SWP Comment
NO. 39 SEPTEMBER 2026

Multilateral Cooperation and Confidence-Building in Cyberspace

The OSCE as a Laboratory for Cooperative Cybersecurity

Nadja Douglas, Jonas Hemmelskamp and Simon Muschick

The number of cyber incidents involving state actors and state-controlled actors is rising worldwide – particularly in the OSCE region – yet the diplomatic instruments designed to contain such incidents receive comparatively little attention. The OSCE (Organisation for Security and Co-operation in Europe) and other regional organisations have adopted a range of confidence-building measures (CBMs) in the cyber domain that provide a basis for deeper multilateral cooperation. It remains unclear, however, to what extent these measures respond to the demands of a changing threat landscape. Cyber diplomacy also continues to face structural shortcomings, while perceptions of threats differ across regions. More fundamentally, the question arises as to the circumstances under which states cooperate in response to cyber incidents and when national sovereignty interests take precedence.

Since 2014, Russia's war of aggression against Ukraine has shaped the security environment in the OSCE region. Numerous cyberattacks since the beginning of Russia's full-scale invasion in 2022 — including those against the satellite communications provider Viasat at the outset of the war, the mobile network operator Kyivstar and, more recently, Poland's energy sector — have demonstrated that the conflict has long since extended into cyberspace.

An analysis of cyberattacks in the OSCE region conducted by state actors, state-linked actors or ostensibly activist groups in 2022 shows that, according to data from the European Repository of Cyber Incidents (EuRepoC) project, 67 per cent of incidents can be linked to the war (see Figure 1). More than 60 per cent of publicly known incidents in the OSCE region involve six countries: Ukraine, the United States, Russia, Germany, the United Kingdom and France. Ukraine and its supporters remain frequent targets of Russian attacks, while Russia is regularly targeted by pro-Ukrainian groups. Since the start of the war, the objectives of cyberattacks across the region have shifted. Before 2022, attacks by these actors were primarily aimed at espionage (44.6 per cent). Since then, operational patterns have become more varied, with disruptive (32.4 per cent) and destructive attacks (10.3 per cent) now more prominent, although the severity of incidents remains relatively low.

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Figure 1

Politically motivated cyber incidents in the OSCE region linked to the Russia-Ukraine war

Number of incidents per year

Source: EuRepoC

Indeed, in certain circumstances cyberspace appears to function as a substitute for conventional kinetic attacks. Thus, signalling strategies can help to slow down rather than accelerate escalation dynamics (off-ramp thesis). Typical targets include critical infrastructure, communications networks and electoral systems.

In addition to the impacts of the war, accelerating digital transformation, the growing importance of artificial intelligence, the crisis of multilateral security arrangements, and increasing regional fragmentation pose major cybersecurity challenges for OSCE participating States.

This SWP Comment examines how the establishment of technical communication channels, combined with capacity-building efforts, can help strengthen international cooperation in cyberspace. The analysis is based on interviews with representatives from academia, selected OSCE participating States in Vienna, the OSCE Secretariat and other regional organisations. It also draws on data from the EuRepoC project.

Cooperation and governance in cyberspace

The growing number of attacks on critical information infrastructure demonstrates that digital networks have become arenas of conflict. Accordingly, cyberspace is also gaining importance in military and security policy. While some experts are critical of the securitisation of cyberspace by state actors, others see it as a legitimate arena for power politics and deterrence. Because cyberattacks are difficult to trace conclusively, attribution — meaning the political or technical identification of the actor responsible for an incident — is subject to considerable uncertainty. The complexity of the attribution process poses significant challenges, particularly for states with less developed cyber capabilities. Various proposals for establishing multilateral attribution mechanisms have therefore been put forward. States nevertheless continue to regard attribution as a national prerogative.

Traditional security governance instruments are inadequate due to the cross-border nature of cyberattacks and the blurred boundaries between civilian and military activities in cyberspace. A transnational approach is therefore required. Cyber governance can be understood as a multi-level model in which global, regional and national processes interact. Efforts to foster cooperation and governance in cyberspace stem from a desire to recognise cybersecurity risks as a threat to international security and to develop responses at the multilateral level. Since 2004, the United Nations (UN) has periodically convened Groups of Governmental Experts (GGEs) to discuss issues of international security relating to information and communication technologies (ICTs) and develop norms of responsible state behaviour. Besides the GGEs, which include only a limited number of experts, an Open-ended Working Group was established as another negotiating format in 2018. In 2026, the process became permanent with the launch of the Global Mechanism. A shared institutional framework for responsible state behaviour has thus emerged at the UN level, although its practical implementation remains politically contested.

CBMs are an instrument of multilateral cyber diplomacy aimed at maintaining stability in cyberspace. They are intended to reduce the risk of misperceptions, unintended incidents and tensions in cyberspace. Unlike conventional weapons systems, states' cyber capabilities are difficult to quantify and verify: They are largely intangible, depend on information and frequently rely on dual-use technologies. Although transparency generally has a stabilising effect in conventional CBMs, in the cyber domain it may expose vulnerabilities and potential targets. Cyber CBMs therefore place greater emphasis on communication, cooperation and crisis management amid technical uncertainty. Their implementation requires coordination among government bodies at both the political and technical levels.

Cyber diplomacy, however, receives comparatively little attention from governments and the private sector. The broader political climate and prevailing discourse on cybersecurity are shaped largely by questions regarding political attribution for cyberattacks and the concept of active cyber defence. It is therefore all the more noteworthy that cybersecurity discussions within the OSCE remain one of the few areas in which states continue to engage with Russia and discuss CBMs.

Regional implementation of norms and CBMs

Regional organisations play a particularly important role in translating globally agreed norms and CBMs into concrete practices and implementation. Conversely, regional experience and best practices should inform the UN process at the global level. Efforts are currently under way to identify ways of institutionalising interregional exchange, particularly with regard to CBMs. Alongside the UN, various regional organisations — including the OSCE, the Organization of American States (OAS), the ASEAN Regional Forum (ARF) and African regional organisations — are developing and implementing rules, cooperation mechanisms and CBMs in cyberspace.

In this context, the OSCE was the first multilateral organisation to begin adopting and implementing practical cyber CBMs in 2013, following recommendations by the UN GGE. The aim of the first package, comprising 11 voluntary, politically non-binding measures, was to build trust and transparency. These included consultation mechanisms intended to reduce the risk of misperception and escalation in connection with cyber incidents (CBM 3), as well as the establishment of a network of national points of contact (PoCs) to facilitate direct communication between participating States (CBM 8). An additional five measures were added in 2016. Originally, the process was to be completed by a third package dealing with stability measures, according to which

participating States would have refrained from destabilising activities such as attacks on civilian and critical infrastructure. However, there was subsequently no longer any political will to expand the measures further. At the UN level, meanwhile, a framework of eight voluntary CBMs was developed between 2022 and 2024 to complement the norms of responsible state behaviour. These measures are intended, in particular, to promote transparency, interstate communication and cooperation, and to reduce the risk of escalation.

The OAS also developed cyber-specific CBMs to complement its existing conventional CBMs. Its agenda, however, places greater emphasis on capacity-building, particularly support for states with limited cyber capabilities. The establishment of national Computer Security Incident Response Teams (CSIRTs) and the development of networks linking them also play an important role. Compared with the OSCE, the OAS has so far been less constrained by geopolitical deadlock. The Association of Southeast Asian Nations (ASEAN) and its Regional Forum (ARF), likewise combine CBMs with the region's tradition of preventive diplomacy. The emphasis lies on dialogue, capacity-building and technical cooperation, with particular importance attached to building a CSIRTs network. Cooperation among technical incident-response teams in Southeast Asia illustrates how trust can initially be built at the functional and technical levels. On the African continent, the Economic Community of West African States (ECOWAS), for example, promotes regional cybersecurity by supporting the development of regional cyber CBMs. One continuing challenge in the region is to avoid treating cybersecurity solely as a technical or security-policy issue and instead to approach it as a state responsibility that must be conceived in conjunction with socio-economic development and efforts to strengthen societal resilience.

The OSCE as a forum for cyber diplomacy

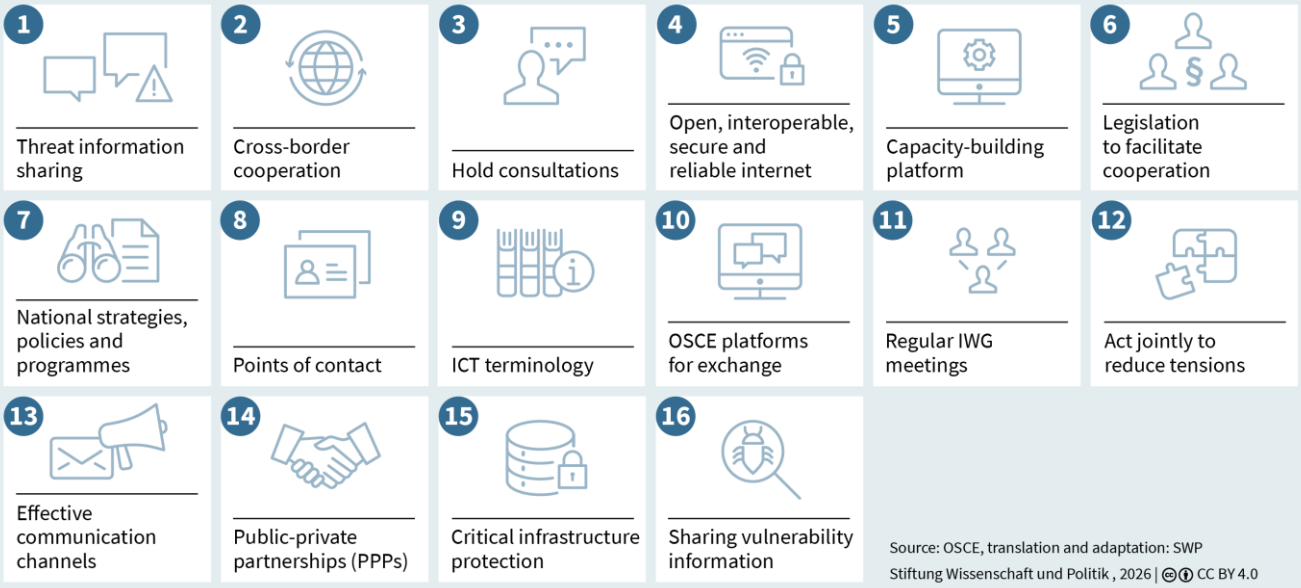
The divergent threat perceptions and resulting polarisation within the OSCE differ markedly from those in other regional contexts. The erosion of geopolitical trust has significantly constrained the organisation's ability to act on core security policy issues, particularly since 2022. Nevertheless, the OSCE has an Informal Working Group (IWG) on cybersecurity and the security of ICTs, established in 2012 under Permanent Council Decision No. 1039, whose purpose is to promote transparency, predictability and stability in addressing ICT-related risks. The agenda and discussions of this primarily technical body are less politicised than those of other OSCE bodies. Participating States regard the IWG, which meets in Vienna two or three times a year, as a kind of "hygiene ritual": It may not generate headlines, but it is considered useful. Participating States use the forum to exchange information on progress in implementing the CBMs and on their current national cyber strategies, doctrines and legislation. According to interviewees, contributions are generally substantive, and participation by delegations remains assured, not least because remote participation is possible. Much of what takes place in the IWG is declaratory in nature, but the exchanges contribute to greater transparency and predictability. As in the UN context, however, difficulties persist in defining key terms, and states are reluctant to accept legally binding commitments. Nonetheless, the group has established a common language and norms whose preservation is valuable in itself.

Some interviewees criticise the lack of clarity about the OSCE's cyber mandate beyond confidence-building. Others also view the complete exclusion of arms-control issues as a shortcoming.

The effectiveness of the 16 CBMs (see Figure 2) depends to a considerable extent on whether participating States not only implement them but also put them into practice. Under the "Adopt-a-CBM" initiative,

Figure 2

OSCE CYBER/ICT Security CBMs



Source: OSCE, translation and adaptation: SWP

individual participating States support the implementation of specific measures, facilitate knowledge exchange and develop concrete implementation formats.

A key point of departure is CBM 10, which envisages the use of existing OSCE platforms, particularly the secure OSCE Communications Network (CommsNet). According to interviewees, participating States differ considerably in their use and acceptance of these mechanisms.

National capacities also vary: Some states still lack the institutional and technical capabilities — and, in some cases, awareness of the relevance of CBMs — required to participate effectively in their practical implementation.

Capacity-building therefore serves a dual purpose: It is a CBM in its own right (CBM 5), while also enabling states to implement other CBMs in the first place. The OSCE's increasing focus on capacity-building can also be interpreted as a response to the constraints on political action in traditional interstate confidence-building.

At the national level, strengthening resilience is also becoming increasingly important, particularly in the protection of critical infrastructure (CBM 15). Since much of this infrastructure is privately owned or operated, cooperation with the private sector is essential (CBM 14 on public—private partnerships).

Both measures call upon states to establish mechanisms for information exchange among public authorities, businesses and civil society. Private companies and civil society actors should therefore be made aware of the CBMs and involved in their implementation.

This approach remains contested between predominantly Western states and countries such as Russia and China. While some states advocate restrictive accreditation and participation procedures, Western states in particular favour broad and inclusive participation by the private sector, academia and civil society. Against this background, the regulatory and technical dimension of cyber governance is becoming increasingly important.

Technical and political cooperation

The OSCE's informal working methods offer potential for significantly improving coop-

eration in cyberspace. An analysis of state responses to cyber incidents can help identify areas in which cooperation within the OSCE and other regional organisations remains possible despite heightened geopolitical tensions. The key question is which forms of cooperation can remain viable even when political trust is low.

The EuRepoC project examined 412 responses by NATO Allies to cyberattacks between 2021 and 2025 (calculations based on the as yet unpublished EuRepoC response dataset). The data indicate that cooperation remains limited, even among allies. At the same time, they suggest that establishing cooperation mechanisms at the technical level is particularly promising, as it avoids the politically contentious issue of collectively attributing responsibility. Overall, responses within the Alliance are strongly shaped by the security discourse. Security advisories account for 45 per cent of all recorded responses. In these advisories, public authorities, for example, draw attention to vulnerabilities, their exploitation or campaigns by specific actors. Other responses include formal attributions of responsibility and operational measures. Despite the increasingly critical cybersecurity environment, states respond to only a small proportion of recorded cyber incidents (17 per cent). Most responses (69 per cent), whatever their form, remain communicative in nature and have no immediate operational consequences.

The difference between the technical and political levels is particularly striking. In contrast to political attribution, technical attribution often identifies the hacker group responsible rather than the state behind it — and sometimes identifies only the group. Political attribution is thus replaced by a purely technical alert that primarily provides defenders with information about the attack vector, while also signalling to the attacker that its activities have been "detected". In this sense, governments can also outsource attribution to IT security companies to preserve diplomatic room for manoeuvre and better manage escalation dynamics. The two levels of attribution also differ in the extent of international cooperation: Closer collaboration is often possible at the technical level. Overall, 21.6 per cent of recorded responses have a multilateral component. Coordinated responses are particularly common: Several states participate and refer to one another, but each issues its own statement. Somewhat less common are joint responses, in which several states act collectively and issue a common statement.

At the political level, coordinated responses are relatively frequent, accounting for 28.3 per cent of political responses. In these cases, states generally respond independently but coordinate their responses and refer to one another. By contrast, closer coordination in the form of joint responses occurs much more frequently at the technical level, accounting for 41.2 per cent of technical responses. Such shared responses are often issued as "joint advisories" by operational cybersecurity agencies. Technical channels thereby depoliticise questions of blame and responsibility and create scope for different forms of action. Joint political statements, on the other hand, tend to be coordinated and issued through international bodies such as NATO's North Atlantic Council, the EU's High Representative or the Council of the EU, respectively, or adopted by foreign ministers at international conferences.

The fact that even allied states cooperate more closely only at the technical level suggests what (limited) options for cooperation may be possible in other regional contexts. Technical forms of cooperation that do not require joint political attribution could, in particular, preserve a certain degree of room for manoeuvre. This points to ways in which the OSCE could maintain cooperation in the cyber domain in a persistently low-trust environment.

Cyber incident classification within the OSCE resembles a patchwork: There are no common thresholds for determining when an incident warrants consultation. At the same time, states prefer existing EU and NATO formats when coordinating responses and attributions with like-minded partners. Ultimately, each state decides for itself what

constitutes a "serious" incident. As a result, the incident reports and quarterly figures presented in the IWG vary considerably. According to observers, the underlying pattern of reportable cyber incidents is often similar; it is the classification systems that differ.

Structural shortcomings and opportunities

Cyber diplomacy and cooperation currently face a tension between the need to maintain technical dialogue as a means of risk reduction and the stagnation caused by geopolitical divisions.

In the current security environment, CBMs tend to preserve existing channels rather than transform relations. Some states increasingly use these forums for political and, occasionally, military signalling; for others, capacity-building is far more important.

Although cyber CBMs are not designed to prevent deliberate attacks, even as the number of incidents rises, they remain important for keeping states in communication and making unintended escalation less likely. Yet states' willingness to cooperate — and, with it, the effectiveness of CBMs — reaches its limits when national security interests, sovereignty or offensive capabilities are at stake. This applies in particular to the classification of incidents, the coordination of responses, and political and technical attribution: Even among allies, cooperation in these areas is limited.

At present, it is difficult to imagine the OSCE or other overarching bodies assisting with the classification or attribution of incidents. The OSCE has neither the mandate nor the capacity to investigate or classify cyber incidents. Consideration should therefore be given to ways of bringing national classification methodologies into closer alignment, for example through subregional groupings or coalitions of the willing. The discussion of stability measures should also be resumed. This could include addressing the consequences of unacceptable or destabilising effects and conduct, including by raising concerns about cyberattacks on certain civilian and critical infrastructure. This would build on Norm 13(f) of the UN GGE Report on Strengthening Responsible State Behaviour in Cyberspace.

In contexts ranging from "low trust" to "no trust", reducing and managing risk at the technical level offers better prospects today than building political trust. Officials from participating States have greater scope to act and can provide a protected space for continued dialogue. This is partly because they offer a higher degree of informality and corresponding communication channels, while politically sensitive questions of attribution can more easily be set aside. This finding should not, however, encourage further separation of silo structures at the technical and political levels. In many states, cybersecurity is still regarded as a purely IT matter. In the event of serious incidents, however, ultimate responsibility rests at the political and diplomatic level. The analysis of state responses based on the EuRepoC response dataset shows that multilateral cooperation is more prevalent when states issue technical alerts than when they make political attributions of responsibility for cyberattacks.

Participating States are also more willing to involve the private sector when an incident involves, for example, cybercrime rather than a politically motivated cyberattack.

Outlook

The governments of OSCE participating States would be well advised to pursue a two-pronged approach: They should continue to invest in and implement CBMs while also strengthening their national cyber resilience. Capacity-building can bridge these two objectives, allowing confidence-building to continue through accessible, practical measures while strengthening national structures and incident-response capabilities across the region. For the time being, cyber CBMs

remain an important alternative, particularly while arms-control measures in the cyber domain remain unfeasible. A ceasefire between Russia and Ukraine, however, should not be expected to bring about a peaceful cyberspace.

Despite all structural shortcomings, attention should remain focused on the opportunities offered by multilateral cooperation and diplomacy in cyberspace.

The online version of this publication contains functioning links to other SWP texts and other relevant sources.

SWP Comments are subject to internal peer review, fact-checking and copy-editing. For further information on our quality control procedures, please visit the SWP website: https://www.swp-berlin.org/en/about-swp/quality-management-for-swp-publications/

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1861-1761
ISSN (Online) 2747-5107
DOI: 10.18449/2026C39

(English version of SWP-Aktuell 43/2026)

Dr Nadja Douglas is a researcher in the Eastern Europe and Eurasia Research Division at SWP. Jonas Hemmelskamp is a data scientist with the European Repository of Cyber Incidents (EuRepoC) project at Heidelberg University. Simon Muschick is an information and data manager at SWP.

This paper is based on findings from a project funded by the German Federal Foreign Office on the role of the OSCE in a new European security order. The authors would like to thank Mia Geiger for her editorial support and assistance in compiling the figures, as well as Dr Alexandra Paulus for her helpful comments on the initial draft.