DCAF Geneva Centre for Security Sector Governance

SSR BACKGROUNDER

DIGITALIZATION AND SECURITY SECTOR GOVERNANCE AND REFORM (SSG/R)

ABOUT THIS SSR BACKGROUNDER

This SSR Backgrounder discusses the impacts of digitalization on good governance of the security sector. As an emerging security challenge, digitalization and the digital processes associated with it are reshaping and reframing traditional ideas of good governance, while involving new emerging security actors within the security sector arena. This Backgrounder first explores digitalization and its associated processes and outlines why it is an emerging security challenge. Then it discusses how good SSG could enhance safety in the digital space and highlights the main challenges, opportunities, and prospects that digitalization poses to good SSG/R. Finally, it identifies specific security sector actors who play a significant role in contributing towards good SSG in the digital space.

THIS SSR BACKGROUNDER ANSWERS THE FOLLOWING QUESTIONS:

What is digitalization? . . . 2
Why is digitalization an emerging security challenge? . . . 2
Why is good SSG important for digitalization? . . . 3
What are the main challenges, opportunities, and prospects of digitalization in key areas of SSG/R? . . . 5
How can security sector actors contribute to good governance of the digital space? 5

ABOUT THIS SERIES

The SSR Backgrounders provide concise introductions to topics and concepts in good security sector governance (SSG) and security sector reform (SSR).
The series summarizes current debates, explains key terms and exposes central tensions based on a broad range of international experiences. The SSR Backgrounders do not promote specific models, policies or proposals for good governance or reform but do provide further resources that will allow readers to extend their knowledge on each topic.
The SSR Backgrounders are a resource for security governance and reform stakeholders seeking to understand and also to critically assess current approaches to good SSG and SSR.

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders.

DCAF wishes to thank
Dawn Lui, with assistance from Alexandru Lazar, for authorship;
Franziska Klopfer, Teodora Fuior, Ann Blomberg for their comments and review; David Wilson for copy editing; Petra Gurtner for layout and design.

Series Editor
Gabriela Manea

To cite this publication
DCAF – Geneva Centre for Security Sector Governance. Digitalization and Security Sector Governance and Reform (SSG/R).
SSR Backgrounder Series. Geneva:
DCAF, 2022.

DCAF
Geneva Centre for Security Sector Governance
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva
Switzerland

☎ +41 22 730 94 00
✉ info@dcaf.ch
@DCAF_Geneva

www.dcaf.ch

WHAT IS DIGITALIZATION?

Digitalization refers to technological processes, such as developments in digital communications and infrastructure, that affect all domains of public and private life. In other words, digitalization is the adoption or increased use of digital or computer technologies by states, organizations, or individuals. Digitalization is a highly contested field, with far-reaching and uncertain consequences for security. The digital revolution has led to an increase in availability of and access to information, empowering individuals and enlarging the democratic space. For instance, security services can reach marginalized individuals more easily due to digital technologies. However, this broader access to information also leads to an increase in disinformation, fake news, and propaganda campaigns, which undermine confidence in public authorities. Autocrats and autocracies, in particular, are known to use digital technologies to curb opposition and manipulate political narratives.

WHY IS DIGITALIZATION AN EMERGING SECURITY CHALLENGE?

While digitalization brings opportunities for more and better security provision and oversight, it can also be considered an 'emerging security challenge' (ESC). ESCs are novel threats that have not previously featured on the mainstream security agenda; they include threats relating to transnational security, as well as threats to human and societal security. ESCs were for several decades a contested concept, but have now penetrated global security thinking and practice as illustrated, for instance, by the parallel use of conventional and hybrid warfare in contemporary conflicts. ESCs are actions or events that put at risk both the material and normative basis of individuals, societies, and states. Such challenges are considered to be 'emerging' when the wider community of experts and policymakers frame them as security risks and security policy responses to counter them are then developed. First, the digitalization of the security sector has sparked debates on the individual and societal right to privacy versus states' obligations and duties to protect citizens. The integrity of the social contract between state and society is under pressure due to the infiltration of digital technologies in all domains of public and individual life. Second, new digital tools and virtual interfaces connected via the internet are at the same time creating a complex landscape of cyberthreats with a growing number of critical failure points. Cyberthreats are outpacing the abilities of many societies to effectively prevent and manage them. For example, cyber actors using ransomware are targeting public utilities, healthcare systems, and even non-governmental organizations (NGOs) delivering aid to vulnerable populations. These emerging actors range from hacktivists to cybercriminals and state-sponsored cyber groups. They target state representatives and human rights activists alike, leading to political tensions, governmental sanctions, and lawsuits.

The advent of new technological tools and actors radically challenges existing frameworks of good governance, including in the security sector. Security sector actors regularly find themselves navigating a world where technological developments outpace the implementation of regulatory mechanisms. This new security environment has outgrown its 'emergent' phase, posing lasting challenges to national security and to democracy, as well as to human rights and the civil liberties of individuals.

FIGURE 1 CONCEPTUAL CLARIFICATIONS

Digitalization vs digitization: Digitalization should not be confused with digitization. Digitization is the technical process of converting and storing text, pictures, and sounds in a digital format. It refers to the transition of data from an analogue to a digital format. Digitization is not within the scope of this Backgrounder.

Digital space: This is an overarching term that refers to the networks and devices used to share information between individuals, between institutions, and between individuals and institutions. It can also be conceived of as a social arena that is accessible through a virtual interface, allowing for interactions between users to access or share data. Unlike other spaces such as land, sea, or air, digital space is viewed as a new domain that extends beyond national borders (similar to outer space).

Cybersecurity: This is the practice of defending digital infrastructure and associated institutions against digital threats and seeking to guarantee safe use of the digital space by every actor involved. Any disruptions to these critical services could lead to devastating outcomes for the population and in the long run for a state's survival. Cybersecurity is a specific, narrow nexus between digitalization and the security sector.

WHY IS GOOD SSG IMPORTANT FOR DIGITALIZATION?

The dual nature of digitalization – as both an opportunity and a threat – is transforming the governance and provision of security services. This section outlines why and how the good governance principles and cross-cutting issues informing good SSG can help to better manage the negative impacts of digitalization on the security sector and on democratic governance.

For more information on the principles of good governance, please refer to the SSR Backgrounder on 'Security Sector Governance'.

Accountability for digital processes in the security sector presupposes external and internal oversight and control mechanisms implemented by independent authorities. As digitalization gives rise to new mechanisms for data management and new data processing techniques, it enables increased oversight of government actions by strengthening the traceability, storage, and retrieval of information. However, it is important to ensure that legislative developments keep pace with technological advances, so that there are clear guidelines on the use of digital tools by the security sector without any infringements upon the rights of individuals.

Transparent use of digital capabilities by the security sector means that information pertaining to security sector institutions is publicly available and accessible. Regulation of confidential information and of related privacy issues is key to preventing data breaches, while digital tools should be adopted to improve the availability, accessibility, processing, and security of information. Security actors need to be careful when collecting and processing data on individuals and ensure that adequate safeguards are in place.

Upholding the **rule of law** in the security sector means that all individuals and institutions, including the state, are subject to public and impartial laws consistent with international and national human rights norms and standards. Misuse of digital technologies can undermine free and fair elections, jeopardize freedom of expression, and limit access to reliable information. The rule of technology may threaten to replace the rule of law, creating conditions for digital authoritarianism whereby digital technologies are used to control or manipulate individuals at home or abroad. Fake news, false rumours, and hateful propaganda against marginalized groups can be used to drum up support for authoritarian interests and can also be instrumentalized as pretexts to enact restrictive media laws that target critics and human rights defenders.

Digitalization of security services means that more individuals can **participate** in the security sector and access services on an equitable and inclusive basis. Central and local administrations can implement online tools and mechanisms to support individuals at risk. Women, racial and linguistic minorities, youth, and individuals with low-paid jobs and poor education tend to have less access to democratic processes due to wide-ranging socioeconomic factors. Decision-makers will be required to bridge gaps in digital literacy, secure public structures from hacking, and protect citizens' privacy to ensure that disadvantaged groups can connect to such services.

Responsiveness in the digital space means that security sector institutions are sensitive to the different security needs of the population and perform their roles and responsibilities in the spirit of a culture of service. Security sector actors can use digital technologies to create complaints forms to obtain a better understanding of local grievances and needs. However, new digital initiatives of this nature should not replicate or exacerbate existing biases and exclusion or discrimination.

Effectiveness in the digital space means that security sector institutions have clearly defined human security objectives and policies and that they fulfil their respective roles, responsibilities, and missions to a high professional standard. It is crucial to attract, retain, and train qualified security sector personnel with sufficient digital skills to effectively engage in the evolving digital space. Digital tools will also be needed not only to integrate a greater variety of training and education methods, but also to target, identify, process, analyse, and solve problems more effectively.

Efficiency in the digital space means that security sector institutions conduct sound financial planning whereby security spending is based on agreed and realistic objectives that are prioritized and make the best possible use of public resources. For example, sharing of real-time information among intelligence and police officers across borders can address drug trafficking or terrorist attacks more efficiently and in a more cost-effective manner. Digital tools can also be used to ensure greater transparency on procurement and use of public funds by the security sector, as well as to process and store administrative data.

FIGURE 2 CHALLENGES, OPPORTUNITIES, AND PROSPECTS OF DIGITALIZATION IN SSG/R

Challenges	Opportunities	Prospects
Oversight and administrative processes		
• Technological developments occur more rapidly than legislative implementation. • Standards and regulations in the digital space are constantly evolving. • There is a lack of up-to-date, forward-looking oversight mechanisms that protect human rights in the evolving digital space.	• The security sector can adopt forward-looking processes to ensure that there are no gaps in the law. • The security sector can implement responsive regulatory frameworks and keep public and private sector actors up to date on any developments in the digital space. • Information can be retrieved more easily and stored more safely, thus preventing delays in inter-departmental cooperation.	• Algorithms might take over the function of reviewing how decisions are implemented. • Security leaders might be less in charge of personnel and more in control of digital processes. • Citizens might be able to access online platforms designed for them to submit security concerns and ask questions.
Capacities and resources of security sector institutions		
• There is limited transparency around the decisions made by different security sector actors to use public funds to acquire digital tools and questions as to whether these tools are fit for purpose in the evolving digital space. • Security sector actors and lawmakers are not up to date with technological developments in the digital space.	• The security sector can invest in digital tools and technologies to improve security provision by making it more accessible and targeted to the population it serves. • The security sector can adopt digital tools to process and analyse data more efficiently, remove human biases in data collection, and improve and standardize administrative and oversight processes.	• Routine tasks are likely to become more digitalized and require less human input, allowing experts to work on more complex tasks. • Security provision might be more responsive to the specific needs of different communities due to improved data analysis and access to information.
Skills and technical knowledge of security sector personnel		
• The security sector has limited digital skills and ability to engage in the evolving digital space. • The security sector is unable to attract and retain qualified personnel.	• The security sector can provide digital training for existing security personnel to increase capacities and attract potential employees. • The security sector can recruit digitally literate and qualified personnel to ensure that it does not lag behind the private sector.	• Digitalization of the security sector might result in a race to keep pace with novel technologies and attract qualified personnel. • The emergence of new security actors might result in operations conducted in the digital space.
Public participation and the digital divide		
• Issues with accessibility, language barriers, and limited infrastructure contribute to widening the digital divide. • Women, elderly people, marginalized communities, and those in rural areas are disproportionally affected. • Vulnerable and marginalized communities have less access to digital technologies.	• There can be a wider availability of information and improved methods of communication between the security sector and the population it serves. • New meeting technologies can encourage participation by those previously excluded due to costs and logistical challenges. • Digital tools can improve women's participation in economic life, with heightened potential to bypass traditional cultural and mobility barriers.	• Security actors might become more responsive to community needs due to the ability to organize online remote meetings that reduce costs and logistical needs. • Online platforms might increase public input into processes of decision-making and security provision. • Individuals are likely to have more opportunities to engage in online public discourse on decisions that affect them.
Human rights, information sharing, and privacy issues		
• Widespread sharing of data and information challenges the boundaries between the public and private spheres. • There is a high risk of security data breaches and leaking of confidential information. • There are increasing tensions between the protection of human rights and the encroachment of government surveillance, particularly in authoritarian contexts.	• Digital tools can provide civil society organizations and the public with channels to easily report human rights abuses by the security sector. • A balance will need to be struck between the accessibility of information and the need for secrecy, which requires the implementation of clear standards and guidelines concerning the use and availability of information.	• Human rights defenders, activists, and whistle-blowers might find themselves at risk of increased surveillance and tracking. • Digital tools will have to be paired with ethical oversight and strong regulations to make sure that they do not exacerbate social inequalities. • A balance will need to be reached between a state's responsibility to protect its citizens and the individual right to privacy.

Security sector actors must abide by **human rights** standards in the conduct of their activities in the digital space. Developments in information and communication technologies (ICTs) are providing greater access to information, facilitating global debates, and fostering enhanced democratic participation. Human rights defenders can more rapidly and thoroughly expose abuses. At the same time, however, human rights defenders can also be subjected to online threats, intimidation, and cyberbullying, which can quickly transition to real-world targeting, harassment, and violence. Furthermore, new technologies are vulnerable to electronic surveillance and interception, can threaten individual rights to privacy and to freedom of expression and association, and ultimately can restrict the free functioning of a vibrant civil society.

Gender equality in the digital space means that specific security and justice needs of women, men, boys, and girls are addressed in the provision, management, and oversight of security. Issues related to accessibility, affordability, and level of education, as well as inherent biases and sociocultural norms, often limit the ability of women and girls to benefit from the transition towards digitalization. The consistently low levels of participation by women and girls in science, technology, engineering, and mathematics (STEM) fields continues to contribute towards widening gaps. Nonetheless, digital technology can improve participation in economic life and facilitate access to healthcare services, as such tools can offer women the potential to bypass traditional cultural and mobility barriers. For LGBTQI+ persons, it has been recognized that social media, dating apps, virtual private networks (VPNs), and blockchain technology have all played a part in creating new safe spaces, providing them with more opportunities to connect and explore issues facing their communities.

WHAT ARE THE MAIN CHALLENGES, OPPORTUNITIES, AND PROSPECTS OF DIGITALIZATION IN KEY AREAS OF SSG/R?

Building upon the previous sections, Figure 2 presents the main challenges, opportunities, and prospects inherent in digitalization in five key areas essential to good SSG/R, namely oversight, resource availability, technical capacity, public participation, and human rights.

HOW CAN SECURITY SECTOR ACTORS CONTRIBUTE TO GOOD GOVERNANCE OF THE DIGITAL SPACE?

This section highlights the potential for new areas of engagement for both traditional and emerging security actors in ensuring good SSG/R in the digital space. Figure 3 presents key recommendations for how specific security actors can contribute to good governance of the digital space.

The legitimacy and effectiveness of the **armed forces** are dependent on their ability to fulfil their mission in an accountable manner within a framework of democratic civilian control, rule of law, and respect for human rights. In particular, the development and use of novel military technologies must be subject to strict scrutiny.

Due to their proximity to the population, actions and decision-making by **law enforcement agencies** directly affect the security of individuals and communities on a daily basis. The use of digital tools in policing has dramatically increased, with questionable consequences for the rights of individuals. Adherence to the principles of good SSG by law enforcement actors, particularly in the digital space, is essential as their actions have the potential to shape the democratic character of the state itself.

Executive and government ministries manage the administration, organization, and budget of the security forces and generally have the final say on security policies. Governments have embraced digital technologies in transformative ways, from setting measurable administrative goals and improving service delivery to making data-driven decisions and enacting evidence-based policies that ensure greater accountability and transparency of state services.

While **parliaments** are unique to each political and legal system, all share similar functions that make them central actors in every democracy. Parliaments use digital technologies to facilitate engagement with citizens in the decision-making process. The digital tools they use range from e-parliament platforms to management systems for documents. However, parliaments often face challenges in digitalizing their processes, particularly those in lower income contexts.

Civil society organizations (CSOs) are key to encouraging a culture of participation that enhances the democratic nature of decision-making on security issues. There are myriad ways in which CSOs have digitalized their activities, including the use of digital tools to work more efficiently across a wide spectrum of contexts and the delivery of critical digital services to vulnerable populations.

Big tech companies are viewed as ‘emerging security actors’ as they play an increasingly important role in facilitating access and participating in public discourse through the digital technologies they produce. Predominantly privately owned entities with distinct priorities, big tech companies are becoming more influential in national politics and international affairs.

FIGURE 3 RECOMMENDATIONS FOR SECURITY SECTOR ACTORS

	Security actor	Recommendations
SECURITY PROVIDERS	Armed forces	• Share information internally and externally to facilitate responses to cyberthreats. • Invest in the modernization of digital infrastructure and in digital capacities, for example by recruiting digitally literate personnel. • Employ digital tools to create gender-sensitive online complaints mechanisms for the public to raise concerns about actions, policies, and regulations. • Increase transparency by developing stronger procurement processes and mechanisms to identify human rights abuses.
	Law enforcement	• Ensure that the use of and access to personal data or sensitive information is properly regulated. • Form a transparent information and communication network to exchange information, analyse data, and make well-informed decisions. • Use digital technologies to streamline processes and to ensure accountable operational responses that respond to the different needs of every community. • Foster strong relationships with overseers in the implementation of new policies and legislation that reflect ongoing technological developments. • Increase online presence to prevent abuses and to increase public awareness of digital threats. • Develop gender-sensitive, anonymous online complaints mechanisms and create safe spaces for marginalized individuals and communities to raise their concerns.
SECURITY OVERSEERS	Executive and government ministries	• Set operational standards for the use of digital technologies by security actors and adopt stronger regulations on big tech companies. • Use digital tools to monitor and assess the performance of security providers and to report on any misconduct or other activities affecting the security of marginalized individuals. • Develop mechanisms to report and monitor hate speech, violent extremism, cyberbullying, and other forms of online harassment. • Create a gender-sensitive national cybersecurity policy and educate security personnel on the challenges posed by digital threats. • Create an inclusive and participatory digital public space, ensuring that communication reaches women, men, boys, and girls, as well as marginalized persons and those in vulnerable situations.
	Parliaments	• Ensure that there is a suitable legal framework governing the security sector in the digital space and that the use of digital tools is aligned with digital developments. • Organize gender-sensitive participatory and inclusive interactions with citizens through online platforms to answer queries and receive feedback during the consultation and law-making process. • Share voting records and oversight activities to strengthen accountability and transparency. • Approve and monitor budgets for security providers to acquire digital resources.
	Civil society organizations (CSOs)	• Collaborate with other CSOs to ensure that security providers respect data protection norms. • Use digital technologies to streamline complaints against public officials or security actors and to detect infringements of human rights. • Raise awareness of internet security and create mechanisms to denounce hate speech, violent extremism, cyberbullying, and other forms of online harassment. • Develop gender-sensitive digital toolkits and training materials to support activists and researchers.
EMERGING SECURITY ACTORS	Big tech companies	• Respect legislation and regulations put in place by governments and encourage better standards for the protection and exchange of private data. • Cooperate with governments, parliaments, and national and international security actors to define standards, regulations, and best practices in the digital space. • Work together with CSOs and national governments to provide these actors with resources and knowledge to prevent cyberattacks. • Develop gender-sensitive mechanisms that allow for the monitoring of content published on online platforms to prevent fake news or online harassment.

WHAT TO READ NEXT

- Sabrina Ellebrecht and Stefan Kaufmann
  Digitalization and Its Security Manifestations
  European Journal for Security Research (5), 2020.

- Cody Collum and Houssain Kettani
  On Security Implications of Emerging Technologies
  Association for Computing Machinery, 2022.

- Graeme P. Herd, Detlef Puhl, and Sean Costigan
  Emerging Security Challenges: Framing the Policy Context
  GCSP Policy Paper 5, 2013.

- Francesco Mancini (ed.)
  New Technology and the Prevention of Violence and Conflict
  New York: International Peace Institute, April 2013.

- DCAF Research Report
  SSG/R in the Digital Space: Projections into the Future
  Geneva, Switzerland. Forthcoming, 2023.

MORE DCAF RESOURCES

DCAF publishes a wide variety of tools, handbooks and guidance on all aspects of SSR and good SSG, available free-for-download at **www.dcaf.ch**
Many resources are also available in languages other than English.

DCAF Geneva Centre for Security Sector Governance

DCAF – Geneva Centre for Security Sector Governance

Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva
Switzerland

☎ +41 22 730 94 00
✉ info@dcaf.ch
@DCAF_Geneva

www.dcaf.ch