CESS Centre for European Security Studies

CESS Volten Brief, No. 12, June 2025

Image: AI generated by authors

VOLTEN BRIEF

Cybersecurity in Bosnia and Herzegovina: Everyone's problem – no one's responsibility

This series of policy briefs is named after CESS founder Peter Volten

Cybersecurity in Bosnia and Herzegovina: Everyone's problem – no one's responsibility

In 2022, Bosnia and Herzegovina (BiH) was the target of a major cyberattack. The Parliamentary Assembly was paralysed, and the confidentiality of sensitive information was compromised. What should have served as a wake-up call, exposing the state's vulnerability to escalating cyber threats, failed to trigger a coordinated institutional response. When hackers managed to shut down the servers of the Parliamentary Assembly, its website remained offline for a week – severely limiting public access to information and forcing officials to reschedule parliamentary proceedings. Despite the scale of the disruption, the response from state institutions was minimal. The State Investigation and Protection Agency (SIPA) launched an inquiry, but its findings were not made public. This incident was not isolated; rather, it underscored a persistent and unaddressed vulnerability. Cyberattacks on BiH are growing in frequency and sophistication, yet the country remains ill-prepared to respond, leaving citizens, companies, and even state institutions exposed to the dangers of the digital world.

Key points:

1. Bosnia and Herzegovina lacks a national cybersecurity strategy and a national Computer Emergency Response Team (CERT), rendering its institutions, critical infrastructure, and citizens vulnerable to increasingly sophisticated cyberattacks.
2. Political fragmentation, lack of will, and everyday political issues have stalled progress, despite substantial international support.
3. The development of a robust legal framework, investment in the cybersecurity capacity of institutions, and structured cooperation with international, private, and non-governmental sectors represent the necessary next steps towards strengthening BiH's cybersecurity.

By Armin Tufo (ed.), Tea Iličić, and Ajna Mešić

Armin Tufo *is a student enrolled in the European Regional Master's Programme in Democracy and Human Rights in South-East Europe, jointly offered by the University of Sarajevo and the University of Bologna.*

Tea Iličić *is a student of International Relations and Diplomacy, currently working at CIVITAS, a local educational centre dedicated to democracy and human rights.*

Ajna Mešić *is a student of Political Science and International Relations at the International University of Sarajevo, working at the Youth Initiative for Human Rights.*

The authors are part of the BIHOS 2025 Young Professionals Trajectory

Globally, with over half of the population connected to the internet, cybersecurity has become the primary concern for governments. A digital environment festering with threats, combined with its increasing relevance in providing access to services and information, is forcing governments to support the transition toward digitalisation. This, in turn, exposes government institutions, private entities, and citizens to malevolent cyberattacks. Despite this context, BiH lacks a coherent and centralised cybersecurity strategy. Notably absent is a national CERT, or a broader Computer Security Incident Response Team (CSIRT).

This policy brief presents findings from research undertaken by the authors on the potential establishment of a CERT in BiH. It explores why BiH currently lacks such a structure, how it addresses cyber threats under the existing framework, and what institutional and legislative measures are necessary for moving forward. The brief concludes by highlighting the importance of a national CERT and outlining key challenges and actionable recommendations. The authors propose the following:

First, adopt a robust and comprehensive national cybersecurity law that harmonises existing legislation and aligns with the European Union's (EU) NIS2 Directive, including provisions for the establishment of a national CERT.
Second, invest in human and financial resources to strengthen cybersecurity, including training programmes, updated IT infrastructure, and competitive remuneration for specialised personnel.
Third, facilitate and incentivise public-private partnerships, including with technology companies and media outlets, through measures such as tax incentives and structured cooperation frameworks.
Fourth, strengthen international collaboration with the EU, the Organisation for Security and Cooperation in Europe (OSCE), and regional CERTs, particularly through legal harmonisation, staff exchanges, and capacity building programmes.[1]

1. The brief is part of the 'Bosnia and Herzegovina Building Inclusive Oversight of Security' (BIHOS) project that includes a Young Professional Trajectory. An earlier draft of the brief was reviewed by Jos Boonstra and Erik Sportel from CESS.

What is a CERT?

A Computer Emergency Response Team is a group of experts responsible for monitoring, preventing, and responding to cyber threats. CERTs play a vital role in safeguarding government institutions, businesses, and citizens by rapidly identifying and mitigating threats. In many cases, they act proactively to prevent incidents altogether. Most countries in Europe have long established CERTs – whether government-run, private, or structured as public-private partnerships – that operate under the oversight of national regulatory agencies or relevant ministries. While the nomenclature may vary – CERT, CSIRT, among others – their core function remains the same: to provide coordinated, swift responses to cybersecurity incidents, including further (legal) investigations.

Although CERTs may occasionally be formed on an *ad hoc* basis to address pressing issues, formalised teams deliver more consistent and effective responses, drawing on institutional experience and specialised knowledge in a specific cyber environment.[2] Under the EU's NIS2 Directive (the EU's cybersecurity law), both member states and candidate countries must set up a CERT or CSIRT. Without such a body in place – not only to respond to attacks but also to raise awareness, issue guidance, and analyse threat landscapes – there is no effective national mechanism to manage cybersecurity risks. In this situation, institutions such as hospitals, universities, schools, and energy companies are left to defend themselves against attacks that can compromise private data or disrupt essential services.

The Bosnia and Herzegovina cyber landscape

Cyber threats are not hypothetical – they occur regularly and have real consequences, from undermining trust in democratic processes to causing economic disruptions. Establishing an initiative-taking cybersecurity posture has the potential to drive wider digital transformation and foster innovation. However, BiH's fragmented institutional structure – lacking a central authority for cybersecurity – poses coordination challenges. The country's administrative complexity, divided across state, entity, and cantonal levels, each with separate ministries, results in duplication of effort and inconsistency in response. Moreover, the constitutional requirement for political consensus often complicates the adoption of a nationwide strategy, limiting the efforts of various ministries to find common ground. Compounding these institutional limitations are widespread public unawareness of cyber risks and a shortage of trained professionals within government structures. Although cyberattacks on private companies and media outlets have created incentives for capacity building and cross-sector partnerships, in the absence of a unified national strategy, such initiatives remain fragmented and reactive rather than preventive.

Bosnia and Herzegovina's highly decentralised institutional and convoluted framework has hindered the adoption of a coherent cybersecurity strategy. The Minister of Communications and Transport, Edin Forto, has pointed out the perceived lack of consensus among institutional actors on establishing a national CERT.[3] Indeed, the various tiers of government operate largely independently, with minimal coordination on cybersecurity – characterising BiH as one of the most intricate political systems in Europe.

2. Cyber Emergency Response Team (CERT), 'Concept, Role and Responsibilities', iNetwork, 2019. Retrieved from https://istanduk.org/wp-content/uploads/2019/08/Cyber-Emergency-Response-BRT-002.pdf (accessed on 6 June 2025).
3. Enes Hodžić, 'Dok BiH stidljivo korača u cyber sigurnost, čekaju se političke odluke', Detektor.ba, 29 September 2023. Retrieved from https://detektor.ba/2023/09/29/dok-bih-stidljivo-koraca-u-cyber-sigurnost-cekaju-se-politicke-odluke/ (accessed on 6 June 2025).

Meanwhile, the politicisation of ethno-national divisions continues to obstruct decision-making at the state level, leaving citizens, businesses, social services, educational institutions, and hospitals increasingly vulnerable to sophisticated cyberattacks. At its core, the absence of a coordinated national response to cyber threats is a political issue. The complexity of BiH's political landscape has kept the matter off the agenda of key decision-makers, resulting in a fragmented and insufficient legal framework, dispersed across varying levels of government with no clear way forward.

This lack of institutional cooperation and political will has resulted in feeble efforts, exposing the internal vulnerability of BiH's domestic politics. In the absence of a unified platform for real-time information sharing and a joint incident response mechanism, gaps in cyber defence persist. These challenges place increasing pressure on national decision-making bodies, which remain largely unresponsive. Moreover, without a critically-informed public capable of exerting pressure on policymakers, complacency persists – contributing to systemic vulnerabilities and a widespread lack of grassroots awareness.

From January to August 2023, the local organisation Cyber Security Excellence Centre (CSEC) recorded over 15 million cyber threats aimed at various BiH actors.[4] In the preceding year, over 9 million attempts were made to compromise sensitive data held by companies and institutions, some of which managed to shut down mainstream media portals. CSEC's 2023 report – the first of its kind in BiH – highlighted the vulnerability of national actors operating without adequate state protection. The most frequently recorded incidents were Distributed Denial of Service (DDoS) attacks targeting Information and Communications Technology (ICT) systems. Additionally, approximately 1.7 million Private Branch Exchange (PBX) attacks were registered, targeting telephone networks. A report by the Centre for Security Studies (CSS) linked such hybrid attacks to Russian intelligence actors, showcasing the high level of sophistication of techniques employed. Other incidents in 2022 included false bomb threats and interference with the Central Election Commission, both believed to be part of a broader wave of cyberattacks stemming from the Russia-Ukraine war.[5]

A particularly concerning incident involved the misuse of official BiH institutional e-mail addresses in phishing campaigns. As a result, sensitive personal data – including passwords and credit card information – was compromised. In the absence of a national CERT, BiH relies on outside support to address these issues. In this case, Spanish authorities notified Serbian CERT teams, who then relayed the warning. In 2022, a serious breach occurred when members of the Parliamentary Assembly were prohibited from using their computers following a cyberattack. According to media reports, both the nature of the attack and the findings of the subsequent investigation remain unclear, as the Ministry of Security lacks the capacity to conduct investigations.[6]

4. Aida Mahmutović, Enes Hodžić, Cyber prijetnje u BiH, April 2023. Retrieved from https://detektor.ba/wp-content/uploads/2023/04/Cyber-prijetnje-u-BiH-ENG-WEB.pdf (accessed on 6 June 2025).
5. Denis Hadžović, Aida Kržalić, Benjamin Plevljak, 'Perspectives on Cybersecurity in BiH', Centre for Security Studies, April 2025. Retrieved from https://css.ba/wp-content/uploads/2025/04/Centre-for-Security-Studies-Perspectives-on-Cybersecurity-in-BiH.pdf (accessed on 6 June 2025).
6. A. Dučić, 'Nevjerovatno: Tužilaštvo BiH od septembra istražuje kibernetički napad na institucije', Fokus.ba, 2 June 2025. Retrieved from https://www.fokus.ba/vijesti/bih/nevjerovatno-tuzilastvo-bih-od-septembra-istrazuje-kiberneticki-napad-na-institucije/2535304/ (accessed on 6 June 2025).

The private sector has also faced persistent targeting. Media outlets have been subject to frequent cyberattacks, undermining their economic stability while inhibiting citizens' access to breaking news and information. These developments underscore the urgent need for a central, authoritative body equipped to provide coordinated and timely responses.

Institutional responsibility

While Bosnia and Herzegovina does not have a state-level CERT, the country's two entities have pursued differing strategies with varying degrees of success. In 2011, Republika Srpska (RS) adopted the Law on Information Security and subsequently established the Agency for Information Society (AIS RS), which monitors ICT development and offers digital training for civil servants. In 2015, RS launched its own Computer Emergency Response Team (CERT RS), tasked with preventing and responding to cyber incidents within its jurisdiction. However, as of the time of writing, the operational activity of CERT RS remains marginal.

The Federation of Bosnia and Herzegovina (FBiH) has only more recently initiated steps towards developing its cybersecurity framework. In late 2022, FBiH drafted a Law on Internet Security, reaffirmed in its 2025 Action Plan. It also drafted its first Law on Information Security, marking an important step toward formalising its cybersecurity framework. However, responsibility for digital policy within FBiH is distributed across several institutions – including the Ministry of Transport and Communications, the Ministry of Education and Science, and the ministries of the ten cantonal units. Additionally, the state-level Communications Regulatory Agency holds oversight and monitoring responsibilities. This administrative complexity has slowed down the development of a coherent cybersecurity policy. Nevertheless, the FBiH government has acknowledged the need for a more centralised approach and has expressed interest in developing its own CERT, currently in the planning stages with international support.

In parallel with these entity-level advances, BiH has taken initial steps towards developing its cybersecurity framework. The country ratified the 2001 Budapest Convention on Cybercrime – a foundational instrument in international cybercrime legislation and cooperation. Ratified in 2006, the Council of Europe Convention standardised the criminalisation of online offences and procedural mechanisms, which led to amendments to the BiH Criminal Code in 2009. In 2008, BiH also signed the EU Stabilisation and Association Agreement, committing to the implementation of both the Cybercrime Convention and the EU's General Data Protection Regulation (GDPR). As EU membership remains a key foreign policy objective, BiH is obligated to adopt more rigorous legal standards and to facilitate international cooperation on cybersecurity and data protection.

In 2023, the Council of Ministers of Bosnia and Herzegovina (CoM) adopted a series of decisions aimed at strengthening digital security. These included measures related to access control and information protection, cybersecurity in the workplace, the use of mobile devices within BiH institutions, and amendments to the internal structure of the Ministry of Security.[7] The CoM also granted approval for the operationalisation of a CERT for BiH institutions; however, this has yet to be implemented.

7. Istinomjer.ba, 'Kibernetička sigurnost', Istinomjer.ba, n.d. Retrieved from https://istinomjer.ba/predizborna-obecanja/kiberneticka-sigurnost/ (accessed on 6 June 2025).

The development and harmonisation of BiH's cybersecurity policies with relevant EU directives and regulations – most notably the NIS2 Directive – should become a central policy priority. Following the 2022 cyberattack on Parliament, the Ministry of Security took part in the ETSI Security Conference in France, supported by the iPROCEEDS-2 project. The event focused on cybersecurity standards and legislation, and by the end of the year, BiH had announced draft legislation on information security and electronic signatures – important steps toward aligning with EU standards. Nevertheless, the future of these proposals remains uncertain. Progress has stalled, despite the availability of international funding and technical support. International partners have consistently voiced concern over the slow pace of reform and the lack of tangible progress in establishing a functioning national CERT.

While cybersecurity remains absent from plenary debates and official communication strategies, there have been a few notable individual efforts. In 2023, Saša Magazinović, a member of the Parliamentary Assembly of Bosnia and Herzegovina representing the Social Democratic Party (SDP), submitted a formal inquiry to the Minister of Security regarding the readiness to establish a state-level CERT and the measures being taken to respond to cybersecurity threats.[8] Similarly, Jasmin Evrić, also a member of the Parliamentary Assembly, has publicly addressed the importance of creating a national CERT through participation in cybersecurity conferences, remarking that 'daily politics' often distract politicians from this issue.[9]

While these examples demonstrate that individual MPs recognise the importance of the issue, such initiatives remain exceptions rather than the rule. As previously noted, the Minister of Communications and Transport has also advocated for the swift adoption of cybersecurity legislation, citing persistent political disagreements as the primary reason Bosnia and Herzegovina remains, in his words, standing in a 'windswept' place.[10]

Towards a CERT

A *laissez-faire* approach to cybersecurity in BiH would entail continued reliance on non-governmental and external actors – such as the Cyber Security Excellence Centre, non-governmental organisations (NGOs) like the Centre for Security Studies, and media organisations such as the Balkan Investigative Reporting Network (BIRN). While there are some advantages to this model, it comes with significant limitations. With support from the OSCE and, subsequently, the United Kingdom, CSEC was able to produce some of the first investigative reports on cyber incidents in BiH and facilitate capacity building and cross-sectoral cooperation with leading IT companies. NGOs and the media benefit from greater flexibility and institutional independence, allowing them to fulfil their oversight and watchdog roles without being hindered by bureaucratic procedures or political deadlock.

8. 'Parlament Bosne i Hercegovine, Prijedlog zapisnika 7. Sjednice', n.d. Retrieved from https://static.parlament.ba/doc/157499_B%20Prijedlog%20zapisnika%207.sjednice.pdf (accessed on 6 June 2025).
9. Nermina Kuloglija-Zolj, 'BiH i dalje bez državnog cyber tima i dokumenata, dok broj napada raste', Detektor.ba, 4 October 2023. Retrieved from https://detektor.ba/2023/10/04/bih-i-dalje-bez-drzavnog-cyber-tima-i-dokumenata-dok-broj-napada-raste/ (accessed on 6 June 2025).
10. Enes Hodžić, 'Dok BiH stidljivo korača u cyber sigurnost, čekaju se političke odluke', Detektor.ba, 29 September 2023. Retrieved from https://detektor.ba/2023/09/29/dok-bih-stidljivo-koraca-u-cyber-sigurnost-cekaju-se-politicke-odluke/ (accessed on 6 June 2025).

Investigative journalism and independent reports have the potential to galvanise and foster public awareness of cybersecurity threats, maintaining international networks, and promoting transparency and accountability.

However, reliance on external actors keeps BiH's cybersecurity governance dependent on foreign or international strategies and financial commitments – rather than enriching domestic ownership of cybersecurity policy. To date, the OSCE has played a key role by establishing an informal group of cybersecurity practitioners and experts, known as the Neretva Group, whose efforts have focused primarily on information-sharing and advisory support. In 2019, the OSCE also produced Guidelines for a Strategic Cybersecurity Framework in BiH, defining the establishment of a national CERT, together with a Cybersecurity Coordination Office (CSCO), a Cybercrime Unit (CCU), and a Data Protection Agency (DPA-BiH) as central pillars of long-term national cyber resilience.[11]

The Guidelines identified main goals, such as the implementation of training programmes for administrative personnel and the promotion of private sector investment in cybersecurity. However, a significant limitation of this externally-driven approach is the lack of enforcement authority and institutional accountability, which can undermine effective responses to cyber incidents. Ultimately, it is the role of state institutions and judicial authorities to address cybercrime through appropriate legal channels.

Without a mandate to act within Bosnia and Herzegovina's domestic affairs, non-governmental and international actors can only contribute through monitoring, technical assistance, and advocacy. While such contributions are valuable, the development of a sustainable and resilient cybersecurity framework requires government-led ownership and coordination. The functions of advice-sharing, dissemination of best practices, and public awareness campaigns remain essential, as they help to maintain pressure on decision-makers and foster greater civic engagement. Nevertheless, the overall impact of these efforts is contingent on the political will of BiH's governing institutions to engage meaningfully and systematically on cybersecurity policy.

BiH needs a cybersecurity strategy and a CERT. Considering these needs, and recognising the leading role of political commitment in advancing institutional reform, attention must focus on four priority areas:

1. Adoption of a robust legal framework on cybersecurity that would include a national CERT

At the time of writing, Bosnia and Herzegovina's legislative framework, at both the state and entity levels, comprises eight laws and four criminal codes that broadly address aspects of internet security. However, there is no comprehensive law on cybersecurity. The adoption of such a law is critical. It should harmonise existing domestic legislation and align with relevant EU frameworks, particularly the NIS2 Directive, which establishes uniform standards and clearly defines the responsibilities of actors involved in national cybersecurity. Such a legislative initiative should be led by the Ministry of Security and the Directorate for European Integration, with support from the Council of Ministers and members of the Parliamentary Assembly.

11. OSCE, 'Strengthening Cybersecurity in South-East Europe', 2019. Retrieved from https://www.osce.org/files/f/documents/1/a/438383.pdf (accessed on 6 June 2025).

Its adoption would not only streamline internal coordination but also serve to deepen Bosnia and Herzegovina's alignment with the EU. The legislation should establish mechanisms to facilitate inter-agency cooperation, intelligence sharing, efficient incident response, and regular reporting to the Parliamentary Assembly. Importantly, this reform does not require significant material investment; rather, it hinges on political will – which, if not generated domestically, may be built through outside pressure, foremost by the EU.

The creation of a national-level CERT and the adoption of a coherent cybersecurity strategy would represent the most effective means of clarifying institutional responsibilities, identifying critical infrastructure and systemic vulnerabilities, and facilitating structured collaboration with civil society and the private sector. The crucial value of a national cybersecurity law would be the removal of overlapping and unclear responsibilities. A national CERT would function as the central coordinating body, while entity-level CERTs should assume complementary roles, responding to localised incidents within their respective jurisdictions. To ensure inter-agency collaboration and coordination, it is essential to establish clear protocols and information-sharing mechanisms that prevent fragmentation and duplication of effort across levels of government.

2. Investment in cybersecurity capacity

Several cyber incidents have already exposed the limited institutional capacity of BiH authorities, particularly with respect to human and financial resources. It is thus imperative to increase investment in cybersecurity, including the provision of adequate compensation to attract and retain qualified personnel. This will require the reallocation and reconfiguration of both entity- and state-level budgets to ensure sufficient funding for the implementation of the Council of Ministers' decision to establish a CERT.

BiH also needs to fund training initiatives to advance cybersecurity knowledge across both the public and private sectors. The country's overall digital resilience would be improved by updating IT infrastructure and boosting funding for cybersecurity projects. These efforts may include support for specialised training, educational programmes, seminars, workshops, and staff exchanges. A notable example was the EU-funded project *Support to Fight Cybercrime in Bosnia and Herzegovina*, which facilitated the exchange of best practices and skills between Austrian and Croatian experts and key BiH institutions, including the Ministry of Security and the State Investigation and Protection Agency (SIPA).

Looking ahead, BiH ministries should also seek to integrate cybersecurity education into school curricula, with particular emphasis on areas such as artificial intelligence, data privacy, and mental health.

3. Facilitation of public-private partnerships

A sustainable cybersecurity framework is essential for modern governance. Given the shared interest of both public and private institutions, closer cooperation between these actors should be facilitated. While government institutions face resource constraints, they stand to benefit significantly from the expertise, tools, and up-to-date intelligence of high-technology companies. In turn, private sector engagement can be incentivised through targeted measures such as tax incentives and other forms of support.

There are already successful examples of collaboration between NGOs and technology firms that could be adapted for the public sector. Although less active than in its first two years, one such example is the Cyber Security Excellence Centre, established in partnership with the University of Sarajevo. Additionally, CSEC has ventured out and established partnerships with prominent technology companies, such as Logosoft – a practice that could be replicated and scaled within the public sector.

Journalists and media outlets are frequent targets of cyberattacks and have a clear incentive to collaborate with national and entity-level CERTs to ensure the timely exchange of information and improve responsiveness to threats. In an age where social and online media play a pivotal role in public discourse, the media's didactic function in raising cybersecurity awareness is unparalleled. This potential should be harnessed to inform citizens and cultivate a sense of civic responsibility, reinforcing public demand for stronger national cybersecurity measures.

4. Increase in international and regional cooperation

As witnessed through initiatives such as the OSCE Strategic Cybersecurity Framework and the Neretva expert group, cooperation with international organisations has proven beneficial to the development of cybersecurity in Bosnia and Herzegovina. These partnerships have provided critical technical and policy guidance, as well as platforms for dialogue within a domestically sparse landscape. Such international cooperation, however, cannot serve as BiH's cybersecurity regime because it needs to be established and agreed upon by BiH's politicians and institutions. Nonetheless, BiH should increase its collaboration with international and regional actors – particularly the EU Delegation – with a focus on the effective implementation and harmonisation of domestic legislation with the EU *acquis*.

In collaboration with the OSCE, BiH should continue to support informal expert and academic groups that address cybersecurity issues. Moreover, regional and international cooperation with established CERT teams is essential to enhancing the competence and operational readiness of BiH's own personnel. This can be achieved through capacity building programmes and staff exchanges. This would ensure that BiH catches up with its neighbours and secures necessary aid and procedural development. An avenue for further development is the Western Balkans Cyber Capacity Centre (WB3C), a regional platform based in Podgorica, Montenegro, which offers training, capacity building support, and policy coordination for cybersecurity stakeholders across the Western Balkans.

The future is now

The adoption of a national cybersecurity strategy and the establishment of a state-level CERT are no longer matters of technical reform alone – they constitute a critical test of political will. Future cyberattacks may not simply inconvenience public institutions; they have the potential to paralyse healthcare systems, compromise electoral integrity, and disrupt critical infrastructure. The current fragmentation of responsibilities, lack of cohesion, and resource scarcity pose serious challenges, with BiH standing to incur substantial financial damage without a cybersecurity strategy and a mandated CERT team.

As the only country in South-East Europe without a national cybersecurity strategy, BiH continues to depend on good neighbourly ties, independent experts, and non-governmental actors to address its cybersecurity needs. This, combined with a need to align its domestic legislation with that of the EU, presents decision-makers in BiH with a clear challenge to overcome and pass the test of political willingness for reform. The question is no longer whether action is needed, but whether decision-makers will rise to the occasion before the costs of inaction become irreversible. With the foundations in place – ranging from draft laws and institutional proposals to international support and expert engagement – the path toward a secure digital future is visible. Now it's time to take it.

Volten Briefs

Peter Volten established CESS in 1993. Peter was a staunch supporter of European unity and strong Transatlantic ties. He sought to contribute to peace and security in Europe by reaching out to people that had lived under authoritarian rule. A mission that remains very relevant today. Peter passed away in December 2022. This series of policy briefs is dedicated to him.

CESS

The Centre for European Security Studies (CESS) is an independent institute for research and training, based in Groningen, the Netherlands. CESS seeks to advance security, development, democracy and human rights by helping governments and civil society face their respective challenges. CESS is an international, multidisciplinary and inclusive institute. Its work is part of the European quest for stability and prosperity, both within and outside Europe. CESS encourages informed debate, empowers individuals, fosters mutual understanding on matters of governance, and promotes democratic structures and processes.

BIHOS – Bosnia and Herzegovina Building Inclusive Oversight of Security

BIHOS seeks to strengthen democratic governance and inclusive oversight of the security sector in Bosnia and Herzegovina at the state, entity, and canton levels. By investing in capacities through providing tools, skills, and techniques to oversight actors; fostering cooperation among parliaments, civil society organisations, and other oversight actors; and by promoting a culture of oversight that is critical and constructive, BIHOS contributes to better informed, more effective, and inclusive oversight of the security sector in BiH.

BIHOS is implemented through intertwined capacity-building and research components. The former includes tailor-made training courses and trajectories, as well as peer-to-peer consultations, training-of-trainers' courses, and study visits. The latter consists of a needs' assessment exercise, a sequence of expert labs, and a functional analysis, presented in a series of publications. The project is implemented by CESS from the Netherlands, in cooperation with the Centre for Security Studies (CSS) and the European Defendology Center (EDC) from BiH.

BIHOS is funded by the Ministry of Foreign Affairs of The Netherlands.

The views expressed by the authors do not necessarily reflect the opinion of CESS.
If you have any comments on this document or any other suggestions, please email us at info@cess.org
© CESS 2025. Edited by CESS. Lutkenieuwstraat 31a, 9712 AW Groningen, The Netherlands.