Centar za sigurnosne studije - BIH

Centre for Security Studies - BH

DIGITAL SECURITY SECTOR GOVERNANCE AND REFORM

2025

Centar za sigurnosne studije - BIH

Centre for Security Studies - BH

DIGITAL SECURITY SECTOR GOVERNANCE AND REFORM

Editor:

Benjamin Plevljak

Author:

Martina Valentini

Martina Valentini holds a Master's degree in Conflict Resolution in Divided Societies from King's College London. She previously earned a BA in Combined Honours (Politics, Japanese, and Spanish) from Newcastle University, which included a semester at Hitotsubashi University in Tokyo. Her research interests include international law, European politics, and transitional justice.

May, 2025

These contents represent the views of the author only and is his/her sole responsibility. The Centre for Security Studies does not accept any responsibility for use that may be made of the information it contain.

ABSTRACT

This paper addresses the topic of how to implement good digital Security Sector Governance and Reform (SSG/R). First, it provides an overview of what SSG/R is, secondly, it details the existing standards at the European Union (EU) level which can be interpreted as good practice examples. In the final section, the principles of good digital SSG/R are analysed both theoretically and in practice, with great attention posed to accountability, transparency and oversight mechanisms. This section specifically provides guidance on parliamentary and civil society oversight, both individually and in collaboration. The paper is based entirely on qualitative desk research, employing a range of secondary sources.

The research concludes that to successfully implement good digital SSG/R, policy and lawmakers need to approach the topic in accordance with the principles of good digital SSG/R, involving all security actors, including civil society, in all phases of the development and implementation process. Oversight mechanisms, pertaining to both parliament and civil society, are essential in the creation and the continued work of good digital SSG/R. The paper also highlights the importance of adhering to EU standards as guidelines to achieve a comprehensive legal framework. Lastly, the recurring emergence of the need for collaboration across security actors, both in theory and practice, underscores the importance of collaboration and coordination mechanisms within security sector actors, civil society, and national and international institutions.

Key words: *Cybersecurity, Digital SSG/R, EU Cybersecurity Policy, Accountability, Transparency, Civil Society Oversight*

Contents

List of Tables

Introduction

European states have experienced a rise in cyberattacks and threats in recent years, which have prompted many states and international organisations, such as the European Union (EU), to develop extensive legal frameworks aimed at improving the state of digital security and increase preparedness in countering cyberthreats. Digital Security Sector Governance and Reform (SSG/R) plays a pivotal role in the digitalisation of the security sector, as it provides guidance on good practices and principles for states that are attempting to create a cybersecurity legal framework or that wish to improve their existing one.

This paper serves as an overview on good digital SSG/R practices, which are to be taken into account by practitioners and lawmakers in the security sector. Firstly, a brief literature review is presented to define the concept of digital SSG/R and to outline the reasons behind its central importance. In the following section, the paper will explore what are key international standards and frameworks regarding Digital SSG/R and in particular cybersecurity and digitalisation, providing an overview of the main directives and policies at the EU level, both generally and in regard to the security sector. These legal frameworks should be understood as an example of good practice for any states wishing to enhance its cybersecurity legal frameworks and/or ultimately accede to the EU. Lastly, great attention is posed on the SSG/R principles of accountability and transparency, with the last section focusing on oversight mechanisms in theory and practice. Firstly, the importance of establishing a good network of oversight actors, both within the government, such as parliament, and outside state institutions, such as civil society actors, is underscored through a theoretical approach. Secondly, examples of oversight practices in Digital SSG/R will be provided, both for parliamentary and state actors and civil society actors separately and highlighting the meeting points for collaboration between the two.

This study adopts a qualitative desk-based research methodology, relying on a range of secondary sources. The sources employed in this paper include EU policies, joint communications and directives as legal sources aimed at providing an understanding of the institutional and regulatory cybersecurity framework. Other sources include academic articles, which provide theoretical frameworks and empirical studies on digital SSG/R, and reports drafted by international organisations and think tanks such as the Geneva Centre for Security Sector Governance (DCAF) and the Organisation for Security and Cooperation in

Europe (OSCE). These reports provide more updated insights in the development of SSG/R studies and offer policy recommendations.

The heavy reliance on policies and reports in this paper is due to the limited existing scholarship on digital SSG/R. While more studies have covered the topic of SSG/R in general, digital SSG/R is still a relatively new addition to the field of security studies and cybersecurity. In addition to this, the rapidly evolving technological developments hamper the advancement of digital SSG/R studies. This results in a limited availability of both theoretical frameworks and empirical studies, which could hinder the in-depth evaluation of research outcomes.

The lack of scholarship on the topic contributes to the relevance of this study. This paper aims at providing an overview of good digital SSG/R, both in theory and practice and with reference to EU standards, in order to provide security sector actors, policy makers, practitioners and scholars with guidelines on the implementation of good digital SSG/R. With the increase in cyber threats states have faced in recent years, the paper also addresses a timely topic, especially relevant for countries which only have a partial cybersecurity framework, or no framework at all.

Literature review

Digital Security Sector Governance and Reform theory: What is digital SSG/R?

In an increasingly digital world, digitalisation as a security challenge is reshaping and reframing our understanding of good governance while also involving new security actors within the security landscape[1]. Society has become increasingly dependent on digital infrastructures, and securing those infrastructures has become a priority for many governments[2]. For this reason, it is of great importance for national governments to develop adequate legal frameworks and national cybersecurity strategies, while also ensuring that technological systems are up to the challenges and roles that they play in society[3]. This is vital to ensure that states have the right resources to face emerging security threats related to digitalisation, which are both threats to transnational security and to human and societal security[4], as digital technologies have exacerbated the stress on the dynamic between individual and societal freedom of expression, and between the right to privacy and the state's obligation to protect its citizens[5].

This is where Digital Security Sector Governance and Reform (SSG/R) comes in. The security sector is widely considered a cornerstone of post-conflict reconstruction, democratisation and state-building efforts[6], which is the reason why great importance is given to good SSG/R, especially in post-conflict societies. SSG/R puts good governance as a central tenet, aiming at exercising power and authority according to a set values-based standards[7], which are generally recognised to include democracy, transparency,

[1] DCAF – Geneva Centre for Security Sector Governance. *Digitalization and Security Sector Governance and Reform (SSG/R).* SSR Backgrounder Series. Geneva: DCAF, 2022. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_23_Digitalization_ENV2.pdf.

[2] Sabrina Ellebrecht, and Stefan Kaufmann. "Digitalization and Its Security Manifestations." *European Journal for Security Research* 5 (2020): 1–3, https://doi.org/10.1007/s41125-019-00063-8.

[3] Cody Collum, and Houssain Kettani. "On Security Implications of Emerging Technologies." In *Proceedings of the 2022 International Conference on Emerging Technologies*, 1–10. Association for Computing Machinery, 2022. https://doi.org/10.1145/3528137.3528159.

[4] DCAF, *Digitalization and Security Sector Governance and Reform.*

[5] Graeme P. Herd, Detlef Puhl, and Sean Costigan. *Emerging Security Challenges: Framing the Policy Context*. GCSP Policy Paper 2013/5. Geneva: Geneva Centre for Security Policy, 2013. https://www.files.ethz.ch/isn/169211/GCSP%20PP%202013-5.pdf.

[6] , Aris Sarjito, and Yin Chhao Rath. "Security Sector Reform and Implementation of Good Governance: A Theoretical Study." *Aplikasi Administrasi: Media Analisa Masalah Administrasi* 27 no. 2 (2024):82-96,https://jaa.hangtuah.ac.id/index.php/jurnal/article/view/257/153.

[7] George R. Lucas, Jr., Dragan Lozancic, Grazvydas Jasutis, Frederic Laker, Kakhaber Kemoklidze, and Rebecca Mikova. *Conceptualizing the Relationship of Good Security Sector Governance to the State Security System*. Geneva: DCAF – Geneva Centre for Security Sector Governance, 2022. https://www.dcaf.ch/sites/default/files/publications/documents/RelationshipGoodSecuritySectorGovernanceStateSecuritySystem_EN.pdf.

accountability, rule of law and gender equality among others to increase a country's ability to meet a range of security needs[8]. Good SSG/R should always take a cross-dimensional approach, considering the links between the different actors in the security sector[9] and feature a comprehensive programming that incorporates deeper and politically sensitive elements ranging from parliamentary oversight and the strengthening of civil society groups[10].

Digitalisation today can be considered an Emerging Security Threat, potentially bringing a reshaping of the existing governance structures and new patterns of cooperation across state security institutions. This, combined with states and societies growing dependency on technology leading to a more complex security landscape[11], has created a scenario in which SSG/R plays an important role in reinforcing (or in some cases establishing) digital governance. With the rapidly evolving of state infrastructure due to new digital technologies, digital SSG/R can ensure that the use of digital technologies is compatible with principles of good governance and international human rights standards[12], while also enabling states to update legal frameworks in a timely manner to keep up with new technological developments.

[8] Paul Jackson. "Introduction: Second-Generation Security Sector Reform." *Journal of Intervention and Statebuilding* 12 no. 1 (2018): 1–10. https://doi.org/10.1080/17502977.2018.1426384 ; Arugay, Aries A., and Justin Keith A. Baquisal. *Accountability, Discourse, and Service Provision: Civil Society's Roles in Security Sector Governance and Reform (SSG/R) and Sustainable Development Goal-16 (SDG-16)*. Geneva: DCAF – Geneva Centre for Security Sector Governance, 2024. https://www.dcaf.ch/sites/default/files/publications/documents/SSR_Paper-Accountability-Discourse.pdf.

[9] Organization for Security and Co-operation in Europe (OSCE). *Security Sector Governance and Reform: Guidelines for OSCE Staff*. Vienna: OSCE Secretariat, Conflict Prevention Centre, Operations Service, 2022. https://www.osce.org/files/f/documents/2/4/512470_0.pdf.

[10] Jackson, "Introduction: Second-Generation Security Sector Reform".

[11] Dawn Lui, and Alexandru Lazar. *Digitalization and SSG/R: Projections into the Future*. Geneva: DCAF – Geneva Centre for Security Sector Governance, 2023. https://www.dcaf.ch/sites/default/files/publications/documents/Digitalization-and-SSGR_Projections-Future_EN-2.pdf.

[12] ibid.

Digital SSG/R International Legal Frameworks: EU Frameworks and Policies

European states have experienced a rise in cyberattacks and threats, which has led many member states and the EU as a whole to develop cybersecurity frameworks that are overall aligned in shared objectives. Such objectives include establishing incident reports mechanisms, addressing cybercrime, engaging in international cooperation, and strengthen training and educational programmes among others[13], and all are essential to the main legislative frameworks at the European Union (EU) level, with many representing requirements in the chapters of the EU acquis regulating EU accession. For aspiring EU members, it is of the utmost importance to ensure that any approved National Cybersecurity Strategy (NCS) is consistently aligned with European frameworks[14], and with the guidelines for the acquis process especially in respect of chapters; 10 on Information, society and media, chapter 23 on Judiciary and fundamental rights, and chapter 24 on Justice, Freedom and Security[15]. These include the alignment with conventions such as the 2001 Budapest Convention on Cybercrimes and subsequent Additional Protocols, and a range of EU regulations on different aspects of digital security. The following paragraphs outline the main EU policies and directives on cybersecurity, which are also summarised in Table 1.

The most relevant EU legal framework on cybersecurity is the NIS2 Directive (Directive 2022/2555) on the new rules on cybersecurity of network and information systems. Approved in 2022, it builds on its predecessor NIS1 (approved in 2016), expanding the sectors included in the directive and updating requirements for Member States. It provides legal measures aimed at boosting the overall level of cybersecurity through legal obligations across 18 sectors of economy, introducing measures such as new security requirements and notification of incidents. It also requires Member States to increase preparedness with missions for Computer Security Incident Response Teams (CSIRTs) and related competent authorities, while promoting cooperation among Member States in all areas of cybersecurity[16].

[13]European Union Agency for Cybersecurity (ENISA). *2024 Report on the State of the Cybersecurity in the Union*. Luxembourg: Publications Office of the European Union, 2024. https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union.

[14] Geneva Centre for Security Sector Governance (DCAF). *National Cybersecurity Strategies in Western Balkan Economies*. Geneva: DCAF, 2021. https://www.dcaf.ch/sites/default/files/publications/documents/NationalCybersecurityStrategiesWB_2021.pdf.

[15] European Commission. “Chapters of the Acquis.” *Enlargement Policy – Conditions for Membership*. Accessed April 22, 2025. https://enlargement.ec.europa.eu/enlargement-policy/conditions-membership/chapters-acquis_en.

[16] Enisa, *2024 Report on the State of the Cybersecurity in the Union.*

It aims to do so by establishing a higher common level of security for network and information systems, creating a unified legal framework which includes the introduction of risk management measures and reporting requirements, and detailed rules on how Member States should cooperate on security and information sharing, the setup of supply chain security, vulnerability management and education awareness on cyberthreats[17].

The EU approved several more frameworks in the years leading up to and following NIS2, with much narrower focus. The 2019 Cybersecurity Act introduced a certification framework for Information and Communication Technology, products and services, while also bestowing ENISA, the European Union Agency for Cybersecurity, with a permanent mandate, tasking it with increasing cooperation at the EU level by helping Member States to handle cybersecurity incidents, supporting coordination in case of large-scale cross-border cyberattacks, informing the public and monitoring the new cybersecurity certification framework[18]. The 2020 Cybersecurity Strategy sets out how the EU can achieve technological sovereignty while ensuring a global and open internet with strong safeguards in regard to European citizens' security and fundamental rights. It does so through three regulatory instruments: resilience, technological sovereignty and leadership; operational capacity to prevent, deter and respond; and cooperation to advance a global and open cyberspace[19]. Another notable EU regulation is the 2022 Critical Entities Resilience Directive, which provides a list of essential services needed to guarantee key societal functions such as the energy, health and transport sectors, and calls for Member States to identity critical entities within these sectors and take measures to ensure their resilience[20]. The most recent developments include the Cyber Resilience Act (2024), which introduces common cybersecurity requirements to any products sold and employed within the EU which has digital elements, aiming at minimising vulnerability and protecting businesses and

[17] European Union. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Official Journal of the European Union L 333, December 27, 2022, pp. 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[18] European Union. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Official Journal of the European Union L 151, June 7, 2019, pp. 15–69. https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[19] European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *The EU's Cybersecurity Strategy for the Digital Decade*. JOIN(2020). Brussels: European Commission, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN.

[20] European Parliament and Council of the European Union. *Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*. Official Journal of the European Union L 333, 27 December 2022, pp. 164–198. https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

institutions buying software and hardware[21], and the Cyber Solidarity Act (2025), which introduces measures to strengthen EU capacities to detect, prepare for and respond to cybersecurity threats and incidents[22].

All the directives and acts outlined above provide a general legal framework for cybersecurity and information networks to cover the majority of areas touched by digitalisation. However, the EU released comprehensive policies also in regard to the security sector. In 2022 the EU has released a Joint Communication outlining its EU Policy on Cyberdefence, aiming at enhancing the EU and Member State's ability to prevent, deter and defend against cyberattacks using all available means, while also increasing cooperation and coordination among the EU's cyber defence actors, including both civilian and military cyber communities, and develop mechanisms for leveraging capabilities at the EU level to achieve a more efficient crisis management mechanism[23]. The EU Policy on Cyberdefence is based on four pillars: acting together for a strong cyberdefence, securing the EU defence ecosystem, invest in cyberdefence capabilities, and partnering to address common challenges[24]. This policy is supported by the 2024 European Defence Industrial Strategy, which aims at strengthening the European Defence and Technological Industrial Based by improving responsiveness of the EU defence industry, increasing collaboration and mainstreaming a defence readiness in EU policies[25]. Moreover, the EU's Permanent Structured Cooperation mechanism (PESCO) includes several cybersecurity-focused projects, all built on impact-based cooperation activities[26].

[21] European Parliament and Council of the European Union. *Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. Official Journal of the European Union L 2847, 20 November 2024, pp. 1–81. https://eur-lex.europa.eu/eli/reg/2024/2847/oj.

[22] European Parliament and Council of the European Union. *Regulation (EU) 2025/38 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)*. Official Journal of the European Union L 38, 15 January 2025, pp. 1–34. https://eur-lex.europa.eu/eli/reg/2025/38/oj.

[23] European External Action Service. *EU Policy on Cyber Defence*. Brussels: EEAS, 2022. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf.

[24] ibid.

[25] European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *Joint Communication: A New European Defence Industrial Strategy—Achieving EU Readiness Through a Responsive and Resilient European Defence Industry*. JOIN(2024). Brussels: European Commission, 2024. https://defence-industry-space.ec.europa.eu/document/download/643c4a00-0da9-4768-83cd-a5628f5c3063_en?filename=EDIS%20Joint%20Communication.pdf.

[26] European Union. *Permanent Structured Cooperation (PESCO)*. Accessed April 28, 2025. https://www.pesco.europa.eu.

YEAR	DIRECTIVE/POLICY	SUMMARY
2001	Budapest Convention on Cybercrime	First international treaty on online crime.
2016	NIS1 Directive (Directive on Security of Network and Information Systems)	First EU-wide legislation on cybersecurity, requiring national strategies, incident reporting and coordination mechanisms.
2019	Cybersecurity Act	Gives ENISA a permanent mandate and establishes a certification framework for ICT products.
2020	EU Cybersecurity Strategy	Aims to ensure technological sovereignty and protect fundamental rights through resilience, operational capacity and global cooperation in cyberspace.
2022	NIS2 Directive (New Rules on Cybersecurity of Network and Information Systems)	Updates NIS1 by expanding the scope to more sectors and strengthening cybersecurity risk management, incident reporting and cooperation.
2022	Critical Entities Resilience Directive	Requires Member States to identify essential services and ensure their resilience against physical and cyber threats.
2022	EU Policy on Cyberdefence	Enhances EU capacity to prevent and respond to cyberattacks, emphasising cooperation across civilian and military actors.
2024	Cyber Resilience Act	Introduces cybersecurity requirements for all digital products sold in the EU, aiming to reduce vulnerabilities.
2024	European Defence Industrial Strategy	Strengthens the EU defence industry with a focus on responsiveness, collaboration and readiness for cyberdefence challenges.
2025	Cyber Solidarity Act	Aims to boost EU capacity for detecting, preparing for and responding to cyberthreats, including cross-border incidents.

Table 1 - Summary of EU directives and policies on cybersecurity

Principles of Accountability and Transparency: The Importance of Government and Civil Society Oversight

Theoretical approaches

The EU legal framework for the digital security sector outlined above is a vital reference point for any state wishing to establish a NCS or updating their existing framework. However, good digital security sector governance and reform is based on principles, most importantly accountability and oversight, of which the practical manifestation are oversight mechanisms, including both government oversight and civil society.

The overarching aim of digital SSG/R is for the security sector to include institutions that serve public interest transparently[27], and it runs the risk of becoming ineffective if such principles of transparency and accountability are overlooked[28]. These two principles sit at the core of SSG/R, with accountability presupposing both internal and external oversight mechanism, often implemented by independent authorities. Transparency usually encompasses the evident use of digital capabilities by security sector actors, which in practice includes the public availability of information from government and other authorities with related increased availability of digital tools and regulations on the sharing of confidential information and privacy issues[29]. Good digital SSG/R also needs to account for other relevant principles, such as rule of law, as all individuals and institutions are subject to impartial laws; participation to bridge the digital divide and provide equitable and inclusive access; responsiveness to clearly define security objectives and policies; efficiency, and human rights. The latter is particularly important, as the digital security sectors carries with it the potential of incurring in human rights abuses by the security sector, for example in relation to privacy issues, and it is of the utmost importance to ensure that the legal mandate of security institutions to use coercive force in the name of national security, in certain situations depriving citizens of their rights, is also subject to democratic control and aimed at protecting individuals and communities[30].

[27] Ursula C. Schroeder and Fairlie Chappuis, "New Perspectives on Security Sector Reform: The Role of Local Agency and Domestic Politics," *International Peacekeeping* 21, no. 2 (2014): 133–48, https://doi.org/10.1080/13533312.2014.910401.
[28] Sarjito and Rath, "Security Sector Reform and Good Governance".
[29] DCAF, *Digitalization and Security Sector Governance and Reform.*
[30] ibid.

It is of particular importance for policy makers and government institutions to take these principles into account when drafting and implementing new legal frameworks for the digital security sector, mostly to ensure the creation of an efficient, effective and transparent legal framework, but also to avoid human rights violations and to achieve a lasting and coherent legal framework able to keep up with new technological and societal developments, and avoid human rights violations. Other issues that might incur are the lack of political will, which is a critical factor not only during the drafting process, but also during the implementation phase[31]. It is also important that these programmes are locally owned to ensure they will be able to respond to local needs and that they can count on public trust[32], and that they account for insider perspectives, such as those of civil society, to assist with advice and concerns over new reforms[33].

To uphold these principles and implement legal frameworks that are compliant with good digital SSG/R, oversight mechanisms need to play a central role. According to the Organisation for Security and Cooperation in Europe (OSCE), democratic oversight can be considered itself a principle of good digital SSG/R[34], given that they are tasked with upholding the remaining principles. The OSCE emphasises the need for oversight bodies have an effective mandate which will allow them to perform their duties effectively through capacity building, while also raising awareness of civil society and media of their role and duties[35], as the integration of public participation and transparent efforts lead to an increase in legitimacy, while also enhancing accountability by allowing citizens to have a voice, and ensuring that policies are accessible to the public[36].

For these reasons, oversight mechanisms need to include both government oversight and civil society oversight, acting in parallel, but with the same goal. Government and parliamentary oversight is particularly important in creating and strengthening of institutions, and more practical aspects such as setting up independent audit offices to monitor expenditure[37], enhancing the overall knowledge level and data literacy of security sector personnel, and develop different entities that are responsible for oversight which will likely acquire different

[31] Sarjito and Rath, “Security Sector Reform and Good Governance”.
[32] Eleanor Gordon, “Security Sector Reform, Statebuilding and Local Ownership: Securing the State or Its People?” *Journal of Intervention and Statebuilding* 8, no. 2–3 (2014): 126–48, https://doi.org/10.1080/17502977.2014.930219.
[33] Schroeder and Chappuis, “New Perspectives on Security Sector Reform”.
[34] OSCE, *Security Sector Governance and Reform.*
[35] ibid.
[36] Sarjito and Rath, “Security Sector Reform and Good Governance”.
[37] ibid.

types of expertise, aimed at better navigating and analysing digital systems and digital transformations[38].

Even more relevant is civil society oversight. A civil society that is engaged with current security issues can be a valuable asset, as it creates a direct channel of communication with the diverse views of the population[39], while also acting as a force counterbalancing government excess by creating a more effective, efficient, responsive, accountable and transparent security institutions, and enabling citizens to influence decisions that directly affect their lives and engage in processes aimed at improving their own security[40]. They can do so as they possess knowledge on the needs of less represented groups and of regional issues, while also holding authorities accountable through activities such as lobbying and advocacy campaigns[41]. Moreover, academia and think tanks can provide research and analysis on current security issues, while the media can assist in ensuring information is publicly available[42]. Lastly, it is fundamental for governments to consider civil society as an important security actor and to include it in the SSG/R process by maintaining a continuous and meaningful dialogue with it and open spaces for new discourses on security and development[43]. On the other hand, it is important for civil society to acquire more knowledge on the topic of SSG/R and constantly keep up with new technological developments, and also seek clarifications with institutions when there is not enough clarity on a given issue[44], both to ensure they are up to date with reforms and to be able to inform the wider public on such developments.

[38] Lui and Lazar, *Digitalization and SSG/R*.

[39] Geneva Centre for Security Sector Governance (DCAF). *Civil Society: Roles and Responsibilities in Good Security Sector Governance*. SSR Backgrounder No. 17. Geneva: DCAF, November 2022. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_17_CivilSociety_Nov2022.pdf.

[40] Gordon, "Security Sector Reform, Statebuilding and Local Ownership".

[41] OSCE, *Security Sector Governance and Reform*.

[42] ibid.

[43] Arugay and Baquisal, "*Accountability, Discourse, and Service Provision".*

[44] ibid.

Practical approaches

In regard to practical oversight activities and policies that both parliament and civil society can focus on, the Geneva Centre for Security Sector Governance (DCAF)[45] and other organisations such as the OSCE[46] and the OECD[47] have outlined a range of suggestions for both.

Parliaments are usually responsible for setting the operational standards for the use of digital technologies by security sector actors, including adopting stronger regulations and have the capacity to strengthen the relation of security providers with human rights through their legislative, representative, budgetary and oversight functions[48]. A strong parliamentary oversight framework is necessary for greater digitalisation in the security sector, with clear tasks and rules being outlined, and with the decisions of oversight actors regarding violation of laws by security agency being binding[49]. For these reasons, their oversight function is extremely important, as they have the ability to directly affect policies and framework through different activities:

- Standardise oversight approaches and strengthen legal frameworks, including providing uniform and impartial reporting standards to ensure the principles of SSG/R are upheld by security institutions;
- Exert pressure on government officials to be efficient and avoid mismanagement and ensure the legal framework development process works for the benefit of citizens;
- Establish cooperation mechanisms with overseas security actors and domestically both with public and private organisations;
- Enact safeguards based on principles and ethical guidelines to ensure security providers respect human rights;

[45] Geneva Centre for Security Sector Governance (DCAF). *Human Rights and Security Sector Governance/Reform*. SSR Backgrounder No. 22. Geneva: DCAF, November 2022. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_22_HumanRights_andSSG_R_Nov2022.pdf.
Lui and Lazar, *Digitalization and SSG/R*.
DCAF, *Digitalization and Security Sector Governance and Reform.*
Lucas et al., Conceptualizing the Relationship of Good Security Sector Governance.
Arugay and Baquisal, Accountability, Discourse, and Service Provision.
[46] OSCE, *Security Sector Governance and Reform.*
[47] Organisation for Economic Co-operation and Development (OECD). *Recommendation of the Council on National Digital Security Strategies*. OECD Legal Instruments, OECD/LEGAL/0480. Paris: OECD, September 26, 2022. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480.
[48] DCAF, *Human Rights and Security Sector Governance/Reform.*
[49] Lui and Lazar, *Digitalization and SSG/R*.

- Define priority tasks for security sector agencies and raise awareness of responsibilities among government agencies; and
- Organise gender-sensitive participatory and inclusive interaction with citizens through online platforms aimed at answering queries and receiving feedback.

Parliamentary oversight needs to be complemented by civil society oversight. A well organised civil society can monitor and uncover systemic issues and human rights abuses by the security sector and raise alarms both nationally and internationally in case of violations[50], while also bringing citizens' perspectives in the drafting and implementation of digital security legal frameworks. Civil society has many points of entry to bring benefit to good digital SSG/R:

- Establish digitalised activities aimed at working efficiently across different contexts and ensure the delivery of critical digital services platforms to vulnerable people and communities;
- Establish a network of collaboration between different CSOs, academia, think tanks to ensure that security providers both act in respect of human rights, and that new policies are up to date with new technological developments;
- The same networks of organisations should engage in other activities such as providing research and analysis and legal advice to each other and to institutions;
- Obtain information on the opinions of citizens to ensure that their needs are met, while also building capacities to include marginalised groups, and provide the government with suggestions on how to improve such policies;
- Monitor the impact of government policies on the communities;
- Support the activities of the defence sector through awareness-raising activities aimed both at security sector actors and at citizens; and
- Create mechanisms to denounce hate speech and to streamline complaints against security sector actors and denounce the infringements of human rights.

While it is important for parliamentary oversight to focus on the developing and upholding of legal standards, and for civil society to focus on amplifying the voice of communities, there are also several meeting points for parliamentary and civil society to collaborate.

[50] DCAF, *Human Rights and Security Sector Governance/Reform.*

First, they need to collaborate on ensuring that new technologies act according to ethical principles, for example in ensuring that there are no biases stemming from algorithmic decision making which can lead to discrimination against certain groups[51]. Secondly, they should collaborate on the creation of accessible digital public spaces while also focusing on empowering marginalised communities. Lastly, a greatly important meeting point is the establishment of training courses, which should cover both the importance of principles of accountability and transparency and comprehensive awareness of technical trends and digital systems[52].

[51] Lui and Lazar, *Digitalization and SSG/R*.

[52] ibid.

Conclusion

This paper has provided an overview of the concept of digital Security Sector Governance and Reform, both from a theoretical perspective and a practical one. It has firstly provided a definition of digital SSG/R within the current context of increased digitalisation, while also underscoring its importance. The second section has focused on international standards, in particular EU-level standards, policies, directive and practices which can serve as a reference for countries that are new to digital SSG/R, or that are developing or updating their National Cybersecurity Strategies. Especially important is the NIS2 directive, which acts as an overarching framework on cybersecurity and information services in the EU. The final section focused on principles of good digital SSG/R, with great attention paid to the principles of accountability and transparency and the oversight mechanisms needed to enforce them, both at the parliamentary level and at the civil society one. A theoretical overview has been given on the importance of both parliamentary and civil society oversight, with the addition of practical activities that can be carried out by each individually, and some activities which in turn need to encompass both parliament and civil society.

The main research findings emerging are focused on the importance of applying the principles of good SSG/R, such as accountability and transparency, to the digital security sector. The application of these principles needs to encompass all security sector actors, including governments, security sector providers and civil society, with all the actors included in all phases of the development and implementation of new or improved cybersecurity legal frameworks. The paper also underscores the high importance of the development of oversight mechanisms, which need to be established both within parliaments and civil society. These two types of oversight institutions need to be established and improved both on their own, in relation to their own specific strengths, but also need to occasionally work together on common projects, such as training courses, to achieve more effective, transparent and accountable digital SSG/R.

Secondly, for countries who are attempting to create a national cybersecurity legal framework, or are aiming to complete or improve existing one, the EU level directives and policies presented in this paper offer valuable guidelines for lawmakers. The EU has emanated directives, policies and communications covering many areas, from security and defence to information network systems, to critical entities.

This comprehensive approach shows the range needed for a cybersecurity framework to be effective, while the constant updates with new directives and policies show that there is a need for governments to be constantly updating legal frameworks to keep up with technological developments.

Lastly, the need for collaboration between institutions, security providers and civil society emerges from both literature and policy recommendations on digital SSG/R and is included in many EU policies and directives. Collaboration and coordination need to happen on all levels, both internally within government institutions, and externally, involving security sector providers, other governments and international organisations, and most importantly civil society actors. The latter are extremely important as they represent the interest and concerns of the wider public and are thus instrumental in understanding citizen’s opinion on the policies, and to collect information on the needs of communities, particularly vulnerable ones. Collaboration and coordination are not only crucial for the creation of a cybersecurity legal framework, but are also vital in ensuring that the framework remains up to date with technological developments and societal changes, which is notably one of the challenges in implementing good digital SSG/R.

Bibliography

Arugay, Aries A., and Justin Keith A. Baquisal. *Accountability, Discourse, and Service Provision: Civil Society's Roles in Security Sector Governance and Reform (SSG/R) and Sustainable Development Goal-16 (SDG-16)*. Geneva: DCAF – Geneva Centre for Security Sector Governance, 2024. https://www.dcaf.ch/sites/default/files/publications/documents/SSR_Paper-Accountability-Discourse.pdf.

Collum, Cody, and Houssain Kettani. "On Security Implications of Emerging Technologies." In *Proceedings of the 2022 International Conference on Emerging Technologies*, 1–10. Association for Computing Machinery, 2022. https://doi.org/10.1145/3528137.3528159.

DCAF – Geneva Centre for Security Sector Governance. *Digitalization and Security Sector Governance and Reform (SSG/R)*. SSR Backgrounder Series. Geneva: DCAF, 2022. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_23_Digitalization_ENV2.pdf.

Ellebrecht, Sabrina, and Stefan Kaufmann. "Digitalization and Its Security Manifestations." *European Journal for Security Research* 5 (2020): 1–3, https://doi.org/10.1007/s41125-019-00063-8.

European Commission. "Chapters of the Acquis." *Enlargement Policy – Conditions for Membership*. Accessed April 22, 2025. https://enlargement.ec.europa.eu/enlargement-policy/conditions-membership/chapters-acquis_en.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *Joint Communication: A New European Defence Industrial Strategy—Achieving EU Readiness Through a Responsive and Resilient European Defence Industry*. JOIN(2024). Brussels: European Commission, 2024. https://defence-industry-space.ec.europa.eu/document/download/643c4a00-0da9-4768-83cd-a5628f5c3063_en?filename=EDIS%20Joint%20Communication.pdf.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *The EU's Cybersecurity Strategy for the Digital Decade*. JOIN(2020). Brussels: European Commission, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN.

European External Action Service. *EU Policy on Cyber Defence*. Brussels: EEAS, 2022. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf.

European Parliament and Council of the European Union. *Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*. Official Journal of the European Union L 333, 27 December 2022, pp. 164–198. https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

European Parliament and Council of the European Union. *Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. Official Journal of the European Union L 2847, 20 November 2024, pp. 1–81. https://eur-lex.europa.eu/eli/reg/2024/2847/oj.

European Parliament and Council of the European Union. *Regulation (EU) 2025/38 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)*. Official Journal of the European Union L 38, 15 January 2025, pp. 1–34. https://eur-lex.europa.eu/eli/reg/2025/38/oj.

European Union. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Official Journal of the European Union L 333, December 27, 2022, pp. 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

European Union. *Permanent Structured Cooperation (PESCO)*. Accessed April 28, 2025. https://www.pesco.europa.eu.

European Union. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Official Journal of the European Union L 151, June 7, 2019, pp. 15–69. https://eur-lex.europa.eu/eli/reg/2019/881/oj.

European Union Agency for Cybersecurity (ENISA). *2024 Report on the State of the Cybersecurity in the Union*. Luxembourg: Publications Office of the European Union, 2024.

https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union.

Geneva Centre for Security Sector Governance (DCAF). *Civil Society: Roles and Responsibilities in Good Security Sector Governance*. SSR Backgrounder No. 17. Geneva: DCAF, November 2022. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_17_CivilSociety_Nov2022.pdf.

Geneva Centre for Security Sector Governance (DCAF). *Human Rights and Security Sector Governance/Reform*. SSR Backgrounder No. 22. Geneva: DCAF, November 2022. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_22_HumanRights_andSSG_R_Nov2022.pdf.

Geneva Centre for Security Sector Governance (DCAF). *National Cybersecurity Strategies in Western Balkan Economies*. Geneva: DCAF, 2021. https://www.dcaf.ch/sites/default/files/publications/documents/NationalCybersecurityStrategiesWB_2021.pdf

Gordon, Eleanor. "Security Sector Reform, Statebuilding and Local Ownership: Securing the State or Its People?" *Journal of Intervention and Statebuilding* 8, no. 2–3 (2014): 126–48, https://doi.org/10.1080/17502977.2014.930219.

Herd, Graeme P., Detlef Puhl, and Sean Costigan. *Emerging Security Challenges: Framing the Policy Context*. GCSP Policy Paper 2013/5. Geneva: Geneva Centre for Security Policy, 2013. https://www.files.ethz.ch/isn/169211/GCSP%20PP%202013-5.pdf.

Jackson, Paul. "Introduction: Second-Generation Security Sector Reform." *Journal of Intervention and Statebuilding* 12 no. 1 (2018): 1–10. https://doi.org/10.1080/17502977.2018.1426384.

Lui, Dawn, and Alexandru Lazar. *Digitalization and SSG/R: Projections into the Future*. Geneva: DCAF – Geneva Centre for Security Sector Governance, 2023. https://www.dcaf.ch/sites/default/files/publications/documents/Digitalization-and-SSGR_Projections-Future_EN-2.pdf.

Lucas, George R., Jr., Dragan Lozancic, Grazvydas Jasutis, Frederic Laker, Kakhaber Kemoklidze, and Rebecca Mikova. *Conceptualizing the Relationship of Good Security Sector Governance to the State Security System*. Geneva: DCAF – Geneva Centre for Security

Sector Governance, 2022. https://www.dcaf.ch/sites/default/files/publications/documents/RelationshipGoodSecuritySectorGovernanceStateSecuritySystem_EN.pdf.

Organisation for Economic Co-operation and Development (OECD). *Recommendation of the Council on National Digital Security Strategies*. OECD Legal Instruments, OECD/LEGAL/0480. Paris: OECD, September 26, 2022. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480.

Organization for Security and Co-operation in Europe (OSCE). *Security Sector Governance and Reform: Guidelines for OSCE Staff*. Vienna: OSCE Secretariat, Conflict Prevention Centre, Operations Service, 2022. https://www.osce.org/files/f/documents/2/4/512470_0.pdf.

Sarjito, Aris, and Yin Chhao Rath. "Security Sector Reform and Implementation of Good Governance: A Theoretical Study." *Aplikasi Administrasi: Media Analisa Masalah Administrasi* 27 no. 2 (2024):82-96, https://doi.org/10.30649/aamama.v27i2.257.

Schroeder, Ursula C. and Fairlie Chappuis, “New Perspectives on Security Sector Reform: The Role of Local Agency and Domestic Politics,” *International Peacekeeping* 21, no. 2 (2014): 133–48, https://doi.org/10.1080/13533312.2014.910401.

Centar za sigurnosne studije - BIH

Centre for Security Studies - BH

BOSNA I HERCEGOVINA
71000 SARAJEVO
BRANILACA SARAJEVA 13/1

TEL:
+ 387 (0)33 262-456

info(at)css.ba

@CSSBIH

www.css.ba