/PERSPECTIVE

Public-Private Partnerships

Aaron Joshua Pinto,
Alexandra Borgeaud dit Avocat,
Elena Lulcheva,
Philipp Dietrich

2021

Preventing Cyberattacks on Critical Infrastructure in the OSCE Region

FRIEDRICH EBERT STIFTUNG

FES Regionalbüro für Zusammenarbeit und Frieden in Europa

FES Regional Office for Cooperation and Peace in Europe

Executive Summary

Critical infrastructure is so deeply rooted in society that its failure or degradation would lead to utter chaos and disruption. Today, threats and attacks to critical infrastructure from cyberspace have skyrocketed, adding to the complexity of the threat landscape and the immense pressure faced by States to respond. While critical infrastructure protection is typically entrusted to national governments, the modern-day cross-border threat of cyberattacks warrants a transnational security response and, in particular, a robust engagement with the private sector, which owns and operates a range of critical infrastructure. As the world's largest regional security organization comprising 57 participating States that span North America and Eurasia, the Organization for Security and Co-operation in Europe (OSCE) is uniquely positioned to strengthen and better enable public-private partnerships to ensure the security and resilience of critical infrastructure. As a recommendation, this paper proposes a public-private partnership framework for the OSCE as a means to coordinate and enhance efforts with industry to protect participating States' critical infrastructure from cyberattacks.

Cyberspace: A New Challenge for Critical Infrastructure

In today's highly industrialized world, societies rely heavily on critical infrastructure, from highways and power grids to financial networks to healthcare or water supply. As structures and facilities of vital importance to a nation's society and economy, adversaries have always viewed national and business infrastructure networks as potential targets for hostile exploits (for instance theft of information, destructive penetration, and denial of service).[1] After all, shutdowns, failures or degradation of critical infrastructure can induce a cascade of societal repercussions and collateral damage, including sustained supply shortages and significant disruption of public safety and security, which can hamper any State or organization, leaving them hostage.

Today, the mounting digitization, connectivity, and automation powering modern critical infrastructure increase the diversity and complexity of threats emanating from cyberspace. In fact, according to the World Economic Forum, cyberattacks on critical infrastructure posed the fifth-highest economic risk in 2020. It called the potential for such attacks "the new normal" across sectors such as energy, healthcare, and transportation.[2]

Cyberattacks on critical infrastructure are now a fact of life. In 2020 and 2021 alone, compounded by the COVID-19 pandemic, the world witnessed a series of major cyberattacks affecting critical infrastructure in many countries. They include, among numerous cases, the supply chain attack emanating from malicious code that paralyzed Texas-based SolarWinds, the ransomware attack on the US' Colonial Pipeline, a cyberattack that shutdown the North American production of meat processing giant JBS, the Irish health service cyberattack, a denial-of-service attack on North Macedonia's elections, and a similar attack that crippled large parts of Belgium's internet services.[3]

The chief executive of Thales, a leading aerospace company dealing with cyber defence, stated that the number of cyberattacks in France alone had multiplied by four in 2020.[4] Such attacks can affect thousands, not just nationally, but globally, and, in some cases, exceed billions in costs and lost revenue.[5] In fact, according to Juniper Research, a technology market researcher, the cost of data breaches will rise from $3 trillion each year to $5 trillion in 2024, an average annual growth of 11%.[6]

The Case for Cooperative Partnerships in Critical Infrastructure Protection

While national governments and regional security organizations can play a vital role in strengthening cyber resilience, the reality is that a large share of internet-dependent critical infrastructure assets, systems, and entities – covering key sectors such as telecom and energy – are privately owned and operated. As a result, defending and securing critical infrastructure takes a very different shape in cyberspace. Simply put, governments cannot do it alone. It is for this reason that cooperation through flexible and collaborative constructs, namely through public-private partnerships, are so essential in limiting cyber risk through the blending of strengths and resources.

Additionally, while critical infrastructure protection is typically conceived as a priority of national jurisdiction, in today's interdependent and interconnected world, their safety and security require the concerted efforts of both public and private actors worldwide. The array of risks and the dynamic

1 "Recommendations," Federal Office for Information Security, accessed September 5, 2021, https://bit.ly/3By7rnG.

2 "Wild Wide Web," in Global Risks Report 2020, accessed September 7, 2021, https://wef.ch/2uQFqLz.

3 Lucian Constantin, "SolarWinds attack," CSO, December 15, 2020, https://bit.ly/3jTwV9i; William Turton and Kartikay Mehrotra, "Hackers Breached," Bloomberg, June 4, 2021, https://bloom.bg/3CATOWh; Hamza Shaban et al., "Cyberattack hits JBS," The Washington Post, June 1, 2021, https://wapo.st/2Zy8OFP; "Cyber-attack," BBC, May 20, 2021, https://bbc.in/3ECeAph; Bojan Stojkovski, "North Macedonia Election Commission," BalkanInsight, July 16, 2020, https://bit.ly/3GDB9LQ; Amer Owaida, "DDoS attack," WeLiveSecurity, May 5, 2021, https://bit.ly/2ZMB73F; "Brno University Hospital," Cyber Law Toolkit, March 13, 2020, https://bit.ly/3GDKWSf.

4 D. Keohane and P. Hollinger, "Pandemic," Financial Times, April 5, 2021, https://on.ft.com/3w1mwxd.

5 "Cyber-attack: US and UK blame North Korea for WannaCry," BBC, December 19, 2017, https://bbc.in/3CBnWAM; "NotPetya cyber-attack," BBC, September 20, 2017, https://bbc.in/3Czfr9A.

6 Juniper Research, "Business Losses," news release, August 19, 2019, https://bit.ly/3w1pr93.

threat landscape have already pushed transnational security imperatives to conceptualize norms on preventing cyberattacks on critical infrastructure. Consequently, today, this has triggered an internationalization of critical infrastructure protection initiatives, policy coordination and legislation at various levels and institutions, including at the G7, Organisation for Economic Co-operation and Development (OECD), and the United Nations (UN).[7]

This paper explores the role of the OSCE, as the largest regional security organization, in the fight against cyberattacks and offers concrete recommendations that help further this important work, specifically by leveraging public-private partnerships to protect critical infrastructure.

The OSCE and Cyber/ICT Security

The OSCE has aimed to promote peace in cyberspace by reducing the risk of conflicts between its participating States that may stem from the use of information and communications technology (ICT). The Organization has been lauded for its work on confidence-building measures (CBMs), in particular having been a regional security organization that adopted the first-ever set of "Cyber/ICT Security CBMs." The OSCE participating States adopted two sets of pioneering CBMs to reduce the risk of misperception, conflict, or escalation stemming from the use of ICTs. The initial measures from 2013 establish, among other things, a network of national contact points and communication lines to prevent possible tensions resulting from cyber activities.[8] The second set, adopted in 2016, focuses on further enhancing cooperation between participating States through increased exchanges. In the context of cyber/ICT security, CBM 14 specifically emphasizes the promotion of public-private partnerships and the development of mechanisms to exchange best practices on responses to common security challenges, while CBM 15 stresses the importance of improving the security of critical infrastructure through regional and subregional common efforts.[9] It is worth noting there is a significant link between CBMs 14 and 15 with public-private partnerships being essential to critical infrastructure protection as most are privately owned and operated.

The topic of protecting critical infrastructure from cyberattacks has emerged as a key concern of national security for the OSCE in recent years. There have been multiple OSCE discussions and conferences on the matter, and a substantial exploration of public-private partnerships. This includes the Austrian Chairmanship's 2017 Cyber Security for Critical Infrastructure Conference, followed by the Italian Chairmanship's 2018 OSCE Permanent Council meeting on promoting cyber stability through private-public cooperation, as well as its Rome conference later the same year.10 Protecting critical infrastructure was the central theme of an international multi-stakeholder conference during the 2019 Vienna Cyber Security Week.[11] In June 2020, the Albanian OSCE Chair also led a discussion on the role of multi-stakeholder initiatives and public-private partnerships in strengthening cyber resilience.[12] Clearly, the topic is one that resonates with participating States.

Considerable efforts have specifically been made by the OSCE on energy-related critical infrastructure. The organization launched the 2013 *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace.*[13]

7 UN Group of Governmental Experts adopted a consensus (2019-21) report in July 2021: https://bit.ly/3ENL1RN. Norm 13 f, g, and h refer to CI. Another working group – the Open-Ended Working Group – was established in parallel with the GGE, and adopted a final report by consensus in March 2021: https://bit.ly/3CJZInW.

8 OSCE, Permanent Council Decision No. 1106 (Vienna: OSCE Permanent Council, 2013), https://bit.ly/3CzN8rp.

9 OSCE, Permanent Council Decision No. 1202 (Vienna: OSCE Permanent Council, 2016), https://bit.ly/3mtWkrS; T. Greminger, "Security in Modern World," speech delivered in Moscow, April 24, 2019, https://bit.ly/3myxxmE.

10 "Cyber Security," OSCE, accessed Aug 13, 2021, https://bit.ly/3BrJS05; OSCE, "Promoting cyber stability," news release, July 12, 2018, https://bit.ly/3GGgR4D; OSCE "New technological features," news release, Sep 28, 2018, https://bit.ly/3BB13fw.

11 "Vienna Cyber Security Week 2019," accessed October 12, 2021, https://bit.ly/3w9F66f.

12 OSCE, "Albanian OSCE Chair," news release, June 15, 2020, https://bit.ly/3br18If.

13 OSCE, Good Practices Guide (Vienna: OSCE, 2013), https://bit.ly/2ZKJmNO.

In 2019, the OSCE also formed a Virtual Competency and Training Centre focused on the protection of critical energy networks.[14]

Overall, issues relating to cyber/ICT security have generally brought positive recognition from the OSCE of the value of industry/private sector expertise. Stakeholders, such as Kaspersky, Cisco, IBM and Microsoft, have been included in various OSCE dialogues. The Organization also broadly promotes and explores public-private partnerships for cyber/ICT-related issues and, in some cases, facilitates their formation. A case in point is the OSCE field operations. For example, the OSCE Mission to Bosnia and Herzegovina convened the Neretva Group, an international coordination group of public-private stakeholders.[15] The Mission to Serbia also published two editions of a "Guide through Information Security" in the country and helped form an informal public-private partnership framework called the Petnica Group, now the Cyber Security Nexus.[16]

Building on the CBMs: Improving Public-Private Partnerships in the OSCE

With cyberattacks against critical infrastructure becoming an increasingly transnational problem, it is commendable that the OSCE has chosen to focus some of its efforts on cyber/ICT security. It is clear, however, that substantial progress is still needed for several OSCE participating States to implement the CBMs, in particular engaging in public-private partnerships for an ever-evolving cyberspace. While there is clearly an enthusiasm that exists within the OSCE to work with the industry/private sector on an issue like critical infrastructure protection, the reality is that the organization's current relationship and engagements with industry are largely ad hoc, rarely formalized, limited and few and far between.

Moreover, in the case of a potential cross-border threat to critical infrastructure, there is no effective interface between certain stakeholders, regional security organizations and governments. Cybersecurity companies, for instance, lament that, while they possess information about potential security threats, they can lose precious time identifying a suitable entity to engage with.[17]

These companies should in fact be leveraged to help with incident response, malware analysis, and digital forensics. In this vein, participating States should carve out a larger role for the OSCE to support greater cross-border efforts via stronger, swifter, more robust industry partnerships.

The OSCE has one decisive advantage: its comprehensive concept of security and its extensive and diverse membership of participating States, which make it an ideal coordinator for common action. The Organization and its participating States must leverage this advantage more actively. Given the unique – and private – nature of modern critical infrastructure, the OSCE should use its ability as a convener to bring more industry into the fold, and integrate and enhance cooperation between participating States and the private sector so that future cyber/ICT security gaps can be quickly identified and remedied together.

In a large regional security organization such as the OSCE, it is certainly not a simple task to bring participating States together under one common denominator, and the incentive to achieve greater cooperation is not necessarily the same for all.[18] However, while there is a "disequilibrium between offensive and defensive cyber capabilities," a large number of OSCE participating States and their critical infrastructure have already become victims of cyberattacks. It would cost more for them to do nothing. All participating States have an interest in minimizing the risks of a potential attack that would otherwise have unpredictable consequences for themselves and their populations.[19]

14 OSCE, "OSCE heads launch virtual centre," news release, December 5, 2019, https://bit.ly/3EullZ1.

15 OSCE Mission to Bosnia and Herzegovina, "Cyber Security," accessed April 20, 2021, https://bit.ly/3jSzSHb.

16 Irina Rizmal, Guide through Information Security (Belgrade: OSCE Mission, 2018), https://bit.ly/3w4KuaB.

17 A. Kazakova, Sr. Public Affairs Manager, Cyber Diplomacy, Kaspersky, interview by P. Dietrich, Sep 9, 2021.

18 Jack Goldsmith, "Cybersecurity Treaties," in Future Challenges, ed. P. Berkowitz (Hoover Institution, 2011).

19 David P. Fidler, "Whither the Web?" Georgetown Journal of International Affairs 16 (2015): 14.

A Public-Private Partnership Framework for Critical Infrastructure Protection

This paper introduces an initial prevention framework for the OSCE with recommendations to enhance the Organization's efforts in building resilience and trust in stronger partnership with the private sector to achieve the objective of reducing cyber risk/attacks against critical infrastructure in the region. The framework focuses on three major themes: enhancing public-private partnership dialogue, boosting connectivity, and cultivating expertise. It comprises recommendations that leverage the OSCE's more conventional role but also makes forward thinking proposals.

Enhancing Dialogue

1. Public-Private Partnership Task Force

A dedicated OSCE body or consortium aimed at bringing together a broad number of stakeholders – particularly critical infrastructure operators, industry, tech companies, and participating States – in the OSCE area to strengthen cooperation on addressing threats to critical infrastructure, as well as share information, practices and ideas on operational approaches to protection and resilience.[20] Such a body should be established on a formal, permanent basis. It can be responsible for implementing the public-private partnership framework for critical infrastructure protection, establishing sectoral industry working groups, ensuring internal coordination, and organizing joint exercises to test procedures.[21]

2. Industry Days

An annual event series specifically dedicated to information exchange between participating States and industry, as well as cooperation on critical infrastructure protection against cyberattacks. Participating States and industry representatives can host panels/workshops to address specific capability problems and understand latest threats, trends, and other developments. Requests for proposals for logistics, systems, support, and services may be solicited, as well as other opportunities that can be presented to industry. On the event's sidelines, the OSCE could offer added value by facilitating government-to-government, business-to-business, and government-to-business matchmaking.

Boosting Connectivity

3. Leveraging Field Operations

Each OSCE field operation should embrace the local public-private partnership models developed by the Missions in Bosnia and Herzegovina and Serbia, which involve cross-sectoral/multi-stakeholder groups focused on public-private partnerships for cyber/ICT security. These homegrown models should encompass a variety of local participants, including critical infrastructure owner-operators, computer emergency response teams or computer security incident response teams, private cyber/ICT security companies and governments, among others. These setups can provide for information sharing, guidance on national regulations, benchmarking, and capacity building. Such an initiative could result in a wider cooperation network across OSCE field operations. Their experiences could also be translated into guidance, such as a manual on best practices that can be shared more broadly to all participating States and partners.

4. E-Portal

Aggregating in a single electronic point of entry to the OSCE, with all the information regarding the Organization's relationship with industry on the topic of critical infrastructure protection. The platform – possibly an enhanced version of the OSCE POLIS community – can be a place to advertise capability problems and future conferences, provide an entry point for industry to contact the OSCE, coordinate the OSCE's outreach to industry, and encourage and support collaboration projects, among other objectives. The portal could connect industry to relevant business opportunities across the OSCE, including

20 M. Bartsch and S. Frey, Cybersecurity Best Practices (Wiesbaden: Springer Fachmedien Wiesbaden, 2018).

21 The work of intergovernmental organizations with a focus on CI, such as the IAEA or the ICAO, could serve as models.

national or multinational procurement opportunities, and potentially fill cross-border gaps in cyber/ICT security expertise.

Cultivating Expertise

5. Secondment of Experts

The private sector can send experts to work temporarily in OSCE institutions/field operations as consultants for their efforts on critical infrastructure protection. Similarly, the OSCE can help establish secondment schemes between national agencies of participating States and cyber/ICT security companies for closer daily collaboration in conducting research, developing cyber capabilities, and supporting operations related to critical infrastructure protection against cyberattacks. Moreover, a technical cooperation program for private critical infrastructure entities could be launched to help identify vulnerabilities and enhance cyber/ICT security maturity.

6. Ethical Hacker Academy

A training fellowship for young cyber specialists focused on transnational cyber/ICT security challenges with a focus on critical infrastructure could be established. Ethical hackers can partake in challenges co-designed by public/private sector representatives to investigate vulnerabilities in critical infrastructure that require fixing. The program could support tech entrepreneurs who are inventing creative solutions in strategic areas, such as intrusion detection, firewall technology, vulnerability testing, and supply chain risk mitigation.

Bibliography

Bartsch, Michael and Stefanie Frey. Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden (Wiesbaden: Springer Fachmedien Wiesbaden, 2018).

"Brno University Hospital." Cyber Law Toolkit. March 13, 2020. https://bit.ly/3GDKWSf.

Constantin, Lucian. "SolarWinds attack explained." CSO. December 15, 2020. https://bit.ly/3jTwV9i.

"Cyber-attack on Irish health service." BBC. May 20, 2021. https://bbc.in/3ECeAph.

"Cyber-attack: US and UK blame North Korea for WannaCry." BBC. December 19, 2017. https://bbc.in/3CBnWAM.

"Cyber Security for Critical Infrastructure." OSCE. Accessed August 13, 2021. https://bit.ly/3BrJS05.

Fidler, David P. "Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection." Georgetown Journal of International Affairs 16 (2015).

Goldsmith, Jack. "Cybersecurity Treaties: A Skeptical View." In Future Challenges in National Security and Law, edited by Peter Berkowitz (Hoover Institution, 2011).

Greminger, Thomas. "Security in Modern World: regional and global factors and trends." Transcript of speech delivered at the VIII Moscow Conference on International Security, April 24, 2019. https://bit.ly/3myxxmE.

Juniper Research. "Business Losses to Cybercrime Data Breaches." News release. August 19, 2019. https://bit.ly/3w1pr93.

Kazakova, Anastasiia. Sr. Public Affairs Manager, Cyber Diplomacy, Kaspersky. Interview by Philipp Dietrich. Phone. September 9, 2021.

Keohane, David and Peggy Hollinger. "Pandemic brought surge in French cyber attacks, warns Thales CEO." Financial Times. April 5, 2021. https://on.ft.com/3w1mwxd.

"NotPetya cyber-attack." BBC. September 20, 2017. https://bbc.in/3Czfr9A.

OSCE. "Albanian OSCE Chair leads discussion on role of multi-stakeholder initiatives and public-private partnerships in strengthening cyber resilience." News release. June 15, 2020. https://bit.ly/3br18If.

OSCE. Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace (Vienna: OSCE, 2013). https://bit.ly/2ZKJmNO.

OSCE. "New technological features, policy engagement and public-private partnerships." News release. September 28, 2018. https://bit.ly/3BB13fw.

Bibliography

OSCE. "OSCE heads launch virtual centre." News release. December 5, 2019. https://bit.ly/3EuIlZ1.

OSCE. Permanent Council Decision No. 1106 (Vienna: OSCE Permanent Council, 2013). https://bit.ly/3CzN8rp.

OSCE. Permanent Council Decision No. 1202 (Vienna: OSCE Permanent Council, 2016). https://bit.ly/3mtWkrS/.

OSCE. "Promoting cyber stability through co-operation between States and private sector explored at meeting of OSCE Permanent Council." News release. July 12, 2018. https://bit.ly/3GGgR4D.

OSCE Mission to Bosnia and Herzegovina. "Cyber Security." Accessed April 20, 2021. https://bit.ly/3jSzSHb.

Owaida, Amer. "DDoS attack knocks Belgian government websites offline." WeLiveSecurity. May 5, 2021. https://bit.ly/2ZMB73F.

"Recommendations for Critical Information Infrastructure Protection." Federal Office for Information Security. Accessed September 5, 2021. https://bit.ly/3By7rnG.

Rizmal, Irina. Guide through Information Security in the Republic of Serbia 2.0. (Belgrade: OSCE Mission to Serbia, Belgrade Unicom Telecom, Belgrade IBM and Belgrade Juniper, 2018). https://bit.ly/3w4KuaB.

Shaban, Hamza et al. "Cyberattack hits JBS." The Washington Post. June 1, 2021. https://wapo.st/2Zy8OFP.

Stojkovski, Bojan. "North Macedonia Election Commission." BalkanInsight. July 16, 2020. https://bit.ly/3GDB9LQ.

Turton, William and Kartikay Mehrotra. "Hackers Breached Colonial Pipeline Using Compromised Password." Bloomberg. June 4, 2021. https://bloom.bg/3CATOWh.

United Nations General Assembly. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (New York: UN Headquarters, July 14, 2021). https://bit.ly/3ENL1RN.

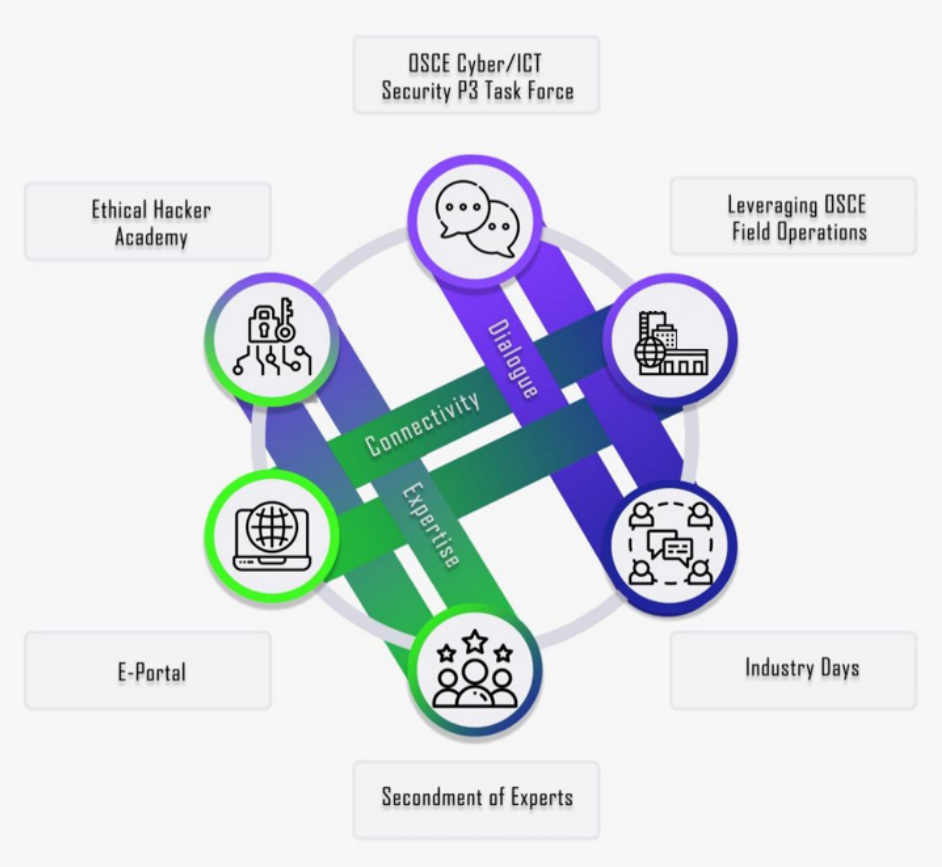
United Nations General Assembly. Open-ended working group on developments in the field of information and telecommunications in the context of international security (New York: UN Headquarters, March 10, 2021). https://bit.ly/3CJZInW.

"Vienna Cyber Security Week 2019." Accessed October 12, 2021. https://bit.ly/3w-9F66f.

"Wild Wide Web: Consequences of Digital Fragmentation." In Global Risks Report 2020. Accessed September 7, 2021. https://wef.ch/2uQFqLz.

Appendix

A Public-Private Partnership Framework for Critical Infrastructure Protection



Colour Legend
Blue: stability and security
Purple: wisdom and trust
Green: innovation and change

Organization for Security and Co-operation in Europe (OSCE)

With 57 participating States in North America, Europe and Asia, the OSCE – the Organization for Security and Co-operation in Europe – is the world's largest regional security organization. The OSCE works to build and sustain stability, peace and democracy for more than one billion people, through political dialogue and projects on the ground. The OSCE is a forum for political dialogue on a wide range of security issues and a platform for joint action to improve the lives of individuals and communities. The Organization helps to bridge differences, build trust and foster co-operation within and between states. With its expert units, institutions and network of field operations, the OSCE addresses issues that have an impact on our common security such as arms control, terrorism, good governance, energy security, human trafficking, democratization, media freedom and national minorities.

The Secretariat, which includes the Conflict Prevention Centre, assists the OSCE Chair in its activities, provides operational and administrative support to field operations and, as appropriate, to other institutions.

The Office for Democratic Institutions and Human Rights in Warsaw promotes democratic elections, respect for human rights, the rule of law, tolerance and non-discrimination, and the rights of Roma and Sinti communities.

The OSCE Academy in Bishkek provides a regional and international public forum for professionals and students in the spirit of co-operation in the fields of international relations, comprehensive security, democratization, the rule of law and human rights.

In cooperation with

OSCE Organization for Security and Co-operation in Europe

FES ROCPE in Vienna

The goal of the FES Regional Office for Cooperation and Peace in Europe (FES ROCPE) of the Friedrich-Ebert-Stiftung in Vienna is to come to terms with the challenges to peace and security in Europe since the collapse of the Soviet Union a quarter of a century ago. These issues should be discussed primarily with the countries of Eastern Europe – Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine – and with Russia, as well as with the countries of the EU and with the US. The security order of Europe, based until recently on the Helsinki Final Act (1975) and the Paris Charter (1990), is under threat. This is, among others, a result of different perceptions of the development of international relations and threats over the last 25 years, resulting in divergent interests among the various states.

For these reasons, ROCPE supports the revival of a peace and security dialogue and the development of new concepts in the spirit of a solution-oriented policy. The aim is to bring scholars and politicians from Eastern Europe, Russia, the EU and the US together to develop a common approach to tackle these challenges, to reduce tensions and to aim towards conflict resolution. It is our belief that organizations such as the FES have the responsibility to come up with new ideas and to integrate them into the political process in Europe.

We support the following activities:

- Regional and international meetings for developing new concepts on cooperation and peace in Europe;
- A regional network of young professionals in the field of cooperation and peace in Europe;
- Cooperation with the OSCE in the three dimensions: the politico-military, the economic and the human.

ISBN 978-3-98628-103-8

FES Regional Office for Cooperation
and Peace in Europe
Reichsratsstr. 13/5, A-1010 Vienna
Phone: +43 1 890 38 11 205
Fax: +43 1 890 38 11 400
https://peace.fes.de/

Responsible: Christos Katsioulis