DDoS) operations targeting government, banking, and media websites, widely attributed to actors linked to Russia following a political dispute over the relocation of a Soviet-era monument. The incident is often considered one of the first cases of a coordinated cyber campaign against a highly digitised state (find more on it here).

33 In 2022, Costa Rica was hit by a series of ransomware operations – primarily attributed to the Conti and Hive group which are based in Russia – that disrupted multiple government institutions, including tax and customs systems, leading the government to declare a national emergency. The operation caused significant economic and administrative disruption, highlighting the vulnerability of state institutions to cyber operations (find more on it here).

34 In 2022, Albania suffered a large-scale cyber operation targeting government digital infrastructure, later attributed by national authorities and partners to Iranian state-linked actors, which led to widespread service disruptions and the severing of diplomatic relations between Albania and Iran. The incident demonstrated how cyber operations can escalate into broader political and diplomatic consequences (find more on it here).

35 See for example OAS CICTE (2025): Concept Note. OAS/Ser.L/X.5.

36 Kavanagh, Camino & Crespo, Laura (2019): Confidence Building Measures and ICT. European Foreign Affairs Review 24 (2), p. 187–202.

However, the geopolitical environment was less strained when it came to the adoption of the OSCE cyber CBMs than it is today. The adoption then was facilitated by the recent development of recommendations in the 2013 UN GGE report,[37] which encouraged their initial implementation through regional organisations. In addition, cybersecurity was increasingly perceived as a topic of security policy.[38] This created political momentum and an opportunity to translate emerging global agreement into regional practice. The OSCE used this momentum as well as the organisation's long-standing role in reducing tensions through dialogue and confidence-building, rooted in the Helsinki Final Act, to adopt the first OSCE cyber CBMs in 2013.

More recent developments demonstrate that heightened tensions can reinforce the value of these existing CBMs. Despite the severe deterioration in international relations following Russia's full-scale invasion of Ukraine, some cyber CBM activities within the OSCE continued,[39] while some states intensified their engagement with the same. Germany, for instance, reported increasing its use of the OSCE PoC network and sharing information about major cyber incidents more actively in response to heightened tensions.[40]

At the global level, states have also continued to negotiate and agree on cyber-related outcomes through periods of geopolitical tension, including within UN processes. These developments suggest that geopolitical crises do not invariably prevent diplomatic agreement or cooperation. However, such a crisis may complicate consensus-building, and reaching consensus during such times does not necessarily translate into meaningful implementation.

This has also been highlighted by OAS CBM 7, which addresses gender equality in cybersecurity:[41] its process illustrates how a particular political moment can create an opportunity to achieve consensus regarding an issue that may have been more contested under different political circumstances. However, consensus alone does not guarantee sustained implementation. Shifts in political priorities in the US and several Latin American states may affect the continued support for gender-related initiatives and the willingness to act on agreed-upon commitments.[42]

37 UN General Assembly, Group of Governmental Experts (2013): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Note by the Secretary-General. A/68/98. UN. // additional recommendations followed in the 2015 GGE Report.

38 See for example here.

39 Toth, Szilvia (2025). Regional Organisations and Confidence-Building Measures. In: A Handbook for the Practice of Cyber Diplomacy.

40 Germany as part of the OEWG Confidence Builders (2023): Input Paper, CBMs in Action.

41 "Encourage and promote the inclusion, leadership, and effective and meaningful participation of women in decision-making processes linked to information and communication technologies by promoting specific actions at the national and international levels, with the aim of addressing dimensions around gender equality, and the reduction of the gender digital divide, in line with the women, peace, and security agenda."

42 High, Tracy Richelle, Jordan, Julia M., & Ostrager, Ann-Elizabeth (2025): President Trump Acts to Roll Back DEI Initiatives.

Factor 4: Prior CBM Experience

Political will can be strengthened through a range of reinforcing factors, one of which is **prior experience with CBMs**. Positive experiences with CBMs – either in the cyber domain or in other areas – can significantly facilitate engagement and lower barriers to participation.[43]

This is particularly evident in the OSCE region: since the end of the Cold War, the organisation and its predecessor have developed and implemented a wide range of CBMs across different domains, including cyberspace.[44] As a result, the OSCE is often described as a pioneer in the development and practical application of CBMs, with such mechanisms effectively being "in its DNA".[45] Furthermore, the OAS could draw on past experiences with such processes within its region, starting with traditional CBMs and subsequently expanding to include non-traditional CBMs.[46]

By contrast, other multilateral settings have less institutional experience with CBMs or focus more on other policy areas or instruments. In forums such as the ARF or the UN, cyber CBMs represent – to a greater extent than in other multilateral organisations – only one element within a broader agenda, suggesting that the focus lies elsewhere. This becomes evident when we look at the UN process, where CBMs are one item on the agenda for discussion, but there is no working group dedicated solely to discussing cyber CBMs, as there is within the OSCE and OAS.

This can affect both the prioritisation of CBMs and the level of familiarity with them among participating states. Institutional legacy provides crucial advantages that can enable CBM adoption and drive successful implementation: states can draw on established practices, shared understandings and existing structures, such as secretariats, communication channels and implementation mechanisms.[47] Such legacy also facilitates the transfer of CBM concepts into the cyber domain, as actors are already familiar with the underlying logic and objectives of CBMs. Whereas, in other cases, states need to first

43 Morales, Isaac (2024): Statement at the United Nations Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies.

44 There are different kinds of CBMs: humanitarian, political, economic, environmental, societal and cultural. Within the OSCE-region a variety of such CBMs exists, training on fighting forest fires - a transboundary threat making cooperation necessary - in the South Caucasus for example presents an environmental CBM, while multilingual education aiming to connect the Serbian and Albanian ethnic communities in southern Serbia since 2011 is an example for a cultural CBMs, and founding a Community Security Initiative in Kyrgyzstan presents a political CBM which aimed to build confidence, dialogue and cooperation between police and the population, as well as the different ethnic local communities following the inter-ethic unrest in southern Kyrgyzstan in 2010 (read more on these examples here).

45 OEWG Chair (2025): (6th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025).

46 The OAS distinguishes between traditional and non-traditional confidence- and security-building measures (CSBMs). While traditional measures focus on military transparency and confidence-building, non-traditional measures address a broader range of regional security challenges, including humanitarian assistance, disaster response, demining, cybersecurity, women, peace and security, and cooperation against organised crime.

47 Dominioni, Samuele & Persi Paoli, Giacomo (2023): Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities.

develop a basic understanding of the instrument itself before meaningful engagement is possible.

This was particularly evident in the UN context, where efforts to establish global cyber CBMs brought together states with extremely different levels of prior exposure to such a tool. When it comes to states without prior CBM experience, additional advocacy and capacity-building efforts are required to build the associated understanding and support. In such contexts, political will is often actively cultivated through dialogue and engagement; sustained advocacy and international dialogue have proven to be key drivers of successful cyber CBM development and implementation.[48] It has certainly helped in this regard that an increasing number of regional organisations already had such processes in place once it became a topic of discussion within the UN.

Another aspect to consider in the global setting is that states may hold fundamentally different views on the purpose and value of CBMs. While many see transparency and information sharing as key tools for building trust and reducing the risk of misperceptions, others view such measures more critically. In the context of cyber CBMs, transparency can involve sharing national cybersecurity strategies or information on cyber incidents, but states may be reluctant to disclose certain information. From the Chinese government's perspective, greater transparency can carry strategic risks: Beijing views itself as being at a disadvantage relative to the US and considers secrecy and ambiguity vital for maintaining a tactical advantage. Therefore, transparency may be perceived as enabling stronger states to exert pressure on weaker ones rather than building trust.[49] This view does not necessarily apply to cyber CBM processes, but it reveals a certain way of thinking about a crucial factor in the context of cyber CBMs.

Meanwhile, the establishment of global cyber CBMs within the UN framework – with the first global cyber CBM having been adopted in 2022 – has obviously broadened states' exposure to the concept, including those with limited prior experience with the same. However, familiarity with agreed-upon commitments does not necessarily translate into the practical experience of implementing them. Explicit implementation of the UN cyber CBMs remains at an early stage, and many of the measures and approaches draw on lessons learnt from earlier regional processes. Hence, prior experience continues to matter: established regional processes can offer practical insights into operationalising commitments, sustaining implementation and addressing implementation challenges – also drawing from prior CBM experiences from other domains – that newer processes may not have encountered yet.

48 Examples of this are a study visit of ECOWAS representatives to the OSCE IWG meeting during their cyber CBM formulation process as well as dialogue within and alongside the OEWG over the last years with representatives of the OSCE and OAS also participating, as well as the exchange and advocacy the Confidence Builders have contributed at the UN-level.

49 Segal, Adam (2014): What Briefing Chinese Officials On Cyber Really Accomplishes.

It is also vital to note that institutional unfamiliarity with CBMs does not necessarily imply resistance. The cyber CBMs implemented by ECOWAS represent the first ever CBMs of the region.

Finally, the growing number of multilateral cyber CBM initiatives may lead to a diffusion effect. As more states observe the perceived benefits of such measures, they may become more inclined to engage in similar processes themselves. This dynamic can gradually strengthen political will across regions and contribute to enabling additional multilateral cyber CBM processes. For instance, the African Union (AU) is currently considering starting a cyber CBM process.[50]

Factor 5: Participation

The success of cyber CBM processes depends on not only how many states participate but also **which states are involved**. While broad participation may lend legitimacy to a given process, its practical relevance will depend on the involvement of states that are central to addressing the risks or tensions in question.[51] The absence of key actors, such as states that have strong cyber capabilities,[52] can limit the effectiveness of a CBM process even if a large number of states have reached consensus regarding the measures. Thus, participation should be assessed not only in quantitative terms but also in terms of the relevance of the states involved.

Some of the multilateral organisations that have cyber CBMs in place can draw on long-standing traditions of cooperation among their member states, which fosters a baseline level of trust and facilitates engagement: the OAS, for example, is often perceived as an organisation with a relatively more homogeneous membership and a history of sustained cooperation.[53] The OSCE also has a long-standing tradition of confidence-building and institutional experience in this region. However, Russia's full-scale invasion of Ukraine has placed severe strain on cooperation across the organisation, making consensus and broader political engagement increasingly difficult.[54] Nevertheless, this has not brought cyber CBM activities to a complete halt: some activities have continued, and certain participating states have maintained or intensified their engagement.

Other forums, such as the ARF, bring together a highly diverse set of actors, including major powers with competing strategic interests, such as the US, EU, China and Russia.

---

50 See the AU's statement at the 2026 July meeting of the Global Mechanism.

51 Said, Mohamed Kadry (1999): Confidence Building Measures: A Practical Approach. Instituto Affari Internazionali.

52 See for example the Belfer Center National Cyber Power Index (2022), IISS assessment of cyber capabilities (2021) or the Lowy Institute Asia Power Index (2025) for an overview of such states and their capabilities.

53 Hurel, Louise Marie (2025): Cyber Diplomacy in Latin America. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James: A Handbook for the Practice of Cyber Diplomacy.

54 Douglas, Nadja (2025): The OSCE as a Yardstick for Multilateral Security.

In such contexts, deep-seated geopolitical tensions and fundamentally different visions for the cyber domain complicate cooperation and can limit both the intention and the practical implementation of cyber CBMs.[55] While the ARF provides a platform for regional dialogue on cyber issues, participating states may prioritise other bilateral, regional or multilateral channels for practical cooperation.[56]

Thus, participation is one of the factors that influences what kind of cyber CBMs get adopted as well as the ability and political will to provide resources to participate in the process or drive it forward.

When it comes to participation, cyber CBM processes face another structural limitation: cybersecurity governance requires a multistakeholder approach, as the vast majority of digital infrastructure is privately owned and operated. This implies that private companies often control the networks, platforms and technical expertise that are crucial during cyber incidents.[57] Recognising this, organisations such as the OAS, OSCE and UN have adopted CBMs that explicitly encourage cooperation with non-state stakeholders (OAS CBM 10, OSCE CBM 12 and 14 and UN CBM 8). However, CBMs remain fundamentally state-centric diplomatic instruments,[58] as these non-governmental actors are not present when the CBMs are negotiated.[59]

A similar disconnect exists in the case of military and intelligence actors. Cyber operations are increasingly being used for military, law enforcement and intelligence purposes, and many of the most sophisticated capabilities are located within defence institutions or intelligence agencies.[60] Yet, cyber CBM processes are primarily diplomatic in nature and tend to involve ministries of foreign affairs as well as national technical agencies. This means that the actors who may ultimately shape cyber escalation dynamics are often absent from confidence-building discussions, which can limit the practical reach of these mechanisms.[61] [62]

55 Markoff, Michelle (2025): The Origins of Cyber Diplomacy: Great Power Cyber Competition and Rapprochement in the United Nations 1998–2021. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James: A Handbook for the Practice of Cyber Diplomacy.

56 For Southeast Asian states ASEAN plays a more central and trusted role in the cyber domain. Many capacity-building activities on various topics are being implemented within ASEAN's framework, including through the ASEAN Cyber Capacity Programme and the ASEAN-Japan Cybersecurity Capacity Building Centre, and the implementation of the norms is also being further developed within this scope. Since 2020, the ASEAN CERT Information Exchange Mechanism has held biannual sessions in which member states share threat intelligence, discuss incidents, and coordinate mitigation measures. Building on this foundation, ASEAN is in the process of establishing a regional CERT – funded and hosted by Singapore – its taskforce convened for the first time in August 2024 under Malaysia's coordination. The EU's engagement in the ARF is also limited, represented only through the European External Action Service (EEAS), with minimal direct involvement of individual member states.

57 Gertz, Geoffrey, and Evers, Miles (2020): Geoeconomic Competition: Will State Capitalism Win? In: Washington Quarterly 43 (2), pp. 117–136.

58 Healey, Jason, Mallery, John C., Jordan, Klara Tothova, Youd, Nathaniel V. (2014): Confidence- Building Measures in Cyberspace. A Multistakeholder Approach for Stability and Security.

59 IGF (2020): IGF Best Practice Forum on Cybersecurity.

60 Olech, Aleksander & Štrucl, Damjan (2025): The evolution of cyber forces in NATO countries.

61 cf. Glosserman, Brad (2017): ARF to the Forefront: Promoting Cybersecurity CBMs in the Asia-Pacific. A Conference Report of the CSCAP Workshop on Cybersecurity in the Asia-Pacific. CSIS Report (17) 7.

62 Altmann (2019) has written a chapter exploring the idea of cyber CSBMs which would also include armed forces and could make agreements politically binding (find more on it here: cf. Altmann, Jürgen (2019): Confidence and Security Building Measures for Cyber Forces. In: Reuter, Christian (Ed.): Information Technology for Peace and Security. IT Applications and Infrastructures in Conflict, Crisis,

These challenges are further compounded by the fact that not all regions are embedded in regional organisational frameworks and not all states within a region are necessarily a part of its regional structures, such as the example of Kosovo and Israel. In this context, the UN serves the crucial function of a "safety net" by providing an inclusive platform for all states to engage in cyber CBM processes, such as through the global PoC directory.[63]

Factor 6: Institutional Design

The aforementioned challenges that stem from the composition of participating states can be reinforced by structural constraints: the ARF processes, for instance, are typically slow and consensus-driven, involve multiple layers of approval and lack a dedicated secretariat to actively support and sustain implementation efforts. As a result, only a very limited number of activities are adopted each year, and progress can be easily stalled.[64] This suggests that challenges to effective adaptation and implementation do not stem solely from state behaviour and are rooted in **institutional design** as well.

This illustrates how the institutional setup of cyber CBM processes can differ across multilateral frameworks. The same applies to the design and formal status of the CBMs themselves. For instance, ECOWAS uniquely adopted its cyber CBMs through a directive, giving the measures a legally defined basis rather than making participation purely voluntary. However, member states retain discretion regarding how the agreed-upon objectives are achieved, as the details of implementation are not specified. It remains to be seen how this situation will develop and whether there will be any differences in the long-term implementation of the measures compared to purely voluntary ones.

A common feature across the OSCE, ARF, OAS and ECOWAS is the existence of dedicated working group meetings focused specifically on cyber CBM implementation. These meetings serve as a driver of implementation by creating continuity, fostering a degree of institutionalisation and providing regular opportunities for participating states to exchange updates on progress, discuss implementation challenges and, perhaps most importantly, create informal spaces where personal relationships and trust can gradually develop. That said, the frequency of these meetings vary considerably across organisations. Within the OSCE, for example, CBM 11 formally calls for three such meetings to be held per year; however, in practice, as many as four meetings are often held, with broad participation by the states involved. In contrast, the OAS and ARF

War, and Peace).

63 OEWG Chair (2025): (6th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025).

64 Seng Tan, See (2019): Rejuvenating the ARF: Challenges and Prospects. In: CSCAP Regional Security Outlook + ARF the next 25 years. // Hassan, Mohamed Jahwar (2021): The ASEAN Regional Forum: Challenges and Prospects. // Simon, Sheldon (2013): The ASEAN Regional Forum - Beyond the Talk Shop?

generally have only one dedicated meeting annually, while the ECOWAS currently also aims to have one meeting per year. In the ARF, many of these meetings have continued to be held in hybrid formats since the COVID-19 pandemic and due to travel restrictions to Russia since the beginning of the war, which was the host country for this meeting in 2024. Such hybrid meetings have increased accessibility in some cases and ensured continuity while simultaneously reducing opportunities for informal interaction.

The COVID-19 pandemic further illustrated how implementation models matter. While all organisations were affected by restrictions on in-person engagement, the ARF was particularly vulnerable because its implementation model heavily relied on workshops. Other organisations demonstrated greater adaptability: the OAS expanded online learning initiatives, while the OSCE continued to extend their alternative implementation formats, including manuals and e-learning courses. In general, having a variety of different implementation activities can help ensure successful implementation, as not every format is equally suitable for every cyber CBM or for all states. Resources such as manuals or e-learning courses can contribute to continuity by providing knowledge over the long term, as opposed to a one-time workshop.

Factor 7: Consensus Building

A key challenge at the formulation stage, which also has direct implications for implementation, is **consensus building**. Multilateral cyber CBMs are typically adopted through consensus, which requires all participating states to agree on their wording. Some CBMs – particularly those that are less politically sensitive or build on existing practices, experiences, resources or initiatives – are easier to agree upon, whereas others address more contentious issues and, therefore, face greater resistance.

For example, there was broad support for UN CBM 1 to establish a global PoC directory as well as for ECOWAS CBM 2 to establish a regional PoC directory, partly because many states were already familiar with them and their benefits through their participation in regional cyber CBM processes that already had such PoC directories in place. Such measures, which are easier to agree on, are vital for getting the process off the ground, so that all involved states can gain joint initial experience and achieve early successes with the process. Furthermore, this may help secure long-term, incremental support for more sensitive or more intrusive measures.[65]

Other CBMs address more contentious areas, such as OSCE CBM 9, which involves sharing and subsequently agreeing on common definitions of key cybersecurity terms.[66]

65 OSCE (2012): OSCE Guide on Non-military Confidence-Building Measures (CBMs).

66 “In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an

This has always been a polarising, contentious issue – a fact that is clearly reflected in the compromise regarding the name of the OSCE cyber CBMs: cyber/ICT security CBMs.[67]

Existing political tensions can further complicate the process of achieving consensus, as states may oppose proposals based on broader geopolitical rivalries – i.e. not based on what the proposal is but, rather, on who is in favour of it or suggesting it.[68]

The formulation phase (sometimes) prioritises finding some kind of compromise to achieve consensus over ensuring clarity or feasibility. This can result in broadly formulated measures without detailed guidance or clearly formulated steps, which can lead to significant challenges during implementation.

The inclusive nature of consensus-based processes also has positive effects with respect to successful implementation, as broad participation fosters a sense of ownership among states. Ultimately, all organisations share the common feature of multiple proposals being made before being discussed, and fine-tuned and, finally, getting narrowed down to those which were possible for all states to adopt through consensus. This enhances the legitimacy of CBMs and increases the likelihood that the states will remain engaged in the implementation phase.[69] One example illustrating this is the extensive, inclusive negotiating process employed for the UN CBMs within several Open-Ended Working Group (OEWG) sessions. Another example of this is the development of the most recent ECOWAS cyber CBMs, which were jointly developed by representatives of all member states during workshops.

Factor 8: Dedicated Secretariat

A key driver of effective implementation – and, importantly, of raising awareness and institutionalisation as well as observable implementation activities and, thus, continuity – is the presence of a (neutral) **dedicated secretariat** within a multilateral organisation. This is, of course, connected to the factor of institutional design discussed earlier. However, an analysis of existing cyber CBM frameworks shows that secretariats are often the primary catalysts of implementation. It is for this reason that this has been considered within this analysis as an independent factor that becomes especially relevant at the implementation stage.

explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary."

67 Ghernaouti, Solange and Crespo, Laura (2017): Building Confidence in the Cyber Realm as a Means of Preventing Conflict - a Swiss Perspective. In: European Cyber Security Journal 3 (1), pp. 10-25. // Ben Hiller (2018): OSCE Experts: Cyber/ICT Security (Video Interview).

68 e.g. see here: Common Space EU (2017): Analysis: Armenia and Azerbaijan hold the OSCE to ransom.

69 OSCE (2024): Statement by OSCE Secretariat at the intersessional meeting of the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025.

Analysing different multilateral cyber CBMs processes reveals that secretariats initiate and support activities, raise awareness, track progress, organise meetings and help sustain momentum over time.[70] In doing so, they provide a degree of institutional continuity that is otherwise difficult to achieve in intergovernmental processes.

Within organisations such as the OSCE (OSCE Secretariat's Transnational Threats Department [TNTD]) and the OAS (Inter-American Committee Against Terrorism [CICTE]), secretariats regularly organise workshops, trainings and capacity-building activities – often in cooperation with individual states.[71] They also contribute to the development of practical resources, such as handbooks or e-learning tools[72] and support regular working-level exchanges, including intersessional meetings that allow states to share updates and discuss implementation progress.

Secretariats also play a crucial operational role in maintaining key cyber CBM mechanisms. For example, within the UN,[73] ECOWAS,[74] OSCE[75] and OAS,[76] the dedicated secretariats are responsible for managing the PoC directories by keeping the associated information up to date, conducting communication tests and providing feedback to all involved states regarding response rates or effectiveness. Beyond these technical functions, they also facilitate cross-regional dialogue by preserving institutional knowledge and disseminating best practices. This is particularly visible in UN processes, where representatives from organisations such as the OSCE and OAS have shared their experiences.

Conversely, where such institutional support is absent, implementation generally tends to be more limited. The ARF, for instance, lacks a dedicated secretariat with an implementation mandate in this regard, and responsibility for advancing cyber CBMs rests largely with individual states, which hinders implementation, as it can lead to fewer and less sustained activities.

---

70 Toth, Szilvia (2025): Regional Organisations and Confidence-Building Measures. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James (Eds.): A Handbook for the Practice of Cyber Diplomacy. EU Institute for Security Studies.

71 e.g. the OAS Cyber Diplomacy Training Program, planned and coordinated by the CICTE Secretariat, has held numerous courses for officials working on cybersecurity within member states. The trainings vary in thematic focus and are tailored to different CBM-related topics. In recent years, workshops and masterclasses have covered CBMs in general, international cyber diplomacy, international law and norms in cyberspace, state responses to cyber operations, cyber diplomacy and critical infrastructure, gender and cybersecurity, digital rights and freedoms, IHL in cyberspace, the Programme of Action (PoA), the PoC Directory, and critical cybersecurity infrastructure, among others. When it comes to the OSCE, for example though the project "support for the Implementation of OSCE Cyber/ICT Security Confidence-Building Measures," the organisation has delivered workshops on gender perspectives in cybersecurity, cyber diplomacy, norms, and the CBMs themselves, alongside tabletop exercises testing their practical applicability. These efforts – implemented by the OSCE Secretariat's TNTD and regional missions, sometimes in cooperation with partners – naturally advance multiple CBMs at once. For example, a scenario-based discussion on responding to a major cyber incident linked CBM 5 to CBM 15. A concrete illustration comes from Serbia, where the OSCE Mission supported initiatives ranging from awareness raising and national strategy development to building effective communication channels, strengthening PPPs, and securing critical infrastructure.

72 e.g. OSCE (2023): Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States.; OSCE (2023): E-Learning course on Coordinated Vulnerability Disclosure.; OAS Cyber Diplomacy Training Program.

73 Annex A of the second APR - UN General Assembly (2023): Developments in the field of information and telecommunications in the context of international security. (A/78/265).

74 ECOWAS (2024): Directive C/DIR.2/12/12 on Cyber/ICT Confidence Building Measures.

75 OSCE (2022): The OSCE Secretariat's intervention at the OEWG intersessional meeting.

76 OAS' Representative (2022): (7th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Third Substantive Session (25-29 July 2022).

At the same time, the role of secretariats has clear limits. While they can facilitate processes, provide expertise and implement activities, the success of the CBMs ultimately depends on the states participating in the process. Trust, in particular, cannot be generated by institutions alone. Moreover, secretariats can only act within the mandates, resources and level of confidence granted to them by states. As has been aptly noted in the OSCE context, multilateral institutions "cannot make states pick up the phone".[77]

Factor 9: Financial and Human Resources

Considering the long-term nature, multilateral CBMs require sustained engagement, regular activities and continuous maintenance – all of which require **financial and human resources**. Thus, resources are a cross-cutting factor with implications for both the formulation and the implementation of cyber CBMs.[78] Their availability is among the most fundamental determinants of whether political commitments can be initiated in the first place and then translated into sustained practical implementation, which makes this one of the most important factors that can either drive or hinder the effectiveness of such processes.

Many states – particularly smaller ones or those with limited resources – have only a small number of personnel dedicated to cybersecurity, sometimes with the same experts being responsible for a wide range of issues.[79] As a result, participation in multiple international processes can strain existing capacities and force prioritisation, potentially affecting the implementation of cyber CBMs across all stages of their lifecycle.[80] During negotiations, states may also be reluctant to commit to measures or processes that they lack the resources to implement. A possibility enabling such a process is therefore to adopt only a small number of CBMs as a first step, which was done within the ECOWAS.

The rotation of diplomatic staff presents an additional challenge with regard to continuity. When responsibility for cyber CBMs moves between officials, maintaining institutional knowledge requires deliberate investment in handover processes and the involvement of multiple relevant actors. Some states have sought to address this challenge by involving both diplomatic and technical experts in cyber CBM processes. For example, the Czech National Cyber and Information Security Agency (NUKIB) also engages in OSCE CBM processes.[81] However, maintaining such broad participation itself requires additional

77 Hiller, Ben (2018): OSCE Experts: Cyber / ICT Security. // OAS CICTE (2024): Presentation. Secretariat of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

78 Kavanagh, Camino & Crespo, Laura (2019): Confidence Building Measures and ICT. European Foreign Affairs Review 24 (2), p. 187–202.

79 see for instance, OAS CICTE (2025): Sixth Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace. Report. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.21/25. // OAS CICTE (2024): Presentation. Secretariat of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace. // Or as Nauru puts it within their statement at the plenary session of the Global Mechanism in July 2026: "In Nauru, the people responsible for our cybersecurity, our diplomacy and our digital policy are often one and the same within our public service. This is not a complaint. Rather, this is our context."

80 Global Cyber Policy Dialogue - Western Balkan (2023): Meeting Summary.

human resources.

During implementation, having different levels of resources can lead to uneven participation and limit the effectiveness of certain measures. The resource requirement of individual cyber CBMs varies considerably. Measures such as OSCE CBM 4, which focuses on capacity-building activities, require sustained institutional engagement and coordination. Other measures may seem relatively inexpensive at first glance but require ongoing investment over time at the national level as well as within the organisation. PoC directories, for example (UN CBM 1, OSCE CBM 8, OAS CBM 2 and 3, ECOWAS CBM 2 and ARF CBM1), represent a core element across multilateral cyber CBM frameworks and initially seem straightforward to implement, as they primarily involve the designation of national contact points. However, maintaining such mechanisms – ensuring that the information remains up to date, conducting and participating in regular tests and promoting the use of the directory – requires sustained human effort and institutional attention.

The resources available to multilateral organisations are often dependent on contributions from its member or participating states or voluntary funding for specific activities.[82] This can make CBM implementation vulnerable to shifts in political priorities and broader geopolitical developments. One consequence of the current crisis in the international order, for example, is that some states, including the US, have reduced their engagement with international organisations, including financial contributions, adding to the liquidity challenges faced by the UN.[83] The OAS has historically relied heavily on US funding for cybersecurity-related initiatives, which means that changes in US policy under the Trump administration have affected the scope and continuity of some activities.[84]

When it comes to effective implementation, the ability to make efficient use of available resources is a crucial enabler. Activities that advance multiple CBMs simultaneously can help reduce the financial and human resources required for implementation. Within the OSCE, for instance, CBMs 2, 4 and 6 all focus on strengthening cyber resilience, preparedness and risk reduction and are thus often advanced through joint workshops and training activities.[85] Similarly, CBMs 3, 8, 10 and 13 all aim to facilitate communication and crisis management between participating states.[86] Rather than addressing these measures separately, the OSCE regularly conducts cyber exercises that operationalise

81 https://nukib.gov.cz/en/about-nukib/organizational-structure/

82 Sapala, Magdalena & Stutzmann, Sophia (2020): Understanding the financing of intergovernmental organisations. A snapshot of the budgets of the UN, NATO and WTO. Briefing for the European Parliament.

83 Kenny, Charles (2025): US Funding of International Organizations Has Collapsed. // Dingwerth, Klaus, Witt, Antonia, Lehmann, Ina (2019): International Organizations under Pressure: Legitimating Global Governance in Challenging Times. Oxford University Press.

84 Perina, Rubén M. (2025): The OAS Is Fragile Ahead of a Key Election.

85 OSCE (2024): Statement by OSCE Secretariat at the intersessional meeting of the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025.

86 Radicevis, Velimir (2017): Promoting Cyber Stability between States: OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (ICTs) in the Context of Global and Regional Security. In: IFSH: OSCE Yearbook.

several of them simultaneously by testing these mechanisms.

A similar dynamic can be observed in the OAS. Its e-learning course supports the implementation of several cyber CBMs – specifically CBMs 4, 5, 7, 8 and 9 – by building knowledge and awareness among member states while enabling available resources to support several measures simultaneously. Likewise, the OAS cyber portal serves as a shared resource that directly supports the implementation of CBMs 1, 2 and 3.[87]

Building on existing initiatives can similarly reduce resource requirements. For example, the UNIDIR Cyber Policy Portal was utilised as a part of UN CBM 3, the OSCE was able to build on an existing communications network for CBM 10, and the OAS was built on existing capacity-building initiatives.

The development of cyber CBMs in the ECOWAS region provides another example of how external resources can support implementation. The process as a whole has been supported by Germany as an external donor, which was a crucial enabling factor.[88] However, such external support can also create structural dependencies and raise questions about the long-term sustainability of CBM processes if funding declines or donor priorities shift.[89]

Factor 10: Capacity, Knowledge and Cyber Maturity

Financial and human resources alone do not determine whether states are able to implement cyber CBMs. States also **differ significantly in their institutional, technical and knowledge capacities**.[90] These differences dictate their ability to meaningfully participate in CBM processes and can affect the extent to which individual measures can be implemented in practice.[91]

While implementation challenges related to capacity exist in all regions, they are particularly prominent in highly diverse settings. Such differences can create different starting points for implementation within the same regional process.[92] This is, for instance, relevant for cyber CBMs that rely on information sharing, such as the exchange of national strategies and legal frameworks (e.g. OSCE CBM 7, ARF CBM 2, ECOWAS

87 OAS CICTE (2024): Presentation. Working Group on Cooperation and Confidence-Building Measures in Cyberspace.
88 Embassy of the Federal Republic of Germany Abuja (2025): Press Release.
89 Aderinto, Adegoke John & Joseph, Samson Ikoh (2026): Foreign Aid Dependency and the Politics of Development in the African Economy.
90 ITU (2024): Global Cybersecurity Index 2024.
91 see for instance, OAS CICTE (2025): Sixth Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace. Report. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.21/25.
92 Barrett, Kerry-Ann (2025): Cybersecurity and Its Influence on Traditional Diplomacy in the Americas. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James (Eds.): A Handbook for the Practice of Cyber Diplomacy. EU Institute for Security Studies. // n.n. (n.d.): OSCE: implementation problems of the Confidence Building Measures (CBMs).

CBM 1 and OAS CBM 1) or incident response practices (e.g. OSCE CBM 15 and OAS CBM 11). For states with well-developed cybersecurity ecosystems, such information may already be readily available and can be shared with relative ease, but other states may still be at an earlier stage of developing basic concepts, policies, institutional structures or technical capabilities.[93] For example, while some states, such as the US and France, may already have established systems for classifying cyber incidents and can engage relatively easily in detailed exchanges as envisaged under OSCE CBM 15[94] or OAS CBM 11,[95] others may first need to develop the domestic structures required to properly generate and organise such information.[96]

Consequently, a lack of information sharing does not necessarily indicate a lack of willingness to implement a CBM and may instead reflect structural limitations in a state's ability to generate, process or share the relevant information. This distinction is important when assessing implementation: differences in observable implementation may partly reflect differences in capacity rather than those in political commitment.

These capacity differences create a structural challenge for multilateral CBMs, which ultimately rely on a certain degree of reciprocity.[97] If states have extremely different capacities to implement a measure, implementation may become uneven, rendering some states unable to engage on equal terms.

To address resource gaps, several multilateral organisations, such as the OSCE and OAS, have integrated targeted cyber capacity-building efforts into their CBM processes. In the OSCE, for instance, many such activities are carried out under the "Activities and Customized Support for the Implementation of OSCE Cyber/ICT Security Confidence-Building Measures" project, which is funded by voluntary financial contributions from participating states.

Factor 11: Ownership

Implementation processes are often driven by individuals: highly motivated and well-connected actors, such as diplomats, chairs of working groups[98] or the staff of international organisations. Such individuals can play a key role in advancing

93 Of course states would not build up such structures or draft a cybersecurity strategy for the sole purpose of implementing cyber CBMs, rather, such a process would be initiated to enhance overall cyber resilience.

94 "Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies. Collaboration may, inter alia, include: (...) Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident (...)."

95 "Develop national cyber incident severity schemas and share information about them."

96 OSCE (2022): Cyber Incident Classification. A Report on Emerging Practices within the OSCE region.

97 OSCE (2012): OSCE Guide on Non-military Confidence-Building Measures (CBMs).

98 OEWG Chair OEWG (2025): (6th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025).

processes.[99] However, this also creates vulnerabilities: if progress depends too heavily on specific actors, continuity may be at risk if they leave. Therefore, the establishment of mechanisms to create ownership is essential to ensure the sustainability of CBM implementation.

Additionally, across different multilateral settings, smaller groups of states have often played a key role in driving cyber CBM processes forward. Within the UN framework, cross-regional groups of states, such as the Confidence Builders,[100] have played a vital role in maintaining momentum, breaching divide, proposing concrete ideas and engaging with states that had reservations or questions.[101] Through their engagement with the topic – which could have potentially been inspired by its alignment with their political priorities – they took over responsibility and, consequently, sought ownership.

A particularly effective feature of such groups has been their diversity: coalitions composed of states from different regions or political alignments are often better positioned to build bridges, foster dialogue and advocate for CBMs among a wider set of participants. This enhances such groups' legitimacy, increasing the likelihood that their proposals will be taken seriously by other states as well as by the OEWG's chair. The Confidence Builders group includes states from different political camps that are continuously shaping the discussions surrounding cyber issues. Support from leadership figures, such as the Chair of the OEWG, has further contributed to keeping CBMs on the agenda and advancing the process.

One example of a successful approach to institutionalising implementation is the OSCE's "adopt a CBM" initiative, which was launched in 2018. Under this framework, participating states assume responsibility of specific CBMs by developing discussion papers outlining implementation pathways, conducting questionnaires to map national approaches and organising supporting activities.[102] This not only distributes the burden of implementation but also strengthens ownership and helps ensure continuity over time. Hence, it contributes to awareness and institutionalisation as well as to observable implementation activities.

Factor 12: Operationalisation

There are several reasons for the **gap between CBMs being in place and their practical**

99 Toth, Szilvia (2025): Regional Organisations and Confidence-Building Measures. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James (Eds.): A Handbook for the Practice of Cyber Diplomacy. EU Institute for Security Studies.

100 The Group of "Confidence Builders" is an open, informal, cross-regional group of states consisting of Australia, Brazil, Canada, Chile, Colombia, Czech Republic, Dominican Republic, Fiji, Ghana, Germany, Israel, Jordan, Republic of Korea, Mexico, The Netherlands, Singapore, Uruguay. It was first initiated during the OEWG's but also continues to exist within the new permanent mechanism.

101 OEWG Chair (2025): (6th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025).

102 OSCE (2023): 10 Years of OSCE/ICT Security Confidence-Building Measures.

use. For example, states with strong bilateral relations often rely on established, more direct communication channels, which may be faster, less formal, better known and more trusted than cyber CBM-specific mechanisms within a multilateral organisation. Conversely, in politically strained relationships, requests made through cyber CBM channels may be ignored or met with reluctance. In other cases, states may simply lack the technical or institutional capacity to respond (which draws attention back to the previously described challenge related to different levels of resources and cyber maturity). As a result, the practical uptake of such cyber CBMs can remain limited.

The implementation of OSCE CBM 10[103] illustrates the broader challenge involved with moving from formal implementation to actual operational use. Significant progress has been made in this regard: a shared understanding of the measure exists, and an increasing number of participating states have connected to the OSCE Communications Network. However, the mechanism has seen limited practical use. One reason for this is that the platform can be cumbersome to use in time-sensitive situations.

In practice, national Computer Emergency Response Team (CERTs) and technical authorities often rely on faster, more informal communication channels that they already trust and use regularly. Consequently, the added value of formal diplomatic mechanisms was not always immediately evident to technical actors, challenging the implementation of CBMs aiming to establish communication channels. This is related to the recurring challenge that technical and diplomatic communities often operate very differently. Successfully implementing cyber CBMs frequently requires bridging the gaps between these communities – a task that can be difficult in practice.

Cyber incidents such as the operation targeting Ukraine's power grid in 2015 could, in principle, have been addressed through the existing cyber CBM crisis management mechanisms (OSCE CBMs 3, 8, 13 and 16), but, according to publicly available information, this did not happen in this case.[104]

Nevertheless, Nauru, for instance, stated the following: "It is precisely because we are small that CBMs matter so much to Nauru. In a serious ICT incident, a small state's response begins with a question: who do we call?"[105] Tonga argues, "Small states do not maintain wide networks of diplomats tasked with cyber-related cooperation. When an incident strikes, trusted, predictable lines of communications between states are needed. Tonga, therefore, strongly supports the Global Points of Contact Directory (...)."[106]

---

103 "Participating States will voluntary exchange views using OSCE platforms and mechanisms inter alia, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs."

104 Marino, Luigi (2018): Give Diplomacy a Chance. OSCE's red Lines in Cyberspace.

105 Tonga's representative (2026): (7th meeting) Plenary Session, Global Mechanism on ICTs in the Context of International Security (20-24 July).

106 Vanuatu's representative (2026): (7th meeting) Plenary Session, Global Mechanism on ICTs in the Context of International Security (20-24 July).

The broader challenge and its importance is highlighted by the OSCE stating that "CBMs are designed with practical application in mind and are only considered 'implemented' by an OSCE participating State if actively used".[107] A statement was made by the representative of Vanuatu at the 2026 meeting of the Global Mechanism as follows: "Confidence is not built by the number of channels that exist or the volume of requests within them, but by the certainty of what happens when one is used."[108]

Factor 13: Understanding of Each CBM

A factor that affects practical CBM use is the **varying degree of concretisation across different cyber CBMs**.[109] Some measures are relatively concrete and describe specific working steps, such as OSCE CBM 11 stating that there should be three intersessional Working Group Meetings a year. Further, CBMs concerning the PoC directory clearly describe necessary working steps to implement the CBM. Others, however, are formulated with a higher level of abstraction, functioning more as general commitments or political signals than as operational measures.

In some cases, this can be explained by consensus building during the formulation stage. However, vague language may lead to divergent interpretations, uneven implementation or situations in which almost any activity can be framed as implementation – potentially diluting the effectiveness of the measure. It can be observed that cyber CBMs that include a concrete shared vision are generally at a more advanced stage of implementation or have greater levels of implementation activity than other ones that are less clearly defined.

Initial ambiguity does not necessarily preclude success. If sufficient political will exists, broadly formulated CBMs can serve as a starting point for iterative development, enabling states to gradually specify and operationalise measures over time. Initiatives such as the Confidence Builder group in the UN context have demonstrated that sustained dialogue and cooperation can help translate general commitments into more concrete practices.

A promising trend has also emerged in recent OEWG sessions: more states now highlight their national cyber CBM activities and explicitly link them to specific UN cyber CBMs.[110] Such efforts help clarify the purpose of each measure, manifest them in the

107 OSCE Secretariat (2020): OSCE Cyber Security Awareness Month.

108 Nauru's representative (2026): (7th meeting) Plenary Session, Global Mechanism on ICTs in the Context of International Security (20-24 July).

109 cf. Mason, Simon J. A.; Siegfried, Matthias (2013): Confidence Building Measures (CBMs) in Peace Processes. In: Managing Peace Processes. Process related questions. A handbook for AU practitioners, pp. 57–77.

110 e.g. Germany (2024): "I would like to focus in particular on CBM2 (...) and CBM6 (...). As part of our ongoing CBM implementation efforts and in line with our G7 ECOWAS cybersecurity action plan, Germany organized a study trip of an ECOWAS delegation to Vienna in September this year. The delegation, alongside representatives from the OAS, the African Union, and the OSCE, participated in the inter-regional conference on cybersecurity organized by the Republic of Korea, North Macedonia, and the OSCE Secretariat. Moreover,

real world and provide models that others can follow. At the same time, these examples – which include highlighting conferences and novel laws, joint research projects or capacity-building efforts – also illustrate how broad the idea of implementing these cyber CBMs is, as they are formulated in a very broad manner.

Factor 14: Measurability

Such varying degrees of concretisation lead to **varying degrees of measurability across different cyber CBMs**, which also affects their practical use.[111] Some of the adopted multilateral cyber CBMs allow for relatively straightforward tracking of their implementation through clearly identifiable outputs, including the following:

- Meetings held; for example, OSCE CBM 11 can be assessed by examining whether meetings have taken place, how frequently they have been held and which states have participated.
- Points of contact (PoCs) nominated; for example, under OSCE CBM 8, UN CBM 1, ECOWAS CBM 2 and OAS CBMs 2 and 3, implementation can be assessed by identifying how many and which states have nominated PoCs.
- Mechanisms established; for instance, OAS CBM 11 can be assessed by examining how many and which states have established a national cyber incident severity schema.

With less concrete cyber CBMs that describe general commitments or political signals instead, implementation is largely implicit. However, there is a possibility that clear measurable indicators can enable implementation by enhancing accountability.[112]

Verification is not the goal of CBMs.[113] A certain degree of flexibility is inherent to CBMs and can be beneficial, allowing states to adapt implementation to their specific contexts. The key challenge, therefore, lies in striking a balance between flexibility and clarity. Without a shared understanding and measurability, such as in the form of regular reviews of objectives and expected outcomes, implementation risks becoming fragmented and inconsistent across states.

---

the ECOWAS delegation observed a meeting of the informal working group of the OSCE, which provided useful insights into regional CBM implementation practices." (Germany's representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024)) or UK (2024): "In support of CBM 7, the UK continues to develop and share tools to raise the resilience of critical national infrastructure internationally. Since 2019, the UK has supported the assessment of national cybersecurity risks in nearly 20 countries" (UK's representative (2024): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024)).

111 cf. Mason, Simon J. A.; Siegfried, Matthias (2013): Confidence Building Measures (CBMs) in Peace Processes. In: Managing Peace Processes. Process related questions. A handbook for AU practitioners, pp. 57–77.

112 Find more ideas on the question of measurability in the cyber domain in Reinhold, Thomas (2021): Toward a Cyber Weapons Assessment Model—Assessment of the Technical Features of Malicious Software.

113 Holst, Johan Jorgen (1983): Confidence-building Measures: A Conceptual Framework. In:Survival 25 (1), pp. 2-15.

Factor 15: Non-Abuse

Finally, the effectiveness of CBMs ultimately depends on their use in good faith.[114] Hence, the **potential misuse** of CBM mechanisms constitutes a significant challenge to individual CBMs as well as the process as a whole. If such instruments are exploited in a way that undermines their purpose, this can erode trust, reduce their practical utility and ultimately weaken the overall process.

Concerns regarding such risks have already been raised in international discussions, particularly in the context of the UN. For example, during recent sessions at the UN level, states expressed apprehension regarding the possible misuse of the global PoC directory. France, for example, urged other states to "not exploit this tool, to not overuse the tool, at the risk of making it inoperable".[115] These concerns were later echoed and further specified in a joint statement made by Germany and France, which highlighted the risk that repeated or unfounded requests – despite the availability of established channels – could place undue strain on national cybersecurity agencies. It was argued that such practices risk undermining both the credibility of the mechanism itself and the broader diplomatic efforts underpinning it, particularly by weakening trust between technical and diplomatic communities. The concerns were supported by additional states in 2026, including Tonga and South Korea.[116]

As mentioned earlier, institutional design can also be exploited for abusive purposes: for instance, during the implementation of cyber CBMs within the ARF, the requirement for consensus-based decision-making was frequently used to stall implementation activities. The reasons for undertaking such actions are presumably not related to the specific activity itself and believed to stem from politicisation or tensions among the participants.

Furthermore, the "one bad apple" scenario can lead to challenges in this context. For example, if there is a state participates with whom information cannot be shared under any circumstances, it could result in no information may be shared at all with any of the other participating states.

---

114 OSCE (2012): OSCE Guide on Non-military Confidence-Building Measures (CBMs).

115 France's Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024)

116 Germany's Representative (2025): (6th meeting) Openended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025) in a joint statement with France. // The concern was reiterated recently during the first plenary session of the Global Mechanism in July 2026 (find the statement here, as well as Tonga's statement here, and South Korea's statement here).

Key findings: patterns across enablers and challenges

CBMs can serve as an important starting point for diplomatic engagement, particularly when deeper forms of cooperation remain out of reach. However, building and sustaining confidence in cyberspace is far from straightforward: trust is difficult to establish, easily undermined and requires continuous effort to maintain. Translating political commitments into sustained practice requires more than just the adoption of the agreed-upon measures. This study identifies several factors that dictate whether cyber CBMs are properly implemented, highlighting not only the obstacles that hinder progress but also the conditions under which implementation can be strengthened.

One of the key findings is that the factors that impede implementation outnumber those that actively facilitate it. However, these categories are not clear-cut: most factors can either enable or constrain implementation depending on the context. Political will, for instance, can sustain engagement, while its absence can stall an otherwise well-designed process. Institutional arrangements can provide continuity and support, but their effectiveness depends on the resources available to maintain them. Therefore, implementation depends not only on creating favourable conditions but also on managing the constraints that can undermine progress. Nevertheless, some conditions can be actively fostered, particularly through institutional design, the strategic use of political windows of opportunity and the creation of ownership by individual states or groups of states.

A further finding of this analysis is that these factors are interconnected rather than independent. Political will can facilitate resource allocation, which strengthens implementation capacity; implementation activities can, in turn, help build trust and reinforce political support. The reverse is also possible: weak implementation can undermine confidence in the process, further reducing political commitment and resources.

The relevance of individual factors also varies across the stages of a CBM process and between regional contexts. Some factors are particularly crucial during formulation, while others become more relevant during implementation (see Figure 1). Established processes may benefit from institutional experience and support structures, whereas newer initiatives may face greater challenges in terms of securing ownership and continuity. Differences in states' resources and cyber maturity, along with regional security dynamics, further shape what CBMs can realistically achieve. Thus, there is no "one size fits all" model for successful implementation when it comes to regional processes; efforts to strengthen CBMs need to account for the specific conditions and needs of each

process.

Taken together, the findings of this analysis highlight the central role of political will and sustained political engagement. Although cyber CBMs address technical issues and may depend on technical expertise, their implementation ultimately relies on political decisions regarding priorities, resources, cooperation and continued participation. While a state's technical capacity matters, it cannot compensate for a lack of political commitment. Conversely, political support alone may be insufficient if the state lacks the capacity to act. Hence, successful implementation requires political willingness as well as the practical means to translate commitments into action.

Cyber CBMs: unique or just another multilateral policy process?

Many of the factors identified in this study are not unique to cyber CBMs, or even to CBMs more broadly. Political will, institutional design, resources, continuity and clarity of objectives have been found to be recurring determinants of implementation across multilateral policy processes, particularly those based on voluntary and non-binding commitments.[117] The findings may, therefore, also inform efforts to understand implementation in other policy domains.

What distinguishes cyber CBMs is the context in which these familiar challenges arise. Persistent uncertainty regarding cyber threats and state behaviour, significant differences in terms of cyber maturity and competition for political attention and resources can complicate implementation. Furthermore, relevant expertise and responsibilities are often distributed across various national authorities, while non-governmental actors may also play a role in the cyber domain without being systematically included in CBM processes. These characteristics amplify well-known implementation challenges.

Another important distinction is related to the security environment in which cyber CBMs operate. Multilateral cyber CBMs are primarily designed as preventive instruments intended to reduce risks before crises emerge; however, in general, CBMs have often also been used in post-conflict settings, situations of prolonged tension or even during ongoing armed conflicts. In such contexts, implementation comes with additional challenges other than the ones discussed within this paper: Actors may have limited interest in reducing tensions, deep historical grievances may continue to shape perceptions and broader questions of reconciliation can affect the willingness to

117 Dominioni for instance analysed multiple PoC directories across different fields and came to the summarizing conclusion, that in whatever field non-responsive PoCs - either due to a lack of capacity or deliberate misuse -, lacking updates, as well as concerns about the safety and reliability of the communication channel can challenge the success of such directories, thus, such challenges are not unique to cyber PoC directories (find the study here).

implement the CBMs. Experiences from regions such as the Western Balkans demonstrate that confidence-building is often embedded within the wider political and societal processes of rebuilding trust.[118] While CBMs can help maintain communication channels and reduce risks, in such settings, there is also the risk that successful CBM cooperation can create an illusion of progress while more fundamental political disputes remain unresolved.[119] Consequently, the objectives and expectations surrounding CBMs will likely differ depending on the settings in which they operate.

Implementation as a continuous process

Cyber CBM implementation is best understood as a continuous and iterative process rather than a linear sequence that has a defined endpoint. Progress varies across measures and regions: some CBMs remain at an early stage, while others become established practices. Even well-established measures, however, may have scope for further operationalisation, more consistent use or more ambitious implementation.

Progress may also become visible through incremental developments that extend beyond the immediate outputs of individual measures. These include improvements in cyber capacity and resilience or the strengthening of bilateral and multilateral partnerships and may manifest through increased dialogue on the topic, coordinated positions in international negotiations, implementation of joint projects, diffusion of norms and language across related international forums[120] or gradual institutionalisation of cyber issues within foreign policy agendas. In some regions, such as the OAS, it is highly likely that the cyber CBM process has contributed to such shifts. Broader trends may also serve as indicators of success, such as a growing number of states participating in cyber CBM implementation activities or the emergence of new regional cyber CBM processes. These developments suggest that states perceive value in such initiatives and expect tangible benefits from engagement.

Finally, the process itself often matters as much – if not even more – as the individual outputs it generates. Particularly during periods of geopolitical tension, the continued willingness of states to engage with each other, exchange views, participate in joint activities and maintain communication mechanisms may constitute a significant success in its own right.

118 OSCE (2012): OSCE Guide on Non-military Confidence-Building Measures (CBMs).

119 Mason, Simon J. A.; Siegfried, Matthias (2013): Confidence Building Measures (CBMs) in Peace Processes. In: Managing Peace Processes. Process related questions. A handbook for AU practitioners.

120 Kavanagh, Camino & Crespo, Laura (2019): Confidence Building Measures and ICT. European Foreign Affairs Review 24 (2), p. 187–202.

Making cyber CBMs work: bridging the implementation gap

The preceding analysis identified factors that influence the success of multilateral cyber CBM processes. Building on these findings, this chapter outlines a set of practical recommendations aimed at strengthening multilateral cyber CBM processes.

Strengthen a shared vision

Cyber CBMs are often interpreted differently by different states. Therefore, developing a common understanding of the objectives and expected outcomes of cyber CBMs via structured exchanges should be consider a priority.[121]

A vital element of such exchanges should be a stronger focus on the practical benefits of cyber CBMs. States should be encouraged to share success stories and concrete implementation experiences. Existing examples – such as the operational use of PoC directories[122] – can help demonstrate that cyber CBMs are not merely political declarations and can generate practical value. Making these experiences more visible could provide inspiration for other states and strengthen confidence in the process.

Additionally, states should exchange experiences related to implementation challenges, unsuccessful approaches and "potential pitfalls".[123] Understanding why certain measures proved difficult to operationalise – or why specific approaches failed – can be just as valuable as highlighting good practices. Such discussions require a certain degree of trust, and they help normalise implementation challenges and enable states to learn from one another instead of repeatedly facing similar obstacles in isolation.

For instance, prior to Working Group meetings, the OAS CICTE Secretariat sends out a standardised questionnaire asking about challenges or considerations relating to implementation; the secretariat then shares the results of this questionnaire, in anonymised form, with all member states.[124] Such a practice can serve as a valuable experience to learn from. Recent discussions within the UN OEWG have also demonstrated an encouraging trend, with an increasing number of states linking national

121 cf. OSCE (2012): OSCE Guide on Non-military Confidence-Building Measures (CBMs).
122 For instance, Germany and Czech Republic shared such experiences regarding the OSCE PoC Directory at the UN level as part of the Confidence Builder group (cf. Germany as part of the OEWG Confidence Builders (2023): Input Paper, CBMs in Action. // Czech Republic as part of the OEWG Confidence Builders (2024): Joint Working Paper, How information sharing contributes to security and stability in cyberspace: Examples from Regional Points of contact networks.)
123 Singapore's representative (2025): (5th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025)
124 Find here a couple for questions as an example:

activities to specific cyber CBMs (e.g. Germany and the UK),[125] effectively contributing to a more concrete vision of the cyber CBM by mapping their implementation efforts.

Similarly, states participating in cyber CBM processes should periodically reflect on whether existing cyber CBMs remain fit for purpose or whether their interpretation needs to evolve in accordance with technological developments and the changing cyber threat landscape. Alternatively, states should adopt a very critical view regarding whether, in light of the experiences gained or changed circumstances, it might not be worth devoting further efforts to a specific CBM and whether to focus their efforts on the implementation of others instead.[126]

Secretariats could play a critical role in this regard by creating the space for such exchange to occur and by facilitating discussions on common challenges, for instance, via standardised questionnaires. Nevertheless, individual states, groups of states (such as the Confidence Builder group) or the chair of a working group (such as the case with the "adopt a CBM" initiative within the OSCE) could also take the initiative to start such efforts or at least to put it on the agenda. At the UN level – where, compared to the OAS and OSCE, such an agenda item has not yet been institutionalised – the Dedicated Thematic Groups (DTGs)[127] (DTG 1 most probably fits best) should be used for such exchanges.[128]

Strengthen implementation mapping efforts

The development of a shared understanding of implementation should be complemented by mechanisms that make implementation more transparent and easier to assess. While cyber CBMs are deliberately made voluntary and should not be verified in the same

125 e.g. Germany (2024): "I would like to focus in particular on CBM2 (...) and CBM6 (...). As part of our ongoing CBM implementation efforts and in line with our G7 ECOWAS cybersecurity action plan, Germany organized a study trip of an ECOWAS delegation to Vienna in September this year. The delegation, alongside representatives from the OAS, the African Union, and the OSCE, participated in the inter-regional conference on cybersecurity organized by the Republic of Korea, North Macedonia, and the OSCE Secretariat. Moreover, the ECOWAS delegation observed a meeting of the informal working group of the OSCE, which provided useful insights into regional CBM implementation practices." (Germany's representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024)) or UK (2024): "In support of CBM 7, the UK continues to develop and share tools to raise the resilience of critical national infrastructure internationally. Since 2019, the UK has supported the assessment of national cybersecurity risks in nearly 20 countries" (UK's representative (2024): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024)).

126 One example in this regard is the second part of the OSCE CBM 9, which aims to find shared definitions of key terms. However, it was decided that the implementation of this is no longer an objective. This reflects broader international developments in cybersecurity, where it has become increasingly evident that agreeing on common definitions poses a major challenge, given that divergent political and ideological perspectives are often embedded in the terminology itself.

127 After almost 25 years of temporary UN cyber formats the Global Mechanism on Information and Communications Technologies got established. The mechanism, which had its first plenary session in New York on 20-24 July, it is intended to bring a more action-oriented approach to the existing framework. Apart from the fact that the new mechanism is permanent, the biggest innovations are the two dedicated thematic groups (DTGs) which complement the annual plenary 'by providing the opportunity for more detailed and action-oriented discussion'. As decided in 2025, dedicated thematic group one focuses on challenges and group two on capacity-building. The first meetings of the DTGs are scheduled for 7-11 December. They will be an important next step in assessing whether broad political support can translate into more focused discussions and practical recommendations, including on the chosen focus of the protection of critical infrastructure and the implementation of the agreed framework.

128 See for example here the Dominican Republic suggesting this as well Germany (see here) during the plenary session of the permanent Global Mechanism in July 2026.

manner as, for instance, legally binding arms control agreements, this does not preclude regular reporting or implementation reviews through the use of standardised questionnaires or similar instruments to enable comparison and anchor the exchange of information.[129]

Therefore, states participating in the process should establish more structured mechanisms to document implementation activities, exchange implementation progress and identify any remaining gaps.[130] This is easier to do with certain cyber CBMs (especially those that describe explicit implementation tasks or deliverables) than with others. Hence, it is particularly important in these cases to be able to refer to a shared vision. Examples of this exist, highlighting that such approaches are feasible:

- The minutes of OAS Working Group meetings show that some states are linking their activities to CBMs in a very structured manner (e.g. Trinidad and Tobago[131]). Similarly, during OSCE Working Group Meetings, co-adopters give an update on the current CBM implementation status or upcoming implementation activities.
- The OAS has established regular public institutional reporting, which aims to achieve greater visibility of implementation activities and, thereby, increase transparency, this does not only focus on cyber CBMs but also includes all the CBMs within the organisations. The process of sharing information has been made as straightforward as possible for states; following the update to the website for the cyber PoCs, states can now submit information via a form on the website.
- Another existing resource aiming to map implementation efforts is the National Survey of Implementation of United Nations Recommendations on the Responsible Use of ICTs by States in the Context of International Security, which includes a section on cyber CBM implementation and could serve as a useful starting point for more structured and transparent reporting.

Unfortunately, so far, such resources have not seen a lot of uptake. The UN implementation survey, for instance, has only been filled in and published by two states (Czech Republic and Canada) since its release in 2022. These experiences could be built upon further without duplicating efforts. However, an updated version would be needed. For example, the current UN implementation survey currently includes a section on cyber CBM implementation, but lacks explicit questions about the UN cyber CBMs or specific regional efforts. This would address suggestions, for instance, by Costa Rica as well as Singapore, who advocated for a “repository for states to submit CBMs” or a “directory for what exists regionally”.[132]

129 Mason, Simon J. A.; Siegfried, Matthias (2013): Confidence Building Measures (CBMs) in Peace Processes. In: Managing Peace Processes. Process related questions. A handbook for AU practitioners. // OSCE (2012): OSCE Guide on Non-military Confidence-Building Measures (CBMs).

130 cf. OAS CICTE (2023): Presentation on OAS/CICTE experiences related to the development and implementation of (a) inter-governmental Points of Contacts directories in the area of ICT security, and (b) other confidence building measures relating to ICT security.

131 See here.

132 Costa Rica’s Representative (2021): “Perhaps having a repository for states to submit CBMs, would advance implementation. Such an undertaking would have to be mindful of existing regional structures in this regard. In this regard, perhaps the UNIDIR Portal can act as a directory for what exists regionally, while also providing space for states that are not members of regional organizations to also participate in exchanges“ (cf. (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - First Substantive

Such initiatives should not aim to simply mark CBMs as completed and, instead, should strive to map out the existing implementation efforts and maintain a clear record of developments. Such regular implementation reviews, voluntary reporting templates or dedicated review conferences could help monitor progress over time and identify cyber CBM efforts more explicitly while preserving the voluntary character of CBMs. Such review mechanisms could also be incorporated into CBMs or the CBM processes and be established more firmly both at a later stage in the implementation phase and (ideally) from the outset of a new process.

These measures could contribute to creating awareness or initiating exchanges across different levels and actors, as cyber CBMs are predominantly perceived as a diplomatic tool. However, depending on the specific CBM, it largely depends on implementation on the national level, where technical experts, ministries or police are needed for successful implementation.

Again, secretariats have a particularly crucial role to play in this regard. By collecting implementation data, tracing developments and coordinating reporting processes, they can strengthen institutional memory and ensure that the mapping of CBM implementation remains a persistent agenda item rather than an ad hoc discussion. Nevertheless, individual states (such as the Czech Republic and Canada did to a certain degree), groups of states or the chair of a working group could also take up the initiative to start such efforts or to at least put it on the agenda.

Strengthen ownership

Ownership is a strong driver of successful implementation. Unlike most other enabling factors, ownership can be actively fostered.

Existing initiatives provide valuable inspiration in this respect. The OSCE's "Adopt a CBM" initiative and the ARF's sponsoring-state approach assign responsibility for individual cyber CBMs and encourage states to voluntarily take a role in promoting implementation. Similar models could be adopted in other multilateral cyber CBM processes.[133]

Session (13-17 December 2021)) // or Singapore's Representative (2025): "Given that the full value of CBMs is only realized when they are actively implemented by all States, it is imperative that we concentrate on efforts to accelerate the implementation of these eight global CBMs. In this regard, we believe it is essential for States which are already implementing CBMs to share best practices, the potential pitfalls, and the ways around them. These exchanges could be consolidated in a repository which could be included as a module in the Global ICT Security Co-operation and Capacity Building Portal proposed by India when it is established." (cf. (5th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025))

133 Serbia's Representative (2021): "in 2018, the Chair of the informal working group launched the 'Adopt a CBM' initiative, which saw participating states volunteering individually or in groups to explore how CBMs can be implemented in practice. OSCE CBMs represents a good example of voluntary cooperation in a regional context, and can serve as one of the valuable sources for the future work of this OEWG." (cf. (7th Meeting) Open-ended working group on Information and Communication Technology (ICT) - First Substantive Session (13-17 December 2021))

States that assume responsibility for particular cyber CBMs can prepare implementation guidance, facilitate dialogue, mobilise financial resources, coordinate activities and promote awareness among states. Making such responsibilities more transparent could further strengthen accountability and visibility, such as by publicly communicating which state adopted which cyber CBM within the OSCE in the way that the ARF publishes which state is a sponsoring state for specific measures.

Strengthen and leverage capacities in a sustainable manner

Resource constraints remain one of the most persistent challenges to implementation across all multilateral cyber CBM processes. Hence, long-term implementation requires sustained investment.

Such capacity-building efforts should be driven by clearly defined implementation needs rather than generic cybersecurity assistance. Identifying which capacities are required for specific cyber CBMs and which existing initiatives already address these needs could help avoid duplication and ensure that the limited resources are used efficiently; such efforts already exist with regard to the implementation of cyber norms.[134] Particularly within the UN framework, many CBMs are already being implemented implicitly through the use of existing resources, such as the Cyber Policy Portal. It has also become easier to achieve consensus on cyber CBMs, where these can build on existing initiatives.

Mapping how individual cyber CBMs contribute to the implementation of the voluntary, non-binding norms for responsible state behaviour or the application of international law within the cyber domain could further strengthen the strategic rationale for investing in cyber CBM implementation. The ASEAN Norms Checklist, an initiative designed to drive the implementation of the norms forward, for instance, emphasises the relevance of PoC directories specifically with regard to Norm A. Moreover, the crucial role of regional dialogue in the implementation of all the norms is emphasised on a regular basis.[135]

Academia, think tanks and implementing organisations can, if requested by the states, provide valuable support by conducting implementation mapping, identifying capacity gaps and evaluating the contribution of cyber CBMs to the broader cyber stability

134 cf. Ott, Nikolas & Osula, Maria (2019): The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level. In: 2019 11th International Conference on Cyber Conflict. // See for example ASEAN (2024): ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace. // OEWG Chair (2024): Chair's Discussion Paper on a Checklist of Practical Actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs [Initial Draft]. Annex B. // Dominioni, Samuele & Persi Paoli, Giacomo (2023): Unpacking Cyber Capacity-Building Needs. Part I. Mapping the Foundational Cyber Capabilities. // Esteve, González, Patricia, Axon, Louise, Creese, Sadie, Dutton, William H., Saunders, Jamie, Carver, Julia & Goldsmith, Michael (2026): Cybersecurity capacities for the application of UN cyber norms.

135 See for example: Dominioni, Samuele & Persi Paoli, Giacomo (2023): Unpacking Cyber Capacity-Building Needs. Part I. Mapping the Foundational Cyber Capabilities. // Pawlak, Patryk (2016): Confidence-Building Measures in Cyberspace: Current Debates and Trends.

framework as well as to the implementation of such capacity activities. Finally, in this case as well, the DTGs (DTG 2 would probably be the best fit here) could be leveraged as a space to identify the capacities needed accordingly.[136]

Strengthen cross-regional learning

Regional cyber CBM processes have generated valuable experiences over the past decade.[137] Greater efforts should be made to exchange experiences across regions and systematically learn from existing practices.[138]

Encouragingly, this has already been done and has become more common in recent years through exchanges between organisations such as the OSCE, OAS, ECOWAS, ASEAN, AU and UN.[139] These efforts should be expanded to avoid dependence on individuals.[140] In the future, regular meetings could take place on the heels of the plenary meetings of the Global Mechanism – as suggested by representatives of the regional organisations themselves.[141] Discussions should also extend to regional organisations that have not yet developed cyber CBMs, thus enabling them to benefit from existing experiences and adapt successful approaches to their own regional contexts.

Some states are members of multiple regional organisations and, consequently, are able to make comparisons regarding cyber CBM processes, which should be leveraged. Canada and the US, for instance, are both members of the OSCE, OAS, ARF and UN, while all European states are members of the OSCE and UN and are represented by the European External Action Service (EEAS) within the ARF. Finally, all ECOWAS member states are also members of the UN and AU.

As suggested by multiple states,[142] the DTGs within the UN Global Mechanism could provide a platform for such cross-regional exchange between states – including states that are members of regional organisations that, so far, have not established cyber CBMs or those that are not members of any other regional organisation – as it should not be only

136 As suggested for example by Argentina at the July Meeting of the Global Mechanism in 2026 (see here).

137 This has also been highlighted in a 2025 non-paper on “Inter-regional Cooperation. The Role of Regional Organizations in Implementing the UN Framework for Responsible State Behaviour in Cyberspace.”

138 cf. Ott, Nikolas, and Osula, Anna-Maria (2019): The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level. In: 2019 11th International Conference on Cyber Conflict.

139 The OSCE Secretariat’s TNTD for instance engages in cross-regional exchange via the 2024 ECOWAS study visit to the OSCE, organised by the EU, Germany, and the CBM adopters (find more on this here). Representatives from the AU and the OAS also attended, further strengthening cross-regional dialogue. Another example is a joint interactive workshops as well as participation in the annual meeting of the OSCE national PoCs joined by representatives from Asian states, Australia, OAS and AU in 2026. To gain insight into how OSCE participating states exchange views and share national practices the representatives of these states and regional organisations also observed a meeting of the IWG. Another way of such cross-regional exchange is that representatives of the OSCE, EU, and OAS participate in the UN discussions on ICT security contributing to the dialogue and sharing good implementation practices there.

140 As for example suggested by the AU at the 2026 July meeting of the Global Mechanism (see the statement here).

141 2025 non-paper on “Inter-regional Cooperation. The Role of Regional Organizations in Implementing the UN Framework for Responsible State Behaviour in Cyberspace.”

142 See for example the Dominican Republic's statement at the 2026 July Meeting of the Global Mechanism here, Switzerland's statement here, or Chile’s statement here.

the secretariats that exchange information. Nevertheless, the inclusion of the secretariats of regional organisations within those DTG discussions is crucial to allow them to share their experiences[143] (here both DTGs would be suitable).[144]

Instead of seeking harmonisation, cross-regional cooperation should aim to promote interoperability where appropriate, facilitate mutual learning and strengthen the overall ecosystem of cyber CBMs. For instance, certain cyber CBMs exist in every region, such as the exchange of strategies and similar documents as well as PoC directories. Such CBMs also exist at the UN level, with all states participating in the process. Discussions should, therefore, take place on how these existing efforts in these regions can be utilised to strengthen overall cyber CBM implementation while being mindful of the use of (human) resources.[145]

With regard to the global PoC directory, for instance, the OAS has committed to cooperating with the UN and striving for harmonisation of the directory entries, whereas the ECOWAS has included in the text of their CBM 2 regarding a regional PoC directory that preference should be given to nominating PoCs that are listed in both the ECOWAS and the UN PoC directories. This could possibly reduce the required resources for keeping it updated (e.g. via comms checks), as duplications or parallel running mechanisms can be avoided – thus enabling the fulfilment of requests by smaller or less-well-resourced states that only have limited personnel capacity.[146]

While these recommendations address different dimensions of implementation, they should not be understood as separate or independent measures. Effective CBM implementation requires a broad and mutually reinforcing strategy with regard to both the practical capacities and the political conditions that enable sustained engagement.

Acknowledgement

This analysis has been supported by the cyber diplomacy working group “Multilateral Cyber Confidence-Building Measures” and through additional interviews with (cyber) diplomats, researchers and practitioners, including with representatives from member

143 This has for example also been suggested by Singapore at the 2026 July Meeting of the Global Mechanism (see here).

144 As suggested for example by Argentina at the 2026 July Meeting of the Global Mechanism in 2026 (see here).

145 This has for example been underlined by Nigeria on behalf of the African Group at the July Meeting of the Global Mechanism (see here) as well as by the 2025 non-paper on “Inter-regional Cooperation. The Role of Regional Organizations in Implementing the UN Framework for Responsible State Behaviour in Cyberspace.”

146 This was for example underlined in Vanuatu's statement at the 2026 July Meeting of the Global Mechanism: “Vanuatu participates in this expanding architecture and we support the directory wholeheartedly, but we speak from the standpoint of the administrations that must operate all of these channels at once, often through the same handful of officials. Our request to this mechanism is that the directory be developed in deliberate awareness of the wider ecosystem, clear guidance on which channels serve which purpose, consistency in points of contact, where national structures allow it, and no duplication of what already functions elsewhere.” as well as by the AU’s statement and the OSCE’s statement.

states from the analyzed organizations, industry, military, academia, and civil society.

The views and opinions expressed in this paper are those of the authors and do not reflect the official policy or position of the experts or that of their respective employer/s.

In alphabetical order, acknowledging essential contributions of the members of the working group:

1. Anastasiya Kazakova, DiploFoundation
2. Catalina Vera Toro, Permanent Mission of Chile to the OAS
3. Eugene Tan, S. Rajaratnam School of International Studies (RSIS)
4. Fabian Hetz, Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GiZ)
5. Folake Olagunju, Economic Community of West African States (ECOWAS)
6. Heli Tiirmaa-Klaar, IT Coalition
7. John Schabedoth, German Federal Foreign Office
8. Jörn-Arne Niemann, Permanent Mission of the Federal Republic of Germany to the OSCE
9. Jürgen Altmann, Technische Universität Dortmund
10. Karsten Geier, German Embassy in Luxembourg / Centre for humanitarian Dialogue
11. Mariana Jaramillo, Organization of American States (OAS)
12. Moliehi Makumane, United Nations Institute for Disarmament Research (UNIDIR)
13. Neno Malisevic, Microsoft
14. Pablo Andrés Castro Hermosilla, Ministry of Foreign Affairs Chile
15. Pavlina Pavlova, Critical Cyber
16. Serge Droz, Swiss Federal Department of Foreign Affairs
17. Sophia Klumpp, German Federal Foreign Office
18. Thomas Reinhold, Peace Research Institute Frankfurt (PRIF)

The author would like to thank the involved subject matter experts for their insights and for sharing their experience.

This project was funded by the German Foundation for Peace Research (DSF).



Author

Helene Pleil
Senior Policy Researcher Cybersecurity & Emerging Threats
hpleil@interface-eu.org

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
c/o Publix
Hermannstraße 90
D-12051 Berlin

This paper is published under CreativeCommons License (CC BY-SA). This allows for copying, publishing, citing and translating the contents of the paper, as long as interface is named and all resulting publications are also published under the license “CC BY-SA”. Please refer to http://creativecommons.org/licenses/by-sa/4.0/ for further information on the license and its terms and conditions.

Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com