DCAF Geneva Centre for Security Sector Governance

DIGITALIZATION AND SSG/R: PROJECTIONS INTO THE FUTURE

About DCAF

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's Foundation Council members represent over 50 countries and the Canton of Geneva. Active in over 70 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality.

For more information visit www.dcaf.ch and follow us on Twitter @DCAF_Geneva.

DCAF – Geneva Centre for Security Sector Governance

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

Tel: +41 22 730 94 00

Email: info@dcaf.ch

Web: www.dcaf.ch

Twitter: @DCAF_Geneva

Contributors

Authors: Dawn Lui, Alexandru Lazar

Copy Editor: Dianne Battersby

Cover Design: Nicola Dotti

Photo: Unsplash.com / James Eades

First published in Switzerland in 2023 by DCAF – Geneva Centre for Security Sector Governance (DCAF Geneva, P.O. Box 1360, CH-1211 Geneva 1, Switzerland)

Cite as: Lui, Dawn and Lazar, Alexandru, Digitalization and SSG/R: Projections into the Future, (Geneva: DCAF 2023).

ISBN: 978-92-9222-718-0

Disclaimer

The opinions expressed in this publication are those of the group of experts and authors alone and do not necessarily reflect the position of the institutions referred to or represented within this publication.

Executive summary

Digital technologies have created a new arena for security sector actors to carry out their duties, leading to the emergence of a more complex security landscape consisting of a rising number of new actors and critical failure points. Digitalization is regarded as an emerging security challenge, as it has the potential to drastically reshape existing governance structures while prompting new patterns of coordination and cooperation within and across state security institutions. The digitalization of the security sector can be defined as the means of equipping institutions and actors with the digital skills, tools, and awareness necessary to facilitate the provision, management, and oversight of security in modern society. This study explores the transformative impact of digitalization on the security sector. New technologies require traditional security sector actors to adapt their approaches and acquire new technical capacities, while ensuring legislation keeps pace with the continuous technological developments, upholding and promoting human rights, and attempting to close the growing digital divide. The evolving digital landscape blurs the lines between traditional security domains and the digital space as emerging actors position themselves in this unclaimed arena of national security.

With three primary objectives, this research aims to shed light on the complex intersection of digitalization and security sector governance (SSG). First, it investigates the multifaceted challenges and opportunities digitalization presents for good SSG. Second, it scrutinizes how key security sector actors have adapted to the digital transition, as well as to the emergence of new players within the security ecosystem. Last, the study provides specific recommendations to effectively navigate the intricacies of digital technologies, recognizing the dual-use nature of these technologies and the critical role of security sector governance and reform (SSG/R) in shaping ethical technology use and robust digital governance frameworks. To achieve these objectives, the current research employs the Delphi method, which is a forecasting framework developed to achieve reliable consensus on complex problems. The method has been used to forecast trends and outcomes, particularly in the fields of science and technology. In the context of this research, the Delphi method is used to harness and organize insights and judgements from 15 different experts. The method is based on an iterative process consisting of three rounds of questionnaires that were sent in 2021 to a larger group of experts.

The study identifies digitalization as a multifaceted emerging security challenge, affecting the governance, provision, and oversight of security services. The research underscores the pivotal role of SSG/R in shaping fair technology utilization and reinforcing digital governance frameworks. It presents the consensus reached among the experts participating in the study in five central thematic areas, namely new technologies, technical capacity, regulation and oversight, human rights, and the digital divide. While new technologies offer tools for enhanced accountability and transparency in security provision, they demand an adequate level of human control and the development of technical proficiency for security sector personnel. Moreover, the need for agile regulations to ensure proper security oversight and human rights in the face of technological advancements becomes paramount and can contribute to addressing the growing digital divide. The study identifies both challenges and opportunities in the digitalization of the security sector. In this vein, while digitalization can exacerbate power imbalances and necessitate urgent regulatory adaptation, it also fosters improved record-keeping, communication, data analysis, and automation of tasks and processes. The research also highlights how key security actors, such as armed forces and law enforcement, have adapted to digitalization, each leveraging technology to enhance their operations and efficiency, from drones in reconnaissance to predictive policing algorithms, while actors such as big tech companies and cybercriminals play an increasing role in the security arena. Overall, the study reveals the evolving landscape of the security sector in the digital age, highlighting both the promise and complexities brought about by the digitalization process.

Based on the consensus reached among the experts, the study offers a set of three recommendations per thematic area. The recommendations are as follows:

New technologies:

- The security sector needs to ensure oversight of its spending on digital resources to ensure transparency and accountability in the allocation of resources for updating legacy systems.
- Security sector actors should adopt digital tools to improve traceability of processes, sharing of information, and record-keeping within the security sector, to ensure better responsiveness, effectiveness, and efficiency.

- New technologies, such as artificial intelligence (AI), need to be implemented with careful consideration of their ethical and legal implications. Security sector actors should ensure that human judgement remains a central component of decision-making to ensure the prevalence of rule of law.

Technical capacity:

- Prioritize and invest in the education and training of security sector personnel to enhance their technical capacities in digital technologies (including cybersecurity, AI, data analytics, digital forensics, and information management), while reinforcing the principles of good SSG.
- Security sector actors should actively seek out individuals with technical expertise and digital skills to meet the growing demand for such talent in the sector.
- Prioritize cooperation, information sharing, and collaboration both domestically and internationally. By working together and sharing best practices, security sector institutions can enhance the skills and knowledge of their personnel, develop innovative strategies, and improve overall security.

Regulation and oversight:

- Security sector actors should work in collaboration across the whole sector to ensure the creation of a stable legislative and regulatory environment that keeps pace with and governs the development and use of digital technologies within the security sector.
- Security sector institutions should proactively standardize oversight approaches and provide uniform, impartial reporting standards to ensure that the principles of good security governance are applied to the oversight of digital technologies.
- Establish strategic partnerships and cooperation with various stakeholders, including academic and research institutions, corporate entities, and technology experts, to ensure participation.

Human rights in the digital age:

- Security overseers should enact safeguards based on legal and ethical guidelines to ensure that security providers respect privacy rights when conducting any form of mass surveillance.
- Security sector actors should adopt a multistakeholder approach and collaborate with public organizations and the private sector to enhance the protection of human rights in order to avoid any form of digital authoritarianism.
- Security sector actors should strengthen legal frameworks, support independent journalism, promote digital literacy initiatives, ensure transparency and accountability within security institutions, and utilize emerging technology (such as AI) to protect human rights in the face of disinformation.

Digital divide:

- Security sector actors should collaborate with the public sector and big tech companies to create accessible public spaces where digital resources and courses are freely accessible, with a focus on empowering marginalized communities. Improving digital literacy can lead to better accountability, rule of law, and governance.
- Security sector actors should use online platforms and technologies to engage with citizens, ensure digital inclusion, and promote public participation in security provision and oversight to leverage greater transparency, accountability, and participation in the security sector.
- Security sector actors should develop a commonly agreed framework for closing the digital gender divide, while reinforcing gender mainstreaming and strengthening women's participation in law enforcement.

DCAF – Geneva Centre for Security Sector Governance is undertaking this study in recognition of the urgent need to support security sector actors in their digital transformation. DCAF's extensive experience reveals gaps in legislation and accountability mechanisms necessary to ensure the responsible use of digital technologies, safeguard democratic values, and protect human rights. The report provides a comprehensive review of relevant literature, details the research methodology, analyses five key thematic areas identified through the literature review and the insights shared by the experts, and concludes with findings, recommendations, and some avenues for future research.

Contents

List of abbreviations

AI	Artificial intelligence
CERT	Cyber emergency response teams
CSAT	Cyber Security Associates and Technologists
CSO	Civil society organizations
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Cybersecurity
GAO	Government Accountability Office
ICT	Information and communication technologies
IHL	International humanitarian law
ITU	International Telecommunication Union
LAWS	Lethal autonomous weapons systems
MoD	Ministry of Defence
MoI	Ministry of Interior
MOOC	Massive Open Online Courses
MR	Mixed reality
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSA	National Security Agency
SADA	Smart Africa Digital Academy
SOC	Security operation centre
SSG	Security sector governance
SSR	Security sector reform
STEM	Science, technology, engineering, and mathematics
UAV	Unmanned aerial vehicles
UNDP	United Nations Development Programme
VR	Virtual reality
WEP	Women's Empowerment Principles

Introduction

Background

Digital technologies have created a new arena for security sector actors to carry out their duties. Datafication, automation, surveillance technologies, AI, and machine learning – among other technical advancements – present huge opportunities for the security sector to create new ways to gather information, communicate, and make data-driven decisions. There is a shared understanding that digital technologies will reshape governance structures, while prompting new patterns of coordination and cooperation within and across state security institutions. As a result, the security sector is becoming increasingly aware of the importance of adopting and implementing robust digitalization processes. The security sector is composed of all the structures, institutions, and personnel responsible for security provision, management, and oversight at the international, national, and local levels. Thus, the digitalization of the security sector can be defined as the means of equipping institutions and actors with the digital skills, tools, and awareness necessary to facilitate the provision, management, and oversight of security in modern society.

However, the growing dependency of governments and societies on digital technologies is leading to the emergence of a more complex security landscape, with a rising number of actors and critical failure points, in which malicious digital actors have increasingly focused on targeting local, state, and federal governments.[1] Geopolitical tensions extend to the digital realm, with states or state-sponsored actors becoming possible sources of threat. Due to the linkages made by state actors between emergent technologies and power politics, digital applications have made their way into many security-related fields, such as the armed forces, intelligence services, police, and border control, to mention a few.[2] The risk of cyberattacks looms over the security sector, as these can compromise the integrity of digital systems and undermine security operations. For example, various cyberattacks, such as ransomware and Distributed Denial of Service (DDoS) attacks, have disrupted the operations of numerous governments across the world.[3] The possibility of digital incidents leading to damage in the physical world having a direct impact on the security of citizens is no longer theoretical. Thus, ensuring the security of digital systems and protecting sensitive data is of utmost importance.

The rate of technological innovation is largely outpacing the competence of the security sector and its ability to keep up with the latest developments and with their potential societal impacts. Security sector actors have systematically underestimated the possible disruption caused by novel technologies, despite international calls for an in-depth analysis of the effects of digitalization on national security.[4] Digital technologies are a product of our time. Relatively easy to access and use, most of them are inherently vulnerable to exploitation and disruption. Most digital technologies are considered to be dual-use, as they can be harnessed to both enhance national security or undermine it.

In addition, the digitalization of the security sector has increased the pressure to properly balance individual human rights, such as the freedom of expression or the right to privacy, with the obligation and duty of states to protect their citizens. Digitalization can then be regarded as an emerging security challenge, as it has the potential to drastically disrupt and change existing frameworks of good governance due to the emergence of new technological tools and actors, all engaging in the uncharted digital space. This new security landscape requires targeted research and policy guidance, as well as thorough discussions regarding the impact of digitalization on the security sector to identify what is required to ensure its good governance and reform (SSG/R) in the digital space.

---

[1] Wolff, A., 'Cyberattacks on Governments Skyrocketed in 2021', SonicWall Blog (28 March 2022).

[2] Hoadley, D. S. and N. J. Lucas, 'Artificial Intelligence and National Security' (Washington, D.C.: Congressional Research Service, 2018).

[3] 'Significant Cyber Incidents Since 2006' (Washington, D.C.: Center for Strategic & International Studies, 2022).

[4] Collum, C. and H. Kettani, 'On Security Implications of Emerging Technologies', *ICEDS '22: Proceedings of the 2022 3rd International Conference on Education Development and Studies*, (2022), pp. 28-31.

Scope and objectives

The purpose of this research study is to assess the overarching impact of digitalization on the security sector. To achieve this aim, the current study has set out three objectives.

First, this research aims to *identify the main challenges and opportunities posed by digitalization to good security sector governance (SSG)*. In this context, good SSG describes how the principles of good governance apply to security provision, management, and oversight by state and non-state actors. The principles of good governance are accountability, transparency, rule of law, effectiveness, efficiency, responsiveness, and participation.[5] To achieve this objective, the current study will analyse five specific thematic areas identified through the review of the available literature on digitalization. These thematic areas are part of the wider digitalization process, ranging from new technologies, the need for technical capacity, strong regulations, the implications of digital technologies for human rights, and the widening digital divide.

Second, by exploring the thematic areas outlined above, the study aims to *illustrate the extent to which key security providers and overseers have adapted to the transition towards the increasing digitalization of their work, and how this adaptation has created spaces for the emergence of new actors*. The security sector includes actors who use force (security providers such as the armed forces, police, border guards, and intelligence services) as well as those responsible for controlling, through management and oversight, how force is used (security overseers, such as government ministries, parliament, and civil society, among others). This second objective aims to highlight the security sector reform (SSR) dimension of the current study.

The third and final objective of this study is to *provide specific recommendations for policymakers to adapt to the challenges and opportunities posed by emerging digital technologies*. As digitalization is a multilayered security challenge that – through its dual nature – can affect the governance, provision, and oversight of security services, SSG/R has a key role to play in defining the fair use of new technologies and in exploring how to strengthen digital governance frameworks.

Why is DCAF undertaking this study?

Over the past five years, the digitalization of the security sector has been a central focus in the work of DCAF – Geneva Centre for Security Sector Governance. For example, DCAF has provided operational support on the ground to a wide range of security sector actors, such as Ministries of Interior (MoI) and Ministries of Defence (MoD) in the Western Balkans, to ensure that, as they commence their digitalization process, they have the appropriate security mechanisms in place to protect their digital workflows.[6] In this context, DCAF's prior experience in this field highlights that legislation and accountability mechanisms related to these new technologies are largely underdeveloped. Such mechanisms will be vital if digital technologies are to serve people in a sustainable way based on democratic control, the rule of law, and respect for human rights. Through this research study, DCAF aims to build consensus on the impact of digitalization on the security sector and to strengthen the capacity of its actors to respect the fundamental principles of good governance in the use of digital technologies, as enshrined in the policies of the United Nations, the European Union, and the African Union. Therefore, DCAF is undertaking this study to contribute to the growing debate surrounding the use of digital technologies in the security sector and to fill the gap in the rather limited literature dealing with this topic.

Methodological considerations

The Delphi method has been used as the primary research method for this study. It is a forecasting framework developed by the RAND Corporation in the 1960s to achieve reliable consensus on complex problems. Since then, the Delphi method has been used to forecast trends and outcomes, particularly in the fields of science and technology. More specifically, this research method is used to harness and organize judgements on complex issues that require intuitive interpretation of informed opinions. The method is based on an iterative process consisting of several rounds of questionnaires that are sent to a larger group of experts with the aim of reaching a

[5] 'Security Sector Governance', SSR Backgrounder Series (Geneva: DCAF, 2015). Available here.

[6] 'National Cybersecurity Strategies in Western Balkan Economies' (Geneva: DCAF, 2021).

consensus. In the ‘Methodology’ chapter, we will further elaborate on the specific use of the Delphi method in this study.

Structure of the report

The following chapter will provide a comprehensive review of the literature on digitalization and SSG/R. Then, the report continues by providing an overview of the main research method employed in this study – the Delphi method – and the overall research design, before heading into the Analysis chapter. The Analysis chapter is divided into the five key thematic areas: (1) new technologies, (2) technical capacity, (3) regulation, (3) human rights, and (5) digital divide. These thematic areas were identified through both the literature review and the consensus reached by the experts participating in this study. The final chapter summarizes the findings of this study and provides key recommendations, as well as some suggestions for future research.

Review of literature on digitalization and SSG/R

This chapter will provide an overview of the existing literature on the nexus between digitalization and SSG/R in order to situate our present study in the broader landscape.

The digital revolution has profoundly transformed society.[7] Recent crises in the field of international security – such as the COVID-19 pandemic or the war in Ukraine – have demonstrated that digitalization is part of a complex constellation of socio-technological phenomena that are the subject of intense debate among scholars, practitioners, and policymakers alike, with consequences in real life.[8] The first contemporary use of the term 'digitalization' appeared in a 1971 essay exploring the objections to and the potential of computer-assisted humanities research.[9] From there, research on digitalization has developed into a vast body of academic literature, which is less concerned with the specific process of converting analogue data into digital information and focusing instead on the ways in which digital technologies structure, shape, and influence all aspects of the contemporary world. After scoping the literature available, the research team has identified a considerable gap in the scholarship assessing digitalization in the context of national security or SSG/R.

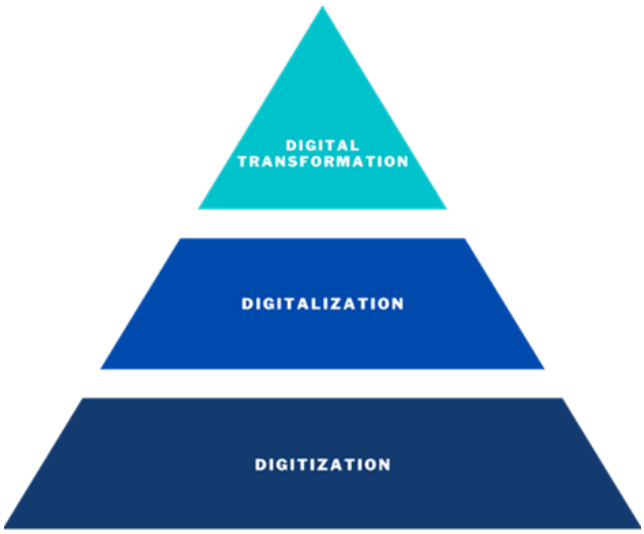


Figure 1. The Triangle of Digital Processes

Few articles distinguish between the concepts of *digitization*, *digitalization*, and *digital transformation*. In general, there appears to be significant confusion regarding the usage of these terms.[10] Digitalization should not be confused with digitization or with the broader process of digital transformation. As illustrated in Figure 1, digitization can be regarded as a first step into the digitalization of operational processes, representing the technical process of converting analogue data into a digital format.[11] Digital transformation, a term originating in the private sector, is the final step generally associated with the profound transformation of skills and business

[7] Kavanagh, C., 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?' (Washington, D.C.: Carnegie Endowment for International Peace, 2019).

[8] Ellebrecht, S. and S. Kaufmann, 'Digitalization and Its Security Manifestations', *European Journal for Security Research*, Vol. 5, (2020), pp. 1-3.

[9] Brennen, S. and D. Kreiss, 'Digitalization & Digitization', in *International Encyclopedia of Communication Theory and Philosophy* (London: Wiley-Blackwell, 2014).

[10] Reis, J., M. Amorim, N. Melao, Y. Cohen, and M. Rodrigues (2020), 'Digitalization: A Literature Review and Research Agenda', in Anisic, Z. et al. (eds.), *IJCIEOM* 2019, (Springer), pp. 443-56.

[11] Bloomberg, J. 'Digitization, Digitalization, and Digital Transformation: Confuse Them At Your Peril', *Forbes* (29 April 2018).

models by employing new technological means that produce added value enabling companies to remain competitive in the modern digital economy.[12]

Scholars argue that much of the literature on digitalization seems rather abstract as to the exact definition of the concept.[13] Only a few articles providing a conceptual definition of digitalization were identified. For example, Clerck defines digitalization as 'the use of digital technologies and of data to create revenue and improve business, whereby digital information is at the core'.[14] At the same time, Gobble's definition states that 'digitalization is composed of digital technologies and digitized information to create and harvest value in new ways'.[15] However, neither of these scholars consider the social or political dimension of digitalization. Srai and Lorentz move away from Clerck and Gobble's business-centric definitions by acknowledging and including the impact of digitalization on the different domains of social life.[16] Ringenson et al. support the definition provided by Srai and Lorentz and even go a step further by highlighting the differences between the technological conditions necessary for digitally related social change to occur.[17] As such, in the context of this study, digitalization can be defined as *the way in which areas of social life are being restructured around digital infrastructures, primarily by leveraging the use of new technologies to enable or improve operational processes* (by an organization, an industry, or a state).

In addition to these conceptual deliberations, scholars have engaged in various debates to discuss how digitalization is shaping contemporary societies. Many see digitalization as the main feature of the contemporary era or as the single communication infrastructure that connects all economic activities of a modern state.[18] For example, the digitalization of the world economy has led to the erosion of national sovereignty by reshaping concepts of materiality and physical space and facilitating new flows of culture, capital, goods, human resources, and capacities.[19] The *digital revolution* has created new professional roles (such as software engineers or social media account managers), new types of organizations (cloud computing providers and social media agencies), new economic sectors (e-commerce and data science), and even new domains of national security (cybersecurity).

Over the last decade, several scholars have argued that radical changes in the production of culture and knowledge have been observed thanks to the emergence of *digital platforms*, such as Facebook, X (formerly known as Twitter), or Wikipedia, to name a few. More specifically, new forms of non-proprietary knowledge production have emerged, changing who is empowered to create knowledge in contemporary societies.[20] For example, thanks to the falling costs of the production and distribution of digital information, individuals and organizations can access and disseminate everything from short videos shot on smartphones in remote parts of the world to political commentaries on specialized blogs. Benkler adds that new technologies are taking organizations into an era of transformation that is challenging traditional methods of information creation.[21] However, other scholars see this as a threat to the concept of truth and its validity, in a world where everyone can produce their own version of the truth, warning against disinformation and the negative impact this development

---

[12] Reis, J., M. Amorim, N. Melão, and P. Matos, 'Digital Transformation: A Literature Review and Guidelines for Future Research', in: Rocha, Á., Adeli, H., Reis, L.P., Costanzo, S. (eds.) *Trends and Advances in Information Systems and Technologies* (WorldCIST, AICS, 2018), Vol. 745, pp. 411-21.

[13] Reis, J., M. Amorim, N. Melao, Y. Cohen, and M. Rodrigues (2020), 'Digitalization: A Literature Review and Research Agenda', in Anisic, Z. et al. (eds.), *IJCIEOM* 2019, (Cham: Springer), pp. 443-56.

[14] Clerck, J., 'Digitization, digitalization, digital and transformation: the differences', *i-SCOOP* (2017).

[15] Gobble, M., 'Digitalization, Digitization, and Innovation', *Res. Technol. Manag*., Vol. 61: No. 4 (2018), pp. 56-9.

[16] Srai, J., and H. Lorentz, 'Developing Design Principles for the Digitalisation of Purchasing and Supply Management', *J. Purch. Supply Manag*., Vol. 25: No. 1 (2019), pp. 78-98.

[17] Ringenson, T., et al., Digitalization and Environmental Aims in Municipalities, *Sustainability,* Vol. 10: No. 4 (2018), pp. 1-16.

[18] Castells, M., *The Rise of the Network Society* (London: Wiley-Blackwell, 2010).

[19] Sassen, S., *Globalization and Its Discontents: Essays on the New Mobility of People and Money* (New York: New Press, 1998).

[20] Benkler, Y., *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven: Yale University Press, 2006).

[21] Ibid.

might have on human rights.[22] Van Dijk warns that while increased access to digital information allows state institutions to reach more people, it also fosters a situation where citizens are constant victims of 'information pollution'.[23] Information pollution can be defined as disinformation, fake news, and propaganda campaigns that aim to destabilize confidence in government and security institutions.[24]

Researchers have also traced the effects of digitalization on the contemporary processes of political participation and collective action. Bimber, Flanagin, and Stohl have detailed how civic engagement evolves in an information environment defined by digitalization. These scholars argue that citizens have radically different expectations and a much greater capacity to shape their own participation in society through new technologies.[25] Other scholars have looked at how digital technologies have facilitated leaderless and decentralized forms of collective action.[26] In this case, Sassen argues that digital media have enabled new forms of cross-border politics, expanded the political arena, and provided more opportunities to link local struggles to global networks defending the same cause.[27] At the same time, Marelli argues that digitalization and new technologies are playing an increasingly important role in today's humanitarian activities.[28] Contemporary humanitarian crises are increasingly fragmented, making it more complicated for humanitarian organizations to reach affected areas and vulnerable populations. Thus, to improve crisis response and operational efficiency, humanitarian organizations have adopted new digital tools and channels to deliver humanitarian assistance. However, as humanitarian organizations become increasingly reliant on digital technologies, they move from being mere bystanders to fully fledged actors in cyberspace, and therefore become susceptible to any malicious actions that would have an impact on their operational capacity to protect and assist vulnerable individuals, pointing towards the poor technical capacity of some of these actors.

Furthermore, scholars point out that the competition between states to own and control new technologies highlights the importance of digitalization for state and security institutions in their quest to affirm their digital power.[29] Digital power can be defined as the ability of any actor to exploit digital data to influence the behaviour of other entities in the international arena to achieve its own ends. Power in the digital space is asymmetrical and requires the ability to create a sustainable virtual ecosystem that can control data, networks, and information.[30] The asymmetric spread of digital power might lead to a deepening digital divide. In this context, the digital space is a general term that includes the networks and devices used to share information between individuals and institutions. It can be understood as a social arena accessible only through a virtual interface that allows its users to share, access, and disseminate data. Unlike other spaces, such as land, sea, or air, digital space is viewed as a new domain that extends beyond national borders (such as outer space).

However, despite the growing interest and attention given to the various manifestations of digitalization in contemporary societies, very few scholars have analysed the *impact of digitalization in the context of national security or security sector governance*. According to Reis et al., there is currently a large knowledge deficit at the state level, which accounts for only one per cent of world research on digitalization.[31] Among the one per cent of

---

[22] Brennen, S. and D. Kreiss, 'Digitalization & Digitization', in *International Encyclopedia of Communication Theory and Philosophy* (London: Wiley-Blackwell, 2014).

[23] Van Dijk, J., *The Network Society: Social Aspects of New Media* (London: Sage, 2005).

[24] Ibid.

[25] Bimber, B., A. J. Flanagin, and C. Stohl, *Collective Action in Organizations: Interaction and Engagement in an Era of Technological Change* (New York: Cambridge University Press, 2012).

[26] Bennett, W. L. and A. Segerberg, *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics* (Cambridge: Cambridge University Press, 2013).

[27] Sassen, S., *Globalization and Its Discontents: Essays on the New Mobility of People and Money* (New York: New Press, 1998).

[28] Marelli, M., 'Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation', *International Review of the Red Cross*, Vol. 102: No. 913 (2020), pp. 367-87.

[29] Fiott, D., 'Digitalising Defence: Protecting Europe in the Age of Quantum Computing and the Cloud', Brief No. 4, European Union Institute for Security Studies. (2020)

[30] Noel, J. C., 'What is Digital Power?', French Institute of International Relations (2019).

[31] Reis, J., M. Amorim, N. Melao, Y. Cohen, and M. Rodrigues (2020), 'Digitalization: A Literature Review and Research Agenda' in Anisic, Z. et al. (eds.), IJCIEOM 2019, (Cham: Springer) pp. 443-56.

scholars who have analysed digitalization at the governmental level, many have suggested that the infrastructure of the state is evolving rapidly under the influence of new digital technologies, resulting in vast changes in the logistics, structure, and even the credibility of state institutions.[32] Kavanagh argues that, with growing geopolitical tensions around the world, most states are increasingly viewing digital technologies as a central element to national security.[33] Similarly, Collum and Kettani state that, as digitalization gradually becomes a priority for governments around the world, it is important to note the constantly changing digital threat landscape, and emerging actors, while ensuring legislation is in place.[34]

In the context of *national security*, Ellebrecht and Kaufmann argue that digitalization empowers law enforcement agencies and rescue services to act and decide based on more information (big data analysis), while at the same time allowing for better surveillance, control, and protection of security personnel through datafication, automated processes, and electronic mediatization.[35] Digitalization has changed the way citizens and security institutions communicate and interact. It has reconfigured the relationship between proximity and distance, as well as between response time and action. Equipped with digital technologies, security sector actors no longer need a physical presence and can both access and share more information in a timely manner.[36] *Data* is generated daily by individuals, institutions, and other entities, and collected for a multitude of reasons. Data can be defined as the material produced by the abstraction of the world into categories, measures, and other representational forms that constitute the basic elements from which information and knowledge are created.[37] In this context, to 'datafy' a phenomenon consists of putting it into a quantified form so that it can be processed on a large scale via forms of analysis that can be automated.[38] Furthermore, *automated systems* perform clear and well-defined tasks.[39] These are processed successively by machines in structured sequences. However, automated processes should not be confused with *autonomous processes*. The latter are different in that they are based on various forms of deep-learning technologies, which are less predictable than automated processes.

These autonomous processes – such as AI – can greatly expand the capabilities of digital systems. Such processes are particularly common when rapid decisions have to be made in complex situations.[40] AI may be broadly defined as a branch of computer science that investigates and develops computational approaches and techniques which allow machines to perform tasks that would normally require some level of human intelligence.[41] Due to the linkages made by state actors between emergent technologies and power politics, AI applications have made their way into many security-related fields.[42] Although certain military organizations showed interest in AI during the Cold War,[43] a broader linkage between AI and the security sector emerged only after the publication of

---

[32] World Economic Forum, 'Understanding the Impact of Digitalization on Society' (2022). Available at: https://reports.weforum.org/digital-transformation/understanding-the-impact-of-digitalization-on-society/

[33] Kavanagh, C. 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?' (Washington, D.C.: Carnegie Endowment for International Peace, 2019).

[34] Collum, C. and H. Kettani, 'On Security Implications of Emerging Technologies' (Association for Computing Machinery, 2022).

[35] Ellebrecht, S. and S. Kaufmann, 'Digitalization and Its Security Manifestations', *European Journal for Security Research*, Vol. 5, (2020), pp. 1-3.

[36] Ibid.

[37] Kitchin, R., *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences* (London: Sage, 2014).

[38] Mayer-Schönberger, V., and K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (London: John Murray, 2013).

[39] Ellebrecht, S. and S. Kaufmann, 'Digitalization and Its Security Manifestations', *European Journal for Security Research*, Vol. 5, (2020), pp. 1-3.

[40] Collum, C. and H. Kettani, 'On Security Implications of Emerging Technologies' (Association for Computing Machinery, 2022).

[41] Coole, M., D. Evans, and J. Medbury, 'Artificial Intelligence in Security: Opportunities and Implications', ASIS Foundation Digital Transformation Series (2021).

[42] Hoadley, D. S. and N. J. Lucas, 'Artificial Intelligence and National Security' (Washington, D.C.: Congressional Research Service, 2018).

[43] Geist, E. and A. J. Lohn, 'How Might Artificial Intelligence Affect the Risk of Nuclear War?', *RAND Corporation* (2018).

three reports by the US government in 2016.[44] These reports highlighted the wide-ranging potential of AI across security domains and subsequently motivated many governments across the world to develop their own AI capabilities, leading more than 30 states to develop national strategies on this topic.[45]

New technologies can use AI algorithms to carry out a number of tasks, such as the identification of patterns and signals (e.g. the acoustic signals created by gunshots); to detect anomalies in patterns of behaviour (e.g. behavioural analysis in surveillance systems); to classify and match images (e.g. using computer vision to differentiate between a person or an animal); or to detect and identify images or materials (e.g. contraband or compounds in X-ray scanners).[46] The use of AI can provide significant benefits for operational security, such as increasing the probability and speed of detection, reducing operator workload and fatigue, as well as helping to focus the attention of security personnel on where it is most needed. At a governance level, AI may reduce costs, direct the allocation of resources, support decision-making, and even present early-intervention opportunities to mitigate insider threats. Within this context, it is undeniable that there is a high potential for AI to improve the quality of services provided by the security sector. However, AI can intensify data and power asymmetries, while penalizing citizens in vulnerable situations – even though AI can enable better data collection and help generate knowledge and solutions by applying advanced predictive analysis, it tends to be invasive and can often further intensify social prejudices and biases.[47] Predictive algorithms are, in fact, prone to error, with many examples of harmful use leading to the creation of paradoxes in control systems and increasing the danger of mass surveillance, even in democratic countries.

As such, even though the literature dealing with the impact of digitalization on the security sector is rather scarce, the research team has identified five recurrent thematic areas that are often discussed by scholars in their analyses. *New technologies*, such as AI, machine learning, and data analytics, present both opportunities and challenges that have not yet been discovered or addressed. Technological innovations have enhanced the ability of states and commercial security sector actors to monitor, decrypt, collect, analyse, and share data on a massive scale. Ensuring the security of new technologies is paramount to reinforcing their reliability, accessibility, and practicality in the security sector.[48] Considering the constantly evolving digital security landscape, security sector actors need to receive adequate training to ensure they are equipped with the *technical capacity* necessary to adequately use digital tools and to defend themselves from digital threats.[49] The very pace of technological change itself fundamentally challenges the ability of state institutions to provide *regulation and oversight* on new technologies, leaving legal lacunae that render the management of digital tools more difficult when used for security provision.[50] Scholars argue that the digitalization of the security sector has increased the pressure on *human rights* protections, having an impact on the dynamic between individual and societal freedom of expression on the one hand, and the obligation and duties of states to protect its citizens on the other, potentially undermining citizens' right to privacy, while further widening the *digital divide* that is reinforcing social differences and grievances.[51] The five themes identified through the existing literature equip the current study with the analytical framework required to assess the impact of digitalization on the security sector. This analytical framework is validated by the preliminary analysis conducted by the research team on the insights provided by the experts.

Thus, the use of digital technologies in the security sector is both an opportunity and a challenge. SSG/R has a key role to play in defining the fair use of new technologies, and in exploring the ways to strengthen digital

---

[44] Fischer, S. C. and A. Wenger, 'Artificial Intelligence, Forward-Looking Governance and the Future of Security, *Swiss Political Science Review*, Vol. 27: No. 1 (2021), pp. 170-79. Available at: https://onlinelibrary.wiley.com/doi/10.1111/spsr.12439

[45] Stanford AI Index, 'AI Policy and National Strategies', Chapter 7, Artificial Intelligence Index Report 2021.

[46] Coole, M., D. Evans, and J. Medbury, 'Artificial Intelligence in Security: Opportunities and Implications', ASIS Foundation Digital Transformation Series (2021).

[47] Misuraca, G., 'The Governance "Of, With and By" AI: Unveiling the Future of AI Government', *Medium* (2023).

[48] Collum, C. and H. Kettani, 'On Security Implications of Emerging Technologies' (Association for Computing Machinery, 2022).

[49] Kavanagh, C. 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?' (Washington, D.C.: Carnegie Endowment for International Peace, 2019).

[50] Ibid.

[51] Graeme, P. H., P. Detlef, and S. Costigan, 'Emerging Security Challenges: Framing the Policy Context', GCSP Policy Paper 2013/5 (2013).

governance frameworks for the security sector and beyond. More precisely, one of the key roles of SSG/R in digitalization is to ensure that the use of digital technologies aligns with the principles of good governance and international human rights standards. This requires establishing policies and regulations that promote responsible and ethical use of digital technologies and safeguard against abuse or misuse. Consequently, the relevance of the current research stems from the need to develop, through the five different themes identified in the literature, a shared understanding of how digitalization will reshape existing good SSG frameworks and reform practices based on the consensus reached by the external experts participating in this study. This study will contribute to enriching the debates and limited literature by exploring and assessing the impact of digitalization on the security sector.

Methodology: Using the Delphi method to reach consensus

What is the Delphi method?

The Delphi method is a forecasting process framework developed by the RAND Corporation in the 1960s to obtain reliable consensus on complex problems.[52] Since then, the Delphi method has been used to forecast trends and outcomes, particularly in the fields of science and technology, for harnessing and organizing judgement on issues that are highly complex and require intuitive interpretation of informed opinions.[53] This method is based on an iterative process comprising several sequential questionnaire rounds that are sent to a larger group of experts. For the current Delphi study, three rounds of questionnaires were created. The Round 1 questionnaire usually *explores the subject matter and collects a broad range of insights and opinions from the experts involved*. In this round, each expert contributes with information that is pertinent to the issue under discussion, based on their experience. The Round 2 questionnaire summarizes the answers given in the first round and *proposes statements* to respondents to capture their stances. This second questionnaire is less rich in qualitative input and starts moving towards identifying a measurable consensus. The Round 3 questionnaire, which acts as a *final evaluation*, occurs when all previously gathered information has been transformed into recommendations and the experts are about to confirm their consensus.[54] This report is the culmination of DCAF's Delphi study on digitalization and SSG/R. Integrated into this report are results that have been extracted from each of the three questionnaire rounds. The draft reports of Rounds 1, 2, and 3 are on file with DCAF and available upon request.

What are the advantages and disadvantages of using the Delphi method for policy research?

One of the primary advantages of using the Delphi method for policy research is its *ability to explore issues that require judgement*. Judgement is the ability to combine relevant knowledge and experience to form opinions. In this context, the Round 1 questionnaire aimed to comprehend the experts' views on the principles of good SSG in relation to digitalization by proposing questions that rely on the knowledge and experience of the experts. However, a disadvantage of the Delphi method is that the overall process requires a considerable amount of time to implement alongside commitment from the experts. For example, the Round 1 questionnaire encountered some unexpected delays that had a further impact on the creation of the Round 2 questionnaire and on the interim summary report. However, the delays did not have an impact on the Round 3 questionnaire nor require a major change in the study's original timeline.

A second advantage of using the Delphi method for policy research is that *the anonymous nature of the questionnaire rounds reduces the impact of dominant individuals and peer pressure*. In this manner, responses are weighted equally, so no expert can shift the opinions of the group to match their views. The Delphi study also allows experts to provide controlled feedback on the 'group opinion' through each questionnaire round, particularly in the Round 2 questionnaire, thus allowing the research team to reconsider certain issues. Even though experts can adjust their answers based on how they interpret the 'group opinion', the Delphi method does not explicitly allow participants to discuss the findings and there is no opportunity for the experts to elaborate on their views. Differing opinions will not be sufficiently investigated, and the facilitators' views might dominate the analysis in some instances. In parallel, the existence of a consensus does not necessarily mean that the correct answer, opinion, or judgement has been found. As such, the Delphi method helps to merely identify areas that the group of experts consider important in relation to that topic.

Nevertheless, another advantage of the Delphi method is its *ability to enable the researcher to overcome spatial borders and to have access to a wide range of experts*. Using the Delphi method allows for the input of various experts who are spatially separated, and to ensure a greater and inclusive participation.[55] The questionnaires created for this Delphi study were placed online to reduce communication delays and other logistical burdens both

[52] Gordon, T. J., 'The Delphi Method', The Millennium Project, Futures Research Methodology (1994), pp. 1-29.

[53] Mitchell, V. W., 'Using Delphi to Forecast in New Technology Industries', *Marketing Intelligence and Planning*, Vol.10: No. 2 (1992).

[54] Linstone, H. and M. Turoff, *The Delphi Method* (Boston: Adison Wesley Publishing Co.,1975).

[55] Dalkey, N., and O. Helmer, 'An Experimental Application of the Delphi Method to the Use of Experts', *Management Science*, Vol. 9 (1963), pp. 458-67.

for the research team and the experts.[56] This approach is a valuable method whereby researchers and policymakers are able to identify common issues of concern and arrive at a consensus on how best to approach the future as predicted by a diverse group of experts.

Why was the Delphi method chosen for this project?

The Delphi method was chosen for three key reasons. *First*, using the Delphi method allowed the facilitators of this study to identify common issues of concern about the impact of digitalization on SSG/R based on the experts' consensus. This led to practical recommendations, contributing to international policy discourse on digitalization and SSG/R for a multitude of actors, such as national security sector actors, international actors supporting SSG/R processes (e.g., UN, OSCE, EU), and national actors supporting SSG/R efforts (e.g., donors, developmental actors). *Second*, as data is lacking on the impact, challenges, and opportunities of digitalization on the security sector, as well as on the role of good SSG in the digital space, the Delphi method provided an efficient and relatively timely approach to gather large amounts of informed opinions and judgements that were easy to administer and analyse. And *third*, due to the project's tight timeframe and the pandemic context that was still ongoing at the time this research was carried out, travel and face-to-face meetings were not feasible. Using the Delphi method allowed the facilitators to design questionnaire rounds that could be posted online. This allowed for the participation of a more diverse group of experts, who otherwise would be too geographically separated to meaningfully participate in the study.

Selection of experts

In total, the project team at DCAF reached out to 25 experts in early September 2021 based on their expertise, region, and gender. Experts from all over the world were contacted for this study. Of the 25 experts approached, 18 agreed to participate, 3 declined, and 4 did not respond.

Figure 2. Geographical Distribution of Experts

In mid-September 2021, the first questionnaire was sent out to the 18 experts, with a 10-day timeframe for completion of the questionnaire and return of the signed contracts. Given the project's time constraints, Round 1 had to proceed with the submissions of 16 experts, that is, without the responses of 2 experts who had agreed to participate. The experts participating in the study consisted of 50 per cent practitioners from the security sector (i.e. security providers and overseers) and 50 per cent experts from academia and think tanks. One expert did not complete Rounds 2 and 3, resulting in a total of 15 experts who fully completed the Delphi study. In terms of gender balance, the team reached out to 8 female experts and 17 male experts.

The responses provided by the experts were anonymised during each round. As such, the research team has coded these answers by associating them with specific rounds and responses based on the submission timestamps, ensuring a structured and chronological coding system (e.g., Round 1, Response 3).

[56] Gordon, T. J., 'The Delphi Method', The Millennium Project, Futures Research Methodology (1994), pp. 1-29.

Analysis

This chapter aims to illustrate the consensus reached by the 15 experts participating in this Delphi study regarding the primary challenges and opportunities posed by digitalization to good SSG/R.[57] To achieve this goal, this chapter will synthesize and analyse the answers provided by the experts, structuring them around five thematic areas. These five thematic areas were initially identified through the literature review. As a result, these thematic areas collectively contribute to shaping the consensus and understanding of the implications of digitalization on SSG/R principles, as perceived by the experts involved in this Delphi study. It is important to reiterate that the quotes included in the analysis below are anonymised.

Based on a comprehensive analysis of the experts' converging viewpoints, each thematic section will focus specifically on one specific area of how digitalization is affecting security provision and oversight. The first thematic area assesses the practicality, functionality, efficiency, and impact of new technologies on the security sector. The second thematic area moves on to analyse the technical capacity of security sector actors to utilize novel technologies, providing insights into their adaptation to increasing digitalization and the emergence of new actors in the security field. The third thematic area explores the disparity between the ability of security sector actors to adopt legislation and ensure oversight that keeps pace with technological advancements. The fourth thematic area examines the human rights implications of the security sector's digitalization process. The fifth and final thematic area focuses on the digital divide in our societies and explores how the security sector can address this gap through digitalization.

Thematic area 1: New technologies

The security sector is on the brink of the next phase of the digital revolution, driven by advanced automation enabled through AI, machine learning, robotics, and other new technologies such as quantum computing. Security sector actors are under growing pressure to provide, develop, and explore new digital tools to deliver adequate security to the communities they serve. Concrete examples of the digitalization of the security sector can be observed in various areas. For instance, law enforcement agencies are increasingly utilizing AI-powered facial recognition systems to identify and track suspects, improving their capabilities in investigations and maintaining public safety. Additionally, machine learning algorithms are employed to analyse large volumes of data from diverse sources to identify patterns and potential threats, aiding in intelligence gathering and counterterrorism efforts. Another example is the use of robotics in bomb disposal units, where specialized machines are deployed to handle explosive devices, minimizing risks to human personnel.

All these new technologies are key elements of the wider process of digitalization and have wide-ranging impacts on good governance of the security sector. This is particularly the case for the increasing prevalence of autonomous processes, where machines using AI applications are performing tasks with minimal or no human assistance or supervision. Uses can range from virtual assistants in everyday life to precision targeting by the military in armed conflict. Automation and autonomous processes yield transformative effects on surveillance, intelligence, and reconnaissance, as well as on command and control. At the same time, the growing accessibility of smartphones has resulted in the increased capture and sharing of questionable actions by security sector actors, such as human rights abuses by the police, while CCTV cameras have become increasingly prevalent in day-to-day life as a result of accessible and affordable technology, leading to concerns regarding policy vacuums in the progressively indiscriminate use of surveillance and interception technology. This newfound ability to document, disseminate, and act upon evidence through digital platforms has had profound implications for the principles of good SSG, namely accountability, transparency, rule of law, participation, responsiveness, effectiveness, and efficiency.

[57] In the context of the present Analysis, it is important to note that most expert opinions and insights were gathered from Round 1 and Round 3 questionnaires. The Round 1 questionnaire provided the experts with open questions, allowing them to freely express their views and experiences. The Round 2 questionnaire asked the experts to validate the initial consensus observed, hence giving them less space for expressing subjective views. The Round 3 questionnaire presented the identified consensus to the experts and asked for their approval, while allowing the experts to further express their views on how digitalization will impact security providers and overseers.

Therefore, this thematic area assesses the practicality, functionality, efficiency, and impact of new technologies on the security sector. The experts touched upon a wide spectrum of issues that fell under the thematic area of new technologies and provided recommendations for security sector actors to address challenges going forward. The research team has narrowed the disparate strands into three main sub-areas, namely (1) the compatibility of legacy systems with new technologies; (2) the opportunities a digital paper trail presents for increased accountability and oversight; and (3) questions surrounding the automatization of decision-making based on big data. The following sub-sections will expand on these themes and integrate the converging viewpoints provided by the experts. In addition, a spotlight section will provide more concrete and practical insights into the potential for using AI in security delivery, before examining the impact new technologies have on various security sector actors.

Updating legacy systems

Legacy systems refer to technologies, both hardware and software, that are outdated and find themselves subject to increasingly limited functionality as new technologies are being developed and released.[58] More precisely, legacy systems can consist of relevant infrastructure, such as equipment, networks, and the fail-proofing of these systems to ensure data can be collected, accessed, and stored safely. The compatibility of old and new technologies used by security sector actors is not to be taken for granted for a wide variety of reasons, including the constantly evolving nature of digital technologies. Legacy systems lead to a lack of compatible information platforms between different security institutions, as highlighted by several experts. One expert noted that as a result of this lack of compatible platforms, 'data cannot be shared and comprehensively analysed to improve decision-making', which therefore limits the capacity for planning and coordination of activities between different security sector actors.[59]

We can imagine that a slow internet connection, or out-of-date software and hardware, can significantly slow down how government institutions perform tasks and provide services that are timely, relevant, and helpful. In addition to these limitations, legacy systems may operate with known vulnerabilities that are difficult or too expensive to address, as, in some cases, where vendors no longer provide support for hardware and software. For example, in 2019, the United States Government Accountability Office (GAO) identified ten federal agencies with critical legacy systems that needed modernization.[60] These legacy systems included a maintenance system that supported wartime readiness which was used for more than 14 years, posing considerable risks to the security of the Department of Defense, and a network that consisted of routers, switches, and other network appliances which was eleven years old, also implying high security risks for the Department of Homeland Security. These examples illustrate the long lifecycles of these systems and the critical role they play in the security sector of a state.

The incompatibilities and limitations of legacy systems could have an impact on the planning and coordination of activities within and between different security institutions, due to both overlaps and gaps in information systems and platforms.[61] Questions therefore remain regarding the extent to which new technologies can be integrated into existing, potentially outdated, infrastructure in such a way that security sector actors can continue to perform tasks and provide services in a manner that is timely, relevant, cost-efficient, and helpful.[62] In this vein, one expert observed that 'the scope of digitalization primarily means the creation of interoperable systems in which data will be collected, processed, provides statistics, and analysis whose results will improve the system in terms of providing services to citizens, education, health, security services […] up to the media and opportunities to exercise fundamental rights'.[63] Therefore, interoperable systems do not refer to only updating legacy systems to new technologies that in the end will be used by only one security institution, but rather to the creation of novel systems, building upon the existing ones in some cases, that are accessible and can facilitate security delivery between varying and different security institutions.

[58] Round 1, Response 1.

[59] Round 1, Response 9.

[60] GAO Insights, United States Government Accountability Officer, 'Agencies Need to Continue Addressing Critical Legacy Systems' (2023).

[61] Round 1, Response 9.

[62] Round 1, Response 6.

[63] Round 1, Response 1.

In recent years, the creation of interoperable systems where information can be safely accessed and transferred among security sector actors and institutions has been a first step in legacy systems modernization. Legacy systems modernization refers to the process of updating and optimizing systems to gain operational effectiveness, address technology constraints, meet expectations, and support the adoption and integration of other systems based on newer technology platforms. The process of legacy modernization is initiated when organizations find themselves stuck between maintaining older, expensive hardware and software that are unable to interoperate with new technologies and undertaking the monumental task of revamping their digital infrastructure to keep pace with new requirements in terms of operations and service delivery. Interoperability is the property that facilitates unrestricted sharing and use of data or resources between distinct systems. For two systems to be interoperable, they must be able to exchange, interpret, and present shared data that is understood by the other. The benefits of interoperability include increased productivity, reduced costs, and reduced errors.[64] For example, interoperable systems facilitate eGovernment solutions that address challenges such as language barriers and streamline service provision for citizens, businesses, and public administration.

> *'Security sector actors are often still using legacy systems, while the private sector (due to financial incentives) has adopted new technologies much more rapidly'.*[65]

Several experts noted both the expensive initial set-up cost of the digitalization process, in terms of purchasing new technologies and training personnel to use them,[66] as well as hidden costs. These additional costs could not only include the acquisition of new technologies, but also their implementation and ensuring compatibility with legacy systems. Unexpected costs of updating legacy systems will need to be accounted for, as hidden costs during or after the initial purchase will affect the ability of security sector actors to use the new technology efficiently.[67] The initial cost of these changes can make security services 'more expensive as they try to grapple with building new systems, obtaining new data sets, analysing data, creating assurance models around analytical processes, and learning to use this for decision-making'.[68] Yet, despite these initial costs, digitalization can reduce expenses in the long run, as security sector actors have found that 'return on investment is substantial as it can save thousands of hours of retrieval time while also reducing the need for expensive storage space'.[69] In parallel, other experts have acknowledged that the process of digitalization has become more affordable in recent years and less time-consuming as technology continues to develop.[70]

Updating legacy systems also presupposes that there is a need to update in parallel not only the skills of existing personnel using these systems, but also the organizational culture of the security institutions. While this will be discussed in the following chapter, it is important to note that the concurrent development of new technologies, and their adoption in the security sector, can only succeed if the personnel tasked with overseeing the transition and using the new technologies are technologically literate in the systems that they are using. One expert observed that one major problem digitalization poses is 'the ability of managers of the security services, and further, the recipients of police activity, usually justice, to analyse and endorse the elements that may have been acquired during police investigations'.[71] In other words: 'Is a manager who has rather undergone technical evolution during his career in a position to be able to control the work provided by his subordinates, from a technical and procedural point of view?'[72] For example, big data analytics are expensive to set up and maintain, and often require intensive data set training, technical expertise, verification, and testing which, in the short term,

[64] Heavy.AI, 'What is Interoperability?' (2023).

[65] Round 3, Response 15.

[66] Round 1, Response 5; Round 1, Response 16.

[67] Round 1, Response 16.

[68] Round 1, Response 5.

[69] Round 1, Response 16.

[70] Round 1, Response 16.

[71] Round 1, Response 7.

[72] Round 1, Response 7.

make them much more expensive than manual methods.[73] One worrying trend, as noted by an expert, is that digitalization is seen as an answer to cut personnel costs, despite complex digital tools requiring competently trained operators to use them.[74]

Similarly, it is important that the organizational culture of security institutions is open to change. As observed by one expert, 'building a digital facsimile of an analogue process is not digitalization – it misses all the things that digitalization is best-suited to achieve! Thus, increasing digitalization will change [SSG] in a meaningful way only as quickly as relevant institutions and organizations are actually adapting their culture to the digital age, that is, their hierarchies, structures, processes, habits and rituals. If this adaptation process takes place within a political, legal, and ethical framework that insists on accountability, improvements are possible.'[75]

Some experts have also highlighted the disparity between governments with resources and those without, with experts suggesting that 'governments with resources will probably develop more sophisticated information management systems (some may even be based on AI) to assess the digital information pertaining to the security sector'[76] while other governments or institutions may have limited access to resources and thus retain legacy systems for longer, having less capacity for interoperability and information sharing. It is in this context that the experts unanimously agreed on the importance of parliamentary oversight of spending by the security sector on digital resources to facilitate their work. It was acknowledged that while parliamentary oversight of financial resources and budgetary questions should already be integrated into annual budgetary discussions,[77] this process should also be included in legislation and policy. While it is the 'task of the government to propose the budget, which should be related to the digitalization of the public security actors', parliament remains 'responsible for approving and monitoring these budgets'.[78] Therefore, updating the legacy systems of different security institutions refers to the incorporation of new technologies as well as the updating of the skills and capacities of personnel. While the costs and the resources of each entity should be kept in mind, investment should nevertheless not be feared if done with appropriate oversight and with the right levels of transparency.

Creating a digital paper trail

Of all the opportunities that digitalization offers, the ability to easily record, retrieve, and disseminate information is one that the experts unanimously agree on as being highly beneficial for the security sector. As it currently stands, many experts observed not only that security sector actors struggle with the amount of paperwork that their work entails, but also that some actors may use the lack of a digital trail to obfuscate and prevent proper oversight of their activities. New technologies enable the security sector to create digital paper trails to deliver security in more accountable, efficient, and innovative ways. A digital paper trail implies that all digital communications and documentation are virtually logged, which, according to an expert, means that 'the risk of cases, evidence, or reports being misplaced or lost can be mitigated' and that 'logging complaints or reporting crimes can become a lower threshold activity than it is when doing so in person'.[79] An increase in reporting accuracy was highlighted as a positive effect of digitalization by many experts, with one noting that 'mismanagement […] of personnel data has been one of the most enduring challenges to accountability in many countries […] Digitalization will make it much more difficult to hide nefarious activities in relation to personnel management.'[80]

---

[73] Round 1, Response 5.

[74] Round 1, Response 4.

[75] Round 1, Response 8.

[76] Round 1, Response 12.

[77] Round 3, Response 13; Round 3, Response 5.

[78] Round 3, Response 8; Round 3, Response 10.

[79] Round 1, Response 4.

[80] Round 1, Response 11: 'Given the antecedents in many of these institutions, one of these challenges is how to prevent the increased ability to carry out security missions from translating into the same institutions being able to also "effectively" violate human rights or hide the misdeeds of their members. In fact, the increased effectiveness, for example, in record management and data analysis digitalisation may increase the temptation in some security sector actors to find loopholes that will enable them to engage in activities that are incompatible with good security sector governance principles.'

According to another expert, as security sector actors will 'inevitably leave "traces" when they carry out their operations',[81] activities can be monitored in real-time, and any concerns addressed immediately. In general, it can be expected that the amount of physical paperwork will be decreased, for processes will likely be more streamlined into digital formats and be less of a burden to security providers, overseers, and the population in general. However, it is worth mentioning that experts also pointed to the attribution problem in the digital space, as it is still challenging to definitively identify the source of an action and the identity of the institution or individuals responsible with existing digital forensic tools.[82] This challenge has the potential to hamper 'the work of independent oversight bodies (such as parts of the judiciary or parliament) and subverts the proper implementation of their control mechanisms', as well as preventing the ability of an independent press to shed light on the actions of security providers.[83] Despite this challenge, an expert observed that increased transparency by security sector actors, and capacity to trace the steps in processing operations, may serve as an additional motivator for personnel to be 'more committed to their work so that errors can […] be avoided'.[84]

> *'With a well-established system and its proper "data feeding", […] personalization of management and political influences […] will be avoided. Digital records are difficult to delete'.*[85]

Digitalization can offer greater and faster access to information for security sector actors through the use of new technologies, thereby facilitating better and more purposeful planning in the execution of tasks.[86] With proper cataloguing of past records and recording of best practices, as well as macro trends discerned from existing data sets, past mistakes can be avoided and successes emulated.[87] For example, one expert observed that 'instantaneous access and analysis of existing data sets on certain terrorist groups/individuals, together with digital monitoring of activities, can assist in deciphering intentions, narrowing down potential targets, and deploying relevant resources to foil pre-meditated actions'.[88] By helping the security sector to access key data more quickly, personnel in the field will be better placed to make 'a faster and, above all, more correct decision'.[89] In this vein, digitalization can also 'allow for better searchability of documentation and other resources, which makes finding relevant information easier, and is highly beneficial for those looking to undertake research on the security sector with a view to engaging with the decision-making processes'.[90]

Digitization of information is often the first step towards improving access to information that, in turn, facilitates enhanced oversight and accountability. Within this context, one expert mentioned the importance of making available information pertaining to 'discussions, decision-making, meetings, communications, planning, and the implementation of activities (such as surveillance, operations, and investigations)' to oversight actors and, where appropriate, to the public.[91] By making access to information easier, actions and operations by security sector providers can be monitored in real-time to ensure that their conduct is in line with relevant laws and regulations. New digital technologies thus bring novel possibilities for documentation and tamper-proof record-keeping to facilitate continuity, create transparency, and help ensure accountability.[92] Digitalization can contribute towards

[81] Round 1, Response 6.

[82] Round 1, Response 8.

[83] Round 1, Response 8.

[84] Round 1, Response 13.

[85] Round 1, Response 1.

[86] Round 1, Response 6.

[87] Round 1, Response 6.

[88] Round 1, Response 6.

[89] Round 1, Response 6.

[90] Round 1, Response 12.

[91] Round 1, Response 12.

[92] Round 1, Response 11 'The actions of security sector actors can be more easily documented, stored, and made available at a click.'; Round 1, Response 12 'The digitization of reports, memos, communiques and other documentation can be digitized and made available for accountability purposes.'

routine, and systematic storing and updating of records of past performances help develop plans that avoid past mistakes and adopt best practices, thereby ensuring more efficient, cost-effective, and seamless service delivery.[93] According to an expert, digitalization 'obviously greatly facilitates conservation of materials and, with sufficient backups, can keep them safe indefinitely as long as storage space is available', and 'provides relatively instantaneous access to stored data for retrieval, for analysis, or just to get relevant information without having to go through (in the pre-digital age) printed or other forms of written materials that will take time and resources'. [94]

The management of sensitive information remains a big concern.[95] It is a critical aspect for security sector actors when utilizing a digital paper trail. While digitalization offers numerous benefits, it also poses challenges in ensuring the confidentiality and security of sensitive data. Security sector actors must implement robust data protection and security measures to safeguard sensitive information from unauthorized access, manipulation, or theft. This involves employing encryption techniques, access controls, secure storage systems, and regular security audits to maintain the integrity and confidentiality of the data. For example, in law enforcement agencies, personal information of witnesses, informants, or undercover agents needs to be securely stored and accessed only by authorized personnel. Digital systems with strong authentication mechanisms, encrypted databases, and restricted user access can help protect this sensitive information from falling into the wrong hands. As such, security sector actors often handle a delicate balance between maintaining transparency and protecting sensitive information. While transparency is crucial for oversight and accountability, certain information, such as ongoing investigations, intelligence sources, or national security details, requires confidentiality to prevent compromise and protect individuals involved. Police departments may adopt digital systems to facilitate the sharing of crime data with the public for community engagement and trust-building purposes; however, sensitive information, such as details of ongoing covert operations or intelligence assets, must be carefully excluded from public access to prevent potential risks.

Digital record-keeping can make disclosing non-classified information less cumbersome and time-consuming, however, especially in response to freedom of information requests. 'Freedom of information requests and proactive publishing of data, particularly when accessible through the internet, can help in restoring or building trust between the community and the security sector and help in digital outreach and digital community policing efforts.'[96] For example, during the COVID-19 pandemic, governments across the world mainly used online platforms to respond to freedom of information requests from the public and the press. Nevertheless, when handling freedom of information requests, security sector actors need to ensure that personal information, confidential investigative techniques, or classified materials are appropriately redacted or withheld to protect sensitive information while fulfilling their obligations to transparency and accountability. In addition, as the reporting process will become increasingly simplified, security sector personnel will be able to devote more time to actions that require human interaction.

At the same time, digital record-keeping can facilitate international cooperation – 'intelligence sharing across various countries provides learning opportunities for all parties involved'.[97] As stressed by another expert, 'secure national, regional, and international cooperation platforms enable the rapid exchange of data related to traditional and contemporary threats, as well as the handling of complex tasks'.[98] Going forward, digitalization offers many opportunities to improve the data collection, retention, and accessibility of security sector actors through the use of new technologies. As posited by one expert, digitalization 'enables more efficient, reliable and faster responses to issues arising and therefore in general improves services delivered',[99] while another observed that digitalization 'allows accurate targeting of issues and problems and, as a result, effective mobilization and use of valuable resources for targeted use to deliver timely and cost-effective services'.[100] With a digitalized set of information, it

[93] Round 1, Response 6.

[94] Round 1, Response 16.

[95] Round 1, Response 16.

[96] Round 1, Response 4.

[97] Round 1, Response 4.

[98] Round 3, Response 9.

[99] Round 1, Response 6.

[100] Round 1, Response 6.

will become easier and faster to systematize, store, identify, and locate relevant and up-to-date information that will facilitate both decision-making as well as command and control.

Automating decision-making

With so much information instantaneously accessible, and with such big databases of existing information, new technologies have been developed to analyse and automate decision-making based on big data. The automatization of reporting and data analysis can ensure not only that there will be less personalization of external political and management influences, but also an increased consistency in the application of norms, promoting accountability by security sector actors. Nevertheless, all AI and autonomous digital processes raise questions concerning the distinction between decisions made by humans versus decisions made by machines, as well as the prerequisite for the final decision to ultimately be made by humans. With the proliferation of AI-enabled tools, many questions have been raised as to the extent to which these tools can result in biased outcomes. As one expert observed, it is often the case that commercial contracts prohibit purchasers from disclosing certain details about the tools, or that security sector actors themselves refuse to disclose relevant details.[101] Using facial recognition as an example, the expert noted that the 'accuracy percentage depends on the conditions within which the camera is deployed, the quality of the reference images, lighting and weather conditions, etc.'[102] and that problems concerning the number of false positives rendered by the tools are exacerbated when AI and machine learning are involved, as 'the code is written by the algorithm itself and the weight given to elements is unknown to the operators'.[103]

> *'Humans will be less involved in the governance and accountability of the security sector, as AI-based programs will do most of their day-to-day work. The role of a person will be reduced to setting up an algorithm for managing security services, methods of monitoring the effectiveness of these services, [and] programs that will analyse the data collected about the works done'.*[104]

Algorithms can help with resource optimization by pooling resources, better allocation of personnel, and mitigating overspending. These tools can facilitate efficiency by identifying patterns and automatically flagging any problems. Through machine learning and office automation, institutions can learn more from their data flows and be more effective in utilizing the information and identifying tasks that no longer require a human interface. New technologies, such as AI, can therefore cut costs and free up personnel for less manual, routine-type jobs. As put by one expert, 'when not cost-effective vis-à-vis office automation, human interfaces can increasingly be replaced by very dumb but smart-looking office automation'.[105] Digitalization also can facilitate fast and secure communication between security sector actors, thereby increasing efficiency, decreasing risks derived from the 'human' factor, and ultimately limiting any potentially negative financial and security consequences. Nevertheless, some experts raised concerns about the insufficient human resources 'to handle large quantit[ies] of data and related digital projects, with questionable decision-making based on limited knowledge of big data analytics, and a general lack of data-driven and evidence-based working culture in security sector institutions'.[106] Consequently, it is vital that automatization is implemented in parallel to the training of personnel to ensure that these new technologies are being operated by individuals and teams that fully understand the potential impact and consequences of these systems.

In this context, a few experts specifically highlighted the impact of automated decision-making on the implementation of international humanitarian law (IHL). One expert suggested that automation in military targeting processes could facilitate a consistent and coherent implementation of IHL on the battlefield, as 'AI-assisted targeting processes may – if implemented properly and ensuring meaningful human control over critical functions of target selection and engagement – be conducive to a more accurate and reliable effectuation of a commander's

[101] Round 1, Response 4.

[102] Round 1, Response 4.

[103] Round 1, Response 4.

[104] Round 1, Response 14.

[105] Round 1, Response 2.

[106] Round 1, Response 16.

intent regarding the application of military force'.[107] However, one must keep in mind that an increase in precision does not necessarily mean heightened compliance with IHL, as human commanders still need to make a judgement call and apply the law. Digital technologies can only assist in performing these tasks faster and, hopefully, in better compliance with IHL.

The use of automated weapons systems raises challenges regarding accountability and responsibility for any harm caused. Within this context, automated weapons systems, also known as lethal autonomous weapons systems (LAWS), refer to weapons that can independently select and engage targets without direct human control.[108] The development and use of such systems raise significant concerns and risks in the context of IHL. One of the primary concerns is the potential lack of human judgement in the decision-making process of selecting and engaging targets, and human judgement, including considerations of proportionality and distinction, is essential for adhering to IHL principles. As expressed by an expert participating in the study, 'stripping targets of autonomous weapon systems of their humanity and dignity, reducing them to mere data points fed into an algorithmic killing machine, represents a violation of IHL'.[109] Removing or diminishing human involvement in targeting decisions can lead to errors, miscalculations, or misidentifications, resulting in indiscriminate or disproportionate attacks. Military commanders need to be the ones making judgements and applying the law accordingly, and, though being assisted by new digital technologies, they should not pass all accountability to the machine.

In the case of an autonomous weapon system committing a violation of IHL, it can be challenging to attribute responsibility to a human actor, as the decision-making process is delegated to the system itself. This complicates accountability mechanisms and may hinder the ability to hold individuals accountable for breaches of IHL, which emphasizes the importance of taking precautionary measures to minimize harm to civilians and civilian objects during armed conflicts.[110] In parallel, the use of automated weapons systems raises concerns about the ability of such systems to effectively comply with the principles of good governance. The complex and unpredictable nature of armed conflicts and the potential for technological failures or malfunctions can increase the risk of civilian casualties or damage to civilian infrastructure. Autonomous weapons lack human qualities, such as empathy and contextual understanding, which are crucial for making nuanced decisions in complex situations. These systems may struggle to accurately assess the intentions, emotions, or motives of individuals, potentially leading to incorrect targeting decisions or the use of excessive force. The use of automated weapons systems raises ethical concerns regarding the dehumanization of warfare. Relying on machines to make life-and-death decisions distances humans from the consequences of their actions, potentially eroding the moral and ethical considerations that underpin IHL. Moreover, automated weapons systems heavily rely on software, algorithms, and communication networks, making them susceptible to hacking and cybersecurity risks. If malicious actors gain control over these systems, they could manipulate their targeting capabilities, leading to unauthorized or unlawful attacks that could cause destruction and harm human life.

Besides the devastating risks these weapons pose to human security, there is a plethora of ethical and legal concerns due to the difficulty in anticipating and limiting their effects, such as acceleration of the use of force beyond human control. A primary concern is the potential for LAWS to operate without any meaningful human control, leading to the loss of accountability of security sector actors employing such tools. The rapid decision-making process of autonomous weapons does not allow for the nuanced judgement necessary to comply with the rules of IHL, leading to gross violations. In addition, concerns exist about the compliance of such weapons with international treaties that govern the conduct of warfare, such as the Geneva Convention. The integration of LAWS into the security sector might strain existing SSG/R efforts, as ensuring responsible and ethical use of such technologies requires the creation of relevant governance structures and oversight mechanisms.

Addressing these concerns related to automated weapons systems requires careful consideration and the establishment of appropriate legal and regulatory frameworks. Discussions on the development, deployment, and use of autonomous weapons are ongoing within the international community, aiming to ensure that IHL principles and human control remain central in determining the use of force and minimizing harm to civilians during armed

[107] Round 1, Response 8.

[108] Davison, N., 'A Legal Perspective: Autonomous Weapon Systems Under International Humanitarian Law', *ICRC* (2018).

[109] Round 1, Response 8.

[110] Davison, N., 'A Legal Perspective: Autonomous Weapon Systems Under International Humanitarian Law', *ICRC* (2018).

conflicts. To date, existing autonomous weapons systems have been used only against well-defined military targets – military radars and enemy tanks – in areas where there are few civilians or civilian objects. Examples of existing autonomous weapons include air defence systems that strike incoming missiles and some loitering munitions developed to target military radars, tanks, and armoured vehicles.[111] Weapon technologies and practices are changing fast, however, just as contemporary conflicts gain new dimensions. Militaries and weapon developers are interested in integrating the autonomous use of force in a wide variety of weapons, including armed drones – also known as unmanned aerial vehicles (UAVs) – that are currently remotely controlled by human operators.

Spotlight: The use of artificial intelligence in the security sector

AI leverages computers and machines to simulate the problem-solving and decision-making capabilities of the human mind, and it allows machines to perform tasks with minimal or no human assistance or supervision. This has myriads of applications in everyday life – ranging from the virtual phone or home assistants to the more recent car autopilot function. Regarding security provision, the experts participating in this study unanimously agreed that *AI yields transformative effects on surveillance, intelligence, and reconnaissance, as well as command and control*. For example, the most widespread use of AI in the Ukraine war is in geospatial intelligence. AI is being used to analyse satellite images and is geolocating and analysing various open-source data, such as social media photos in geopolitically sensitive locations. Neural networks are used, for example, to combine ground-level photos, drone video footage, and satellite imagery to enhance intelligence in unique ways to produce strategic and tactical intelligence advantages.[112] At the same time, AI is playing an important role in communications interception, as it has been deployed to analyse unencrypted Russian radio communications.

Another important use of AI in and around the Ukraine conflict is in cyber warfare, especially in support of defensive capabilities. A report published by Microsoft showed that cyber defences may have proven relatively successful, mostly thanks to advances in AI-enhanced threat intelligence and the quick distribution of protective software.[113] However, AI is massively used to spread misinformation and foster biases. AI software has been used to create images and content for fake social media accounts used in propaganda campaigns. While the spread of disinformation is not new, AI offers numerous unprecedented opportunities for scaling and targeting such campaigns, especially in combination with the broad range of social media platforms. Yet, there is a tragic paradox to the use of AI in the Ukraine war: as the conflict rages on and human lives are lost, AI systems are trained with real data from the battleground not to stop the suffering of innocent civilians, but to become more effective in fighting future wars.[114]

Along these lines, the experts have identified several challenges with the available AI tools in the security sector. First, AI might exacerbate existing problems of accountability and transparency in terms of the use of such tools by security sector actors. Security sector actors need to ensure that the logic for deploying AI tools is clearly explained to relevant stakeholders. Second, AI might pose some challenges in terms of efficiency of the security sector actors in employing such tools. There is the risk that the security sector actors in charge of AI software might spend too much of their time justifying the results produced by the machine, leading to more paperwork rather than efficiency. Humans will be less involved in the governance and accountability of the security sector, as AI-based programs will do most of their daily work. The role of a person will be reduced to setting up an algorithm for managing security services, developing methods of monitoring the effectiveness of these services, and implementing programs that analyse the data collected. And third, the experts suggest that too many of the data sets used to train AI applications reproduce and reinforce the widespread societal biases about race, gender, sexual orientation, age, and so on. For example, applied for determining bail, sentencing, or parole, the use of AI undercuts the rule of law, while when used for spatial analysis to identify ‘street crime’ and at-risk areas, it has the power to stigmatize and discriminate.[115] It creates significant risks to privacy, data protection, and is prone to discriminatory misuse – which is why numerous international entities have requested stricter regulations to prevent

[111] Ibid.

[112] Fontes, R., and J. Kamminga, ‘Ukraine: A Living Lab for AI Warfare’, *National Defense* (2023).

[113] Microsoft, ‘Defending Ukraine: Early Lessons from the Cyber War’ (2022).

[114] Fontes, R., and J. Kamminga, ‘Ukraine: A Living Lab for AI Warfare’, *National Defense* (2023).

[115] Round 1, Response 13.

human rights violations. In this context, AI and other new technologies need to be paired with ethical oversight mechanisms to ensure they do not exacerbate existing social inequalities or lead to human rights violations.

However, not everything related to AI is doom and gloom. First, experts agree that by employing AI applications, security sector institutions can learn more from their data flow, thus improving their effectiveness in utilizing the information and implementing relevant follow-up actions. Second, experts add that governments with resources will probably develop more sophisticated information management systems (some may even be based on AI) to assess the digital information pertaining to the security sector. For example, using AI in the justice sector can mean intelligent search engines for analysing court rulings.[116] With such tools, large amounts of data are analysed by cataloguing the content and extracting sought terms or contract clauses. And third, experts believe that in terms of intelligence gathering, the military can adopt and integrate AI into the collection and interpretation of satellite and UAV surveillance data feeds to provide a clearer picture of a conflict or crisis zones.

In this context, if implemented properly and ensuring meaningful human control over critical functions, the use of AI furthers the opportunity for security sector institutions and actors to analyse a huge amount of data to solve problems faster and be conducive to a more accurate and reliable effectuation of a commander's intent regarding the application of military force, by improving their situational awareness. However, AI and other new technologies should be regarded as tools, and not as replacements for human control and command, in order to avoid violations, abuses, and other harms detrimental to human life and security.

Security sector actors and new technologies

The experts participating in this study have highlighted that traditional security sector actors have a central role in the implementation and use of new digital technologies. Experts unanimously agreed that the digital revolution is visible in existing military processes and equipment (e.g. precision targeting, unmanned area vehicles), as it is opening an entire domain through which warfare is conducted digitally and remotely (e.g. hostile disinformation campaigns). Modern technologies are more cost-efficient than the physical arsenal employed by armed forces and they have an asymmetrical impact. The same experts claimed that digitalization offers armed forces the opportunity to divest themselves of outdated legacy systems by investing in emerging technologies (e.g. AI, cloud computing, machine learning, and big data) to improve their efficiency in the digital space. In addition, the experts mentioned that the police have made considerable steps in updating legacy systems. The expert states that the 'police are impacted by any technological progress and must be able to constantly adapt to execute their mission. This is both an extraordinary opportunity but also a significant pressure.'[117] Police officers now enjoy individual workstations that allow them to efficiently carry out their duties and to search for additional information. In parallel, the introduction of smartphones for police officers has facilitated their communication through dedicated police applications. The digitalization of police services 'enables more efficient, reliable, and faster responses to arising issues' and by using digital data set, 'it is relatively easy and faster to locate relevant information necessary for performing certain tasks'.[118]

The experts recognize that new technologies have introduced new players to the security field. For example, the experts unanimously agreed that cybercriminals have access to the latest digital tools, which therefore places 'high pressure on security sector institutions and actors to update their digital systems to face the demands and challenges of their operational needs'.[119] In addition, the lack of security around new digital technologies makes them more prone to cyberattacks. Moreover, the experts claimed that there is a need for big tech companies to not only set up the infrastructure to store security information, but also to build new digital tools that can ensure a high level of security.

Key recommendations: New technologies

Within the context of the current Delphi study, 15 experts engaged in a collaborative process to establish consensus on the opportunities and challenges digitalization poses for the security sector. In terms of new

[116] Round 1, Response 13.

[117] Round 1, Response 7.

[118] Round 1, Response 6.

[119] Round 3, Response 13.

technologies, the following three recommendations were developed by synthesizing the participating experts' insights and opinions that were presented in the previous sections:

1. The security sector needs to ensure oversight of its spending on digital resources to ensure transparency and accountability in the allocation of resources for updating legacy systems.
2. Security sector actors should adopt digital tools to improve traceability of processes, sharing of information, and record-keeping within the security sector, to ensure better responsiveness, effectiveness, and efficiency.
3. New technologies, such as AI, need to be implemented with careful consideration of their ethical and legal implications. Security sector actors should ensure that human judgement remains a central component of decision-making to ensure the prevalence of rule of law.

Thematic area 2: Technical capacity

One of the central issues posed by digitalization in good SSG is the technical capacity of security sector actors. The technical capacity of security sector actors refers to their ability to effectively utilize and leverage technological tools and resources to fulfil their roles and responsibilities related to security and defence. Experts noted that investments are needed not only in infrastructure, but also in the technical capacities of current and prospective security sector personnel to effectively leverage digital tools and stay ahead of cyber threats. As a matter of fact, there is an urgent need to promote integration of technology in education programmes in all aspects of everyday life, as growing differences in the level of digital development around the world have the potential to cause security problems, instability, and even conflict.

Security sector actors are confronted by access to new technology to assist their mandate as well as new security challenges – and emerging actors – as a result of digitalization. Digitalization has brought about a host of new security challenges, particularly in the realms of cybersecurity and cyber warfare. In some cases, security sector actors are confronted with the task of safeguarding critical infrastructure, sensitive data, and citizens' privacy from sophisticated cyber threats. Yet, as stated by numerous experts participating in this study, security sector actors neither have the training nor the policy frameworks in place to effectively manage the changing digital environment, especially when it comes to emerging cyber threats and cybercrime. Therefore, in today's digital age, cybersecurity has become a critical aspect of the security sector. Security sector actors must have the knowledge and tools to protect their own systems and infrastructure from cyber threats, while also possessing the knowledge and skills to employ a wide breadth of digital tools in their daily work.

This thematic area analyses the technical capacity of security sector actors to utilize novel technologies, providing insights into their adaptation to increasing digitalization and the emergence of new actors in the security field. The research team has narrowed the consensus reached by the experts into three main sub-areas, namely (1) educating and training existing personnel; (2) recruiting and retaining qualified personnel; and (3) cooperation and sharing of best practices between different security institutions. The following sub-sections will expand on these areas and integrate the converging viewpoints provided by the experts. In addition, a spotlight section will provide concrete insights into the unanimous consensus reached on the need to enhance cybersecurity awareness and digital hygiene practices among security personnel, before delving further into examining the influence of the technical capacities of security sector actors on their daily operations.

Educating and training existing personnel

Experts expressed serious concerns regarding the limited, or lack of, education and training for security sector personnel. A competent and well-educated workforce that is up to date, tech savvy, and familiar with the systems and tasks at hand is essential for ensuring a successful digitalization process that respects the principles of good SSG. This is not necessarily about having the knowledge to code or to develop digital tools, but rather about acquiring a comprehensive awareness and understanding of technical trends, and of best practices in terms of using new technologies. More specifically, experts emphasized the importance of all security sector actors being given extensive training in the accountability and human rights aspects of their activities, including the legal and oversight mechanisms governing the use of digital capabilities in line with human rights law. For one expert, it was important that security sector actors 'know they have both the responsibility of ensuring and providing security, and

accountability in how they use information obtained through increasing digitalization'[120] and at the same time be able to 'manage the proper balance between the requirements of law and the imperative of timely actions to prevent and stop harms to public security'.[121] Another expert raised an important question: 'For example, is a manager who has […] undergone technical evolution during his career in a position to be able to control the work provided by his subordinates, from a technical and procedural point of view?'[122] Therefore, it can be deduced that the lack of knowledge and awareness of the potential impacts and consequences of digitalization by senior security sector actors can lead to gaps in oversight in the provision of security, even if there is a well-educated and trained cohort of junior staff.

> *'…a very basic challenge is digital literacy and competence, especially in public security sector organizations. At least in my country, there's little reason to assume that they are able to operate at a high professional standard in the digital sphere.'*[123]

Increased technical capacity of the security sector can be achieved in a myriad of ways. At an individual level, security sector personnel can benefit from online training and educational material and courses, as well as specialized training with virtual reality (VR) or mixed reality (MR) technologies, which can train and educate learners before they enter the classroom so the physical session can focus on the aspects that cannot be replaced with virtual training (e.g. certain skills or simulations). One expert suggested that course curricula, training/academic materials, training methods, and external evaluations can be digitized, along with the assessments/grading of trainees, to allow for oversight bodies to be more able to determine the quality of the training and whether trainees are being provided with relevant (and legal) instruction.

The experts placed a lot of emphasis on the need to raise the digital capacities and skills of entities and personnel that oversee security providers, so to prevent poorly worded legislation and lack of oversight for security provider operations in the digital space due to lawmakers having a poor grasp of digital issues. In other words, oversight bodies and judicial agencies lack sufficient technical expertise and knowledge of digitalization to be able to effectively interpret the information provided by security providers and to ask the right questions. Experts underlined the importance of providing consistent and up-to-date technical training so that existing security sector personnel are able both to effectively manage and to continue delivering security in the changing digital environment.

Security sector organizations should establish specialized training courses that focus on the specific digital technologies relevant to their operations. These courses should cover areas such as cybersecurity, AI, data analytics, digital forensics, and information management. The training should be delivered by subject matter experts and experienced professionals to ensure the highest quality and practical relevance. Moreover, inculcating principles of good SSG is vital during this training process. Understanding the legal and human rights implications of using digital technologies in security operations is imperative to prevent misuse and safeguard the privacy of individuals. Simulated exercises and real-world scenarios should be integrated into the training curriculum to provide practical experience. This hands-on approach allows security sector personnel to understand how to navigate complex situations while utilizing digital tools effectively and responsibly. Furthermore, collaboration and coordination between different security sector actors should be emphasized during training to promote information sharing and efficient responses to security threats.

For example, the UK's Ministry of Defence (MoD) has placed a strong emphasis on digital technology education for its security sector personnel.[124] It has implemented training programmes focusing on cybersecurity, data analytics, and digital intelligence, among other areas. The UK's National Cyber Security Centre (NCSC) works closely with government agencies and the private sector to enhance cyber capabilities and promote best practices.

[120] Round 1, Response 6.

[121] Round 1, Response 6.

[122] Round 1, Response 7.

[123] Round 1, Response 8.

[124] UK Government, Press release, 'UK Defence Cyber Skills to be Boosted Through Industry Partnership' (2022).

In addition, Estonia is often regarded as a leader in digital governance and security.[125] The Estonian Defence Forces have prioritized cyber defence education and training for their personnel, recognizing the importance of staying ahead in the digital realm.[126] Estonia's Cyber Defence League is an example of a voluntary organization where citizens with digital expertise support the country's cyber defence efforts.

Continuing education and professional development should be encouraged for security sector personnel throughout their careers. Digital technologies evolve rapidly, and ongoing training ensures that security sector actors remain up to date with the latest advancements and best practices. To maintain good SSG, it is essential to establish oversight mechanisms to monitor the implementation of digital technologies within security operations. Regular audits and evaluations can help identify potential issues and ensure that technical capacities are being used in line with established principles and guidelines. Educating and training security sector personnel to improve their technical capacities in digital technologies while adhering to the principles of good SSG is essential for effective and responsible security provision. By equipping security sector actors with the right knowledge, skills, and ethical awareness, they can leverage digital tools to protect communities while upholding the values of transparency, accountability, and respect for human rights.

Recruiting and retaining qualified personnel

In addition to training existing personnel, it is important to continuously recruit qualified personnel, and to provide incentives to ensure the retention of talent. The scarcity of talent will continue to persist as the demand for technical personnel increases in all sectors. One expert pointed to lack of qualified personnel as a consequence of school programmes in many countries remaining focused on last-century approaches to education while failing to create digitally proficient individuals for the 21st century.[127] Limited attention is given to digital skills in primary and secondary education (such as a basic understanding of digital productivity tools or data hygiene) thereby rendering students unprepared for the challenges of a digital world.

Many experts pointed to the challenges faced by security sector actors in recruiting talent, due to qualified personnel being in high demand in both the public and private sectors. According to one expert, 'due to the scarcity of qualified personnel, recruiting talent in the security sector is difficult. Whilst the security sector offers meaningful work, it rarely offers a competitive salary or secondary benefits matching the private sector.'[128] The inability of security sector actors to attract qualified personnel was identified by many experts as a major roadblock in the process towards facilitating digitalization. Limited resources and the comparatively backward and hierarchical structure of the public sector further fuelled the lack of interest of qualified personnel in entering the security sector.

Security sector actors therefore also face difficulties in *retaining talent*. 'Although the security sector once was on the bleeding edge of innovation', observed one expert, 'currently it is characterized by bureaucratic processes for adopting innovations.'[129] Moreover, 'career paths are deterministic and not (that) flexible'[130], further disincentivising qualified personnel to remain. 'Organizations will have to adopt flexible models to accommodate specific career paths for technical personnel and have to shed experience-based models of promotion and adopt skill-based models of promotion'[131], as argued by an expert. To be able to compete with private sector employers, security sector actors will need to find innovative ways of attracting and retaining qualified personnel. This could include more competitive salaries and benefits, as well as programmes such as graduate training schemes, better professional development opportunities, and flexible secondment openings.

---

[125] National Cybersecurity Centre UK, Home page (2023). Available at: https://www.ncsc.gov.uk/

[126] Kohler, K., 'Estonia's National Cybersecurity and Cyberdefense Posture', Cyberdefense Report, ETH Zurich (2020).

[127] Round 1, Response 2.

[128] Round 1, Response 2.

[129] Round 1, Response 2.

[130] Round 1, Response 2.

[131] Round 1, Response 2.

'…the public sector generally is unable to attract the required talent. Standard wages don't compare to what the private sector has to offer – why work for the Ministry of the Interior when you can land a job at Google or Microsoft? The job profiles are too unattractive [in the security sector].'[132]

For example, the U.S. Cyber Command has been successful in recruiting and retaining tech talent by offering unique opportunities for personal growth and development.[133] The Command emphasizes the importance of its mission in defending the nation's critical infrastructure from cyber threats. Additionally, it has implemented a 'Cyber Excepted Service', which provides greater flexibility in hiring and compensation for cybersecurity professionals.[134] The Singaporean government has established initiatives such as the Cyber Security Associates and Technologists (CSAT) programme, which offers training and internships to tech professionals interested in working for the government.[135] This initiative helps bridge the gap between the private and public sectors and provides a pathway for tech talent to contribute to national cybersecurity efforts. As such, recruiting and retaining security sector personnel with technical capacities is indeed challenging, given the competition with the private sector. However, by adopting competitive compensation packages, fostering collaborative partnerships, offering flexibility, and emphasizing the importance of their mission, security sector actors can attract and retain more personnel with digital skills. The examples provided demonstrate that with the right strategies and approaches, security sector organizations can successfully build and maintain a skilled workforce capable of addressing complex security challenges in the digital age.

Cooperating and sharing best practices

Cooperation and the sharing of best practices between security sector institutions is essential in the effort towards enhancing the overall level of skills and knowledge of all security sector personnel. Different security sector actors and institutions possess diverse expertise and knowledge. By collaborating and sharing best practices, they can harness collective wisdom to develop comprehensive and innovative strategies for addressing security challenges. For instance, intelligence agencies can share their analytical skills with law enforcement agencies, leading to more effective crime prevention efforts. Cooperation fosters better coordination among various actors, minimizing duplication of effort and improving the allocation of resources, while sharing best practices aids in capacity building, especially in areas where certain security sector actors may lack specific expertise.

'On an organizational level, security sector actors can share industry best practices to enhance the overall security in the public and private sectors.'[136]

As a result of digitalization and instantaneous communication services, it is easier for personnel to coordinate between themselves and with other institutions, share information on their work progress, and review their action plans in the digital space. Institutions could develop escalation levels within governments and national emergency exercises to train the various organizations to work together, and could designate information-sharing hubs between institutions with different mandates. This could be the case not only domestically within existing government structures, but also internationally with different offices or institutions operating across different time zones. For example, a government could cooperate with academic institutions to develop training courses for personnel, or devise personnel exchange programmes within different security institutions to share best practices and lessons learned.[137] Similar to military assistance in the physical dimension, one expert suggested that IT

[132] Round 1, Response 8.

[133] United States Ministry of Defense, 'DoD Cyber Workforce Strategy' (2023).

[134] Ibid.

[135] Cybersecurity Agency of Singapore, 'Initiatives, Programmes and Schemes' (2023).

[136] Round 1, Response 2.

[137] Round 1, Response 2.

specialists could train security sector actors in defensive measures to find, fix, and mitigate vulnerabilities in their systems and share other information regarding best practices.[138]

Transparency and accountability will therefore improve as digital processes are implemented and overall data literacy of the security sector is increased. Entities responsible for the oversight of security sector actors and organizations (such as the legislature and/or independent government agencies) are likely to increasingly develop or acquire various types of expertise to better navigate and analyse digital systems and digital information. For example, one expert pointed to the defence sector, arguing that as the skills of other individuals and oversight actors improve, they will be empowered to keep security sector actors 'on their toes'.[139] This would therefore 'translate into better management and governance since security agencies will be constantly aware that they are being watched, by better informed constituents. This, in turn, enhances accountability and effectiveness.'[140] At the same time, industry best practices can also be shared with government by private sector actors, which could involve enforcing standards (ISO-certifications or similar), sharing best practices regarding network architecture, configurations of network applications, patch management, incident response, and so on. According to one expert, we are likely to see growing partnerships with the private sector as governments seek increased digital expertise.[141]

Spotlight: Cybersecurity awareness for security sector actors

As the security sector is increasingly adopting new technologies to improve their operational processes, there is growing consensus about the need to enhance cybersecurity awareness and digital hygiene practices among security personnel. One expert participating in this research mentioned that 'the digital environment is developing very quickly, and specialists in various fields need to constantly improve their competencies and acquire new knowledge'.[142] However, this area is not yet very much noticed in public administration, and the number of qualified personnel is not enough. The European Union Agency for Cybersecurity (ENISA) recognizes the fact that even though cybersecurity is one of the most important challenges faced by governments today, the awareness of security sector personnel remains limited.[143] According to some experts, given the global reach of digitalization, governance and societal stability can be severely undermined by cyberattacks.[144]

As technology advances, so do the techniques cybercriminals use to gain access to our computer networks. Hence, intelligence gathering, law enforcement, and other security sector institutions require the necessary expertise, resources, and legal frameworks to tackle cybersecurity issues. According to a UNDP report, cybercrime's damage in 2021 was estimated at about $6 trillion – up 600 per cent since the beginning of the COVID-19 pandemic in 2020 – in addition to the harms and impact on human security.[145] Cybersecurity can be defined as the notion that the safe use of the digital space by all should be guaranteed and that critical infrastructure and institutions should be protected from digital threats. Thus, it is paramount for law enforcement and other security sector institutions to have access to and receive adequate cybersecurity awareness training to enhance their comprehension of threats and potential mitigation solutions.

In 2017, the WannaCry cyberattack infected more than 200,000 computers in 150 countries, including national governments, security sector institutions, and critical infrastructure.[146] Another significant cyberattack on the security sector breached the US military and multiple federal agencies, including agencies responsible for nuclear weapons. This cyberattack is known as SolarWinds and was conducted by APT29, an organized cybercrime group

[138] Round 1, Response 2.

[139] Round 1, Response 11.

[140] Round 1, Response 11.

[141] Round 3, Response 3.

[142] Round 1, Response 14.

[143] Sarri, A. and R. Arcus, 'Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies', European Union Agency for Cybersecurity (2021).

[144] Round 1, Response 2.

[145] United Nations Development Programme, '2022 Special Report on Human Security: New Threats to Human Security in the Anthropocene' (2022).

[146] Ghafur, S., S. Kristensen, K. Honeyford, et al., 'A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS', *npj Digit. Med*, Vol. 2: No. 98 (2019). Available at: https://www.nature.com/articles/s41746-019-0161-6

connected to the Russian government.[147] According to the Centre for Strategic and International Studies, in April 2023 alone there were at least 11 documented cyberattacks targeting governments and security sector institutions.[148] The number of cyberattacks targeting government agencies saw an increase of 95 per cent in 2022, compared with 2021.[149] Government agencies often gather and keep large quantities of data, including information about citizens. There is also a risk that national security and military data could be accessed and used by hostile nation states. In addition, there was a notable increase in hacktivist attacks or hacking for political motives in 2022. Numerous cyber aggressors act along various political and religious beliefs, or against economic events and policies.

The experts argue that cybersecurity poses several challenges to security institutions and actors. First, one of the issues facing all security sector institutions and actors is the exponential increase of critical failure points and emerging actors in the digital space, because of the digitalization process. For this reason, security sector actors need to be trained and rendered aware of the impact of a cyberattack on security operations or investigations. As security sector actors are collecting digital evidence for their cases, particular attention should be given when opening files from unknown sources so as to not be exposed to a malware or other viruses. Second, digitalization has proliferated cybercrime, as new phishing attacks, data breaches, and spyware have challenged the ability of law enforcement to respond effectively. It is thus important to render security sector actors aware of data privacy and protection mechanisms, as well as different digital threats. Third, there is a lack of a shared cybersecurity maturity level across the security sector. More advanced players will be able to find and fix vulnerabilities, while others will fall behind. At the same time, the security sector finds itself limited by the cybersecurity legislation of the state it operates in, leading some to misuse their cyber capabilities. The security forces, both police and military, must be equipped with the knowledge and resources to respond to all forms of cyber threats created in the digital space. The main concern is the growing depletion of state resources, which will necessarily have an impact on this capacity to respond to new threats.

Nevertheless, the experts argue that security sector institutions and actors have a great opportunity to improve their security culture and take a more proactive stance towards their institution's digital security. The establishment of a high level of cybersecurity, as well as the engagement of independent professional entities providing training courses and certification, will lead to the digital evolution of the security sector. The response to the challenges posed by cybersecurity can be successful only in the case of well-established procedures for cooperation between all security sector stakeholders. In the past few years, due to the rapid increase in damage caused by cyber threats and governments' various efforts to raise awareness, the security sector has improved its comprehension of the importance of cybersecurity. However, experts agreed that a gap persists between perception and practice, as security sector actors do not always implement basic cybersecurity rules and information protection measures in their daily operations. As such, the experts have reached a consensus on the need for continuous training of security sector employees with digital skills and capacities, which is crucial for solving the cybersecurity skills gap in the security sector.

Security sector actors and technical capacity

The experts participating in this study have highlighted that traditional security sector actors are in dire need of improving their technical capacity. For example, the experts have argued that digitalization has added increasing cybersecurity demands on the armed forces and law enforcement. Due to the increasing complexity of the security concept itself and the involvement of more actors in the activities of the security sector, boundaries are no longer as clear as they once were. As such, both law enforcement and the military require professional training that can provide them with the knowledge and awareness necessary to handle and avoid cyber threats. In this context, law enforcement – as frontline actors ensuring the security of citizens – require regularly training in relation to criminal offences in the digital space (e.g. fraud, scams, impersonation, ransomware, phishing, and cyber bullying). At the same time, the quality and level of digital education of armed forces personnel can have a considerable impact on the efficiency of the national security sector in responding to emerging threats. As stated by an expert 'in the era of digitalization, the security sector requires more human resources who have a background in IT, computer programming or engineering. Recruiting people with the right talents has therefore become a priority. However, the

[147] Oladimeji, S. and S. M. Kerner, 'SolarWinds Hack Explained: Everything You Need to Know' *TechTarget* (2023).

[148] Center for Strategic and International Studies, 'Significant Cyber Incidents' (2023).

[149] Reed, J., 'Cyberattacks Rise Sharply Against Governments and Schools', *Security Intelligence* (2023).

job market also competes to hire these people and the salaries provided by private sectors are more flexible and competitive than the security sector.'[150]

Many experts highlighted the fact that governments, parliaments, and civil society organizations (CSOs) lack basic knowledge of technical aspects of security, especially issues such as cybersecurity. For example, CSOs – as organizations that have as their main role assisting vulnerable individuals – can suffer greatly from cyberattacks. Such attacks place much pressure on the limited resources of CSOs, which require extensive training to improve their cybersecurity awareness and assistance to strengthen their infrastructure. However, lack of resources may mean many organizations are unable to employ dedicated staff towards comprehensive cyber protection, which explains why NGOs are increasingly attacked online. Security sector actors can often obstruct efforts of civil society by restricting access to information and can prevent its participation in the development and implementation of security policies. It is therefore essential that governments provide extensive support to CSOs, so that they build a safe environment with enhanced digital capabilities to conduct their activities effectively.

Furthermore, in terms of emerging actors, the experts unanimously recognized the fact that big tech companies can develop IT programs, create educational courses, and form an ethical digital environment to improve the work of the security sector. This knowledge could be used to improve the digital skills of employees in the security sector, but equally help design better training on overarching themes such as human rights and ethics when using digital tools. As such, big tech companies can share industry best practices to enhance the overall public security sector. As an expert suggested, 'on an organizational level this could involve enforcing standards (ISO-certifications, NIST framework, or similar), sharing best practices regarding network architecture, configurations of network applications, patch management, or the creation of a security operation centre (SOC) specifically configured to assist the security sector with incident response'.[151]

Recommendations: Technical capacity

In terms of technical capacity, the following three recommendations were developed by synthesizing the insights of the participating experts, as presented in the previous sections:

1. Prioritize and invest in the education and training of security sector personnel to enhance their technical capacities in digital technologies (including cybersecurity, AI, data analytics, digital forensics, and information management), while reinforcing the principles of good SSG.
2. Security sector actors should actively seek out individuals with technical expertise and digital skills to meet the growing demand for such talent in the sector.
3. Prioritize cooperation, information sharing, and collaboration both domestically and internationally. By working together and sharing best practices, security sector institutions can enhance the skills and knowledge of their personnel, develop innovative strategies, and improve overall security.

Thematic area 3: Regulation and oversight

The integration of digital technologies into the security sector offers security sector actors unprecedented capabilities in surveillance, data analysis, and communication. However, concerns related to privacy, civil liberties, and the potential for abuse have developed in parallel. As such, the regulation and oversight of digital technologies in the security sector have become critical issues in contemporary society. A strong regulatory and oversight framework is essential in the shift towards greater digitalization in the security sector. As stated by an expert, 'digitalisation, as such, is neutral. The security environment, more specifically the threats or the perceived threats that the state is facing, will likely play a major role in defining regulations and norms.'[152] Another expert added that 'for oversight mechanisms to work, there needs to be clear rules and guidelines about the use of digital tools by security sector actors. Lacking those, we enter a morally grey area where what security providers do may not necessarily be illegal but could also likely not be morally or ethically acceptable. Given that legislation cannot be

[150] Round 1, Response 16.

[151] Round 1, Response 2.

[152] Round 1, Response 11.

adopted at the same pace of technical developments, legislation may not be in place, which means that oversight is hampered, and human rights threatened.'[153]

While governments have a central role in adopting and harmonizing a stable legislative and regulatory environment, legislation often does not keep pace with new technological developments, resulting in legal gaps that are often not well understood by lawmakers. This is mainly because there are relatively few people who 'speak' both legal and computer science terminology and can properly bridge this divide. The gaps in legislation regulating emerging technologies will lead to social differences and other implications or security risks, such as disinformation, as well as a rapidly expanding digital divide. More specifically, governments need to ensure that the setting of standards is able to adequately answer different stages of societal change and development, especially with regard to transformation caused by big data analysis, AI, and other technologies. At the same time, it is important to have sufficient resources for relevant actors and industries to engage in R&D and in the implementation of digital networks and infrastructures.

As such, this thematic area explores the challenges faced by security sector overseers to adopt legislation and ensure that oversight keeps pace with technological advancements. The experts discussed different challenges that fell under the topic of regulation and oversight, while providing recommendations for security sector actors to address these challenges going forward. The consensus reached by the experts is divided into three main sub-areas, namely (1) developing legislation and technologies in parallel; (2) overseeing the use of digital technologies; and (3) managing the wide breadth of actors and technologies employed in the security sector. The following sub-sections will expand on these areas and integrate the converging viewpoints provided by the experts. In addition, a spotlight section will provide additional insights into the current data protection regulation practices in the security sector, before examining the impact regulation and oversight of digital technologies have on security sector actors.

Developing legislation and technologies in parallel

One of the central concerns regarding digitalization and new technologies is that the pace of development is always going to be much faster than the implementation of the rules and procedures for its use, as well as any accountability mechanisms. Due to rapid technological development, the legal framework for the security sector is constantly lagging behind, and therefore cannot fully capture the full breadth of technological advancements. This leads to a situation where either oversight is incomplete or security sector actors cannot fully use the potential of the new technologies. It is therefore important that legislation is developed in parallel with technological progress, in compliance with human rights norms and national obligations, so to ensure a safe, secure, confidential and resilient digital environment for the benefit of the population. Where technological development progresses faster than the implementation of legislative rules governing the use of digital technologies, the risk is that the deployment of these technologies will not be in line with human rights standards and protections. As noted by one expert, 'as human rights impact assessments are not (yet) mandatory prior to deployment in many countries, [the] lack of awareness of how to deploy a certain tool and/or faulty tools can seriously impact human rights'.[154] In this context, the experts were concerned about data protection and privacy. One expert observed that while individuals may voluntarily offer personal information to receive more personalized and customized services, concerns remain with regard to the protection of collected personal information and how this information is used by security sector actors.[155]

> *'The growth of digital space […] has meant that […] the ability of oversight mechanisms to hold security institutions and actors accountable has not kept pace with technical developments. Oversight and accountability mechanisms find themselves unable or slow to respond, feeding into an increasing suspicion of the legitimacy of the security sector actions when using emerging technologies.'*[156]

[153] Round 1, Response 4.

[154] Round 1, Response 4.

[155] Round 1, Response 4.

[156] Round 1, Response 10.

Instinctively, security services are guided by the premise that 'the end justifies the means'. The means offered to them by modern technological tools are on the precipice of a slippery slope towards potential violation of human rights. Many experts posited that governments have the main responsibility for enacting legislation governing the development and use of digital technologies by the security sector. One expert observed that while various actors are impacted and play a principal role in digitalization, the government remains primarily responsible for 'adopting and harmonizing a stable legislative and regulatory environment, by adopting operational plans for broadband, promoting standardization, and creating tools for safe use'. Nevertheless, experts also observed that the telecommunications entities have a big role to play in establishing adequate infrastructure and 'are an indispensable factor and actor to meet those needs'.[157] Another expert argued that it is important for the government to not only 'enact legislation governing how digitalization and its use is regulated', but also provide legislation specifically 'in critical domains related to national security and industrial policy'.[158] Similarly, another expert argued that 'any new digital tool implemented should go through a complete legislative process, to determine exactly what is the outcome, intern surveillance, budget, etc. It is the role of parliamentarians to conduct hearings of providers and users and to set clear objectives related to data protection, in accordance with the rule of law and human rights.'[159] The experts generally agreed that parliaments should take a lead role in adopting the rules and regulations overseeing the development and use of digital technologies in the security sector, while concurrently emphasizing the role of other security sector actors in supporting parliaments and its parliamentarians in this effort.

Another concern the experts identified centres around the political will and democratic capacity of all branches of government to undertake investigations where required and to enforce punitive and corrective measures where security agencies have violated laws. As highlighted by an expert, 'the level of political will and democratic capacity remains the most important for modern technologies to first help and "service" the legally prescribed needs of the security sector for internal control and supervision'.[160] It is necessary to ensure that differing political views on how the digital space is regulated are managed properly, and that laws are enforced impartially. Decisions of oversight actors should be binding, and in the process of reaching their decisions, oversight bodies should have 'constant, complete and direct access to the information and documents necessary to fulfil their mandate to exercise their legal power to initiate their own investigations'. In parallel, at the international level, more efforts are needed to design and adopt universally accepted legislation regulating digital space. For example, few states have ratified the Budapest Convention on Cybercrime.[161] As such, there is a gap in the legislation that states have adopted at the national level and the legal framework that exists at the international level. Consequently, as expressed by an expert, 'security actors can flexibly (mis)use unregulated territories to conduct their activities with impunity, in particular in cyberspace'.[162] This disparity at the national and international levels is further amplified by the differences in technological developments between states at the international level, which presents further challenges in ensuring that the gap does not progressively become even larger.

Overseeing the use of digital technologies

Oversight on the use of digital technologies by the security sector may be hampered by the *lack of technical knowledge* on the part of security sector overseers if they are unable to effectively interpret the information provided by security agencies, or even have the capacity to ask and frame the right questions. This could result in the need to acquire specialist knowledge, which may not always be possible due to budgetary constraints. Oversight bodies may have to maintain oversight of increasing volumes and diversity of digital evidence and surveillance tools, for which they may not always have the requisite knowledge or mandate. Consequently, it seems 'more likely that oversight and governance bodies will be less well equipped, and, in fact, governance and accountability will be in relative decline',[163] – one expert pointed to many oversight bodies reporting they had less access to technical expertise and capabilities in comparison to domestic security agencies. There is therefore a need for expert support of the oversight and control bodies (especially for parliament). Lack of technical knowledge

[157] Round 1, Response 1.

[158] Round 1, Response 3.

[159] Round 3, Response 1.

[160] Round 1, Response 1.

[161] Council of Europe, 'Convention on Cybercrime' (2022).

[162] Round 1, Response 2.

[163] Round 1, Response 5.

is a major recurring source of concern, which was previously examined in greater detail in Thematic area 2: Technical capacity.

> *'[…] digitalization allows more accurate and instant monitoring of activities of the security sector actors as they inevitably leave "traces" as they carry out their operations. Provided that relevant laws are clearly defined, in place, and made known to relevant parties, then compliance and accountability benchmarks can be set up against malicious behaviours.'*[164]

Nevertheless, digitalization can facilitate increased *accountability and oversight* in various ways. One expert suggested that security sector institutions could 'proactively build, for the benefit of its various constituents (parliamentary committees, select civil society organisations, etc.), databases or websites that will enable them to have access to information they may need to carry out their functions'.[165] By providing further technical support to security sector overseers, greater opportunities present themselves for improved access to security and justice. Another expert noted that digitalization could allow oversight authorities 'access, at regular but non-intrusive intervals, to have more instantaneous "on-site inspections" so as to check the level of compliance'.[166] The increased use of digital technology in security institutions could thus contribute towards reducing systematic corruption and mismanagement and thereby increase the productivity and effectiveness of security institutions.

Adopting standard operating procedures for conducting control and supervision over the security services – checklists, matrices, and reports that will be filled in, verified, and stored for further action – not only facilitates the work of professionals, but also minimizes the possibility of abuse. Political or individual pressure should also decrease, which thereby allows for more opportunities for objective oversight mechanisms and processes. In this vein, one expert argued that digitalization can 'standardize approaches to oversight of the security sector and provide uniform, impartial reporting standards for security sector personnel working at different levels in different regions of the state'.[167] As a result of technological developments, it is not possible to 'adjust digital standards for all services at once, [thereby] create the ability to collect responses to established standards, assess their compliance, analyse dynamics, and make a forecast for the future'.[168] As supervision and oversight of security sector actors become increasingly standardized as a result of streamlined digital processes, this shift will require the parallel development of a response capacity by security sector providers. To this end, the standardization of oversight processes through digital means will ensure that accountability mechanisms are not only predictable, but also able to promote further transparency in the security sector.

Managing actors and technologies

One of the main challenges is delineating the roles and responsibilities of security sector actors for providing or supporting digital security within societies, with one expert noting that 'for many institutions this is relatively new, and some have not internally integrated digital security in decision-making or within the structure of the institution'.[169] This therefore 'poses challenges to leadership […] and impacts the role of (public) institutions'.[170] In this context, one expert observed that 'impartial enforcement of laws is often easier said than done given inter-branch and bureaucratic politics, complex and onerous procedures, and the very fact that some individuals fall as victims of abuse by more powerful actors'.[171] In this context, the attribution problem in digital space can make it extremely difficult to identify the source of an action and the identity of the institution or individual responsible,

[164] Round 1, Response 6.

[165] Round 1, Response 11.

[166] Round 1, Response 6.

[167] Round 1, Response 14.

[168] Round 1, Response 6.

[169] Round 1, Response 2.

[170] Round 1, Response 2.

[171] Round 1, Response 6.

thereby hampering the work of security overseers and subverting the proper implementation of their control mechanisms.

> *'Digital security provision in many countries has grown into a confusing and overlapping patchwork of public institutions, private companies, and various other actors, making proper […] management more challenging.'*[172]

In many contexts, the media, CSOs, and independent thinktanks are key actors in ensuring accountability and oversight of security sector actors. While digitalization provides many tools and mechanisms for these actors to promote greater transparency and security provision, it nevertheless can also hamper their efforts. As noted by one expert, digitalization 'can also prevent an independent press – as the fourth estate – from shedding light on the actions of security providers. […] in many countries, whistle-blowers face a hostile legal and political landscape […].'[173] The challenges faced by human rights defenders and CSOs in holding states to account will be further examined in Thematic area 4: Human rights in the digital age. Nevertheless, it remains important to note that the diversity of actors involved in both the provision of security and its oversight makes it increasingly challenging to understand and navigate the existing framework of security provision, thereby fostering the risk of widening gaps in oversight.

There is thus a need to implement strategic partnerships ranging from academic and research institutions to corporate and technology experts, to ensure not only that technological development in all sectors is aligned, but also that oversight by the legislature proceeds at the same pace. In this vein, 'the response to the challenges in digital space can be successful only in the case of well-established procedures for cooperation between all stakeholders who can contribute to the field'.[174] Some governments may even develop specialized departments, agencies, or cross-departmental task teams to provide for the effective oversight of the security sector in a digital age. Some experts pointed to the development of national cyber security centres (NCSC) or national cyber emergency response teams (CERT) in this context.[175] Other experts thus noted that close cooperation is needed between the various entities of the security sector, 'which prevents the security structures from remaining closed until the end, primarily in the area of procurement and control and supervision (oversight) by various state entities and the civil sector'.[176] According to another expert, it is also possible that 'like-minded governments will increasingly share information on how to better enhance the accountability of the security sector in terms of digitalization'.[177]

Spotlight: Data regulation in the security sector

All experts participating in the current study unanimously agree that technological innovations are outpacing states' ability to keep abreast of the latest developments and their potential national security impact in terms of data protection. Most of the contemporary technological innovations are centred on the gathering, processing, and analysing of enormous amounts of data emerging from the multitude of digital devices and platforms. There are mounting concerns that these technologies and how they are used by security sector actors will pose serious challenges and new risks to public safety. Every day, interactions between humans and machines generate 2.5 trillion megabytes of data.[178] As data becomes more prevalent in contemporary societies, so does the temptation to use this data for national security. Big data is important for intelligence services, which have relied for a long time on multiple data sources to produce intelligence reports. In the past few decades, intelligence agencies across the world have institutionalized big data analytics through the development of specialized units and tools. Large data sets fed into AI software can detect patterns, identify anomalies, and provide insights that improve

[172] Round 1, Response 8.

[173] Round 1, Response 8.

[174] Round 1, Response 1.

[175] Round 1, Response 2.

[176] Round 3, Response 15.

[177] Round 1, Response 12.

[178] Van Puyvelde, D., S. Hossain, and S. Coulthart, 'National Security Relies More and More on Big Data. Here's Why', *The Washington Post* (2017).

situational awareness and support decision-making. For example, US intelligence services have used big data analytics to identify hostile activities of the Islamic State terrorist group.

However, the aggregation of large-scale data sets poses a risk of unauthorized access or misuse of sensitive information. Breaches or leaks of these data sets can expose personal details, financial information, or other sensitive data, leading to identity theft, blackmail, or other malicious activities. Additionally, the extensive collection and analysis of personal data can infringe on individuals' privacy rights. When individuals' online activities, communications, or personal information are continuously monitored and stored, it can create a chilling effect on free expression and undermine the right to privacy. Due to the sheer abundance of data, the line between national security and individual privacy is blurred by current data collection practices and regulations that fail to keep pace with the constantly evolving nature of digital technologies.

The technologies are mostly dual use, in the sense that they can be used as much to serve malicious or lethal purposes as they can be harnessed to enhance security provision and oversight, rendering efforts to manage and regulate them much more complex. This calls for a deeper understanding of the social, cultural, economic, and geopolitical contexts in which policy, norms, and regulations are crafted, as well as a firmer grasp of the overarching questions of power and conflict that shape humanity's relationships with technology.[179] Today's technological advances are deemed disruptive not only in market terms but also in the sense that they are provoking disruptions of legal and regulatory orders and have the potential to disturb the deep values upon which the legitimacy of existing social orders rests and on which accepted legal and regulatory frameworks draw. Complex, dynamic frameworks already govern some fields of technology. For instance, cyberspace is governed by an amalgamation of complicated political agreements, technical standards, certifications, protocols, trade and business standards, national regulations, and self-regulation in the private sector. All these legal and normative touchstones are underpinned by existing norms, values, and principles, yet they are neither binding nor universally accepted or recognized.

Digitalization makes it easier to process big data, enabling security sector actors to predict potential threats and find reasonable solutions. However, the experts have identified some challenges regarding data regulation in the security sector. First, experts state that the boundary between national security and individual privacy is blurred by current data collection practices. The sheer abundance of data is changing the nature of privacy in society and what constitutes 'intrusiveness' by security sector actors. As digitalization provides greater ease for security sector actors to collect information from citizens, with or without consent, the potential misuse of this data can create serious problems and damage the trust placed in security institutions. Second, in many states around the world, multiple data sets are regulated differently based on who collects the data, uses it, shares it, or stores it. This means that the same information can be collected in a variety of ways (for example signals intelligence, telecommunications data, application-based data collection, and digital advertising services) and regulated differently. Clearer universal regulations are needed to identify what data can be collected and for what purposes. Third, the security sector must preserve the data it gathers through relevant safeguards and regulations to avoid data leaks that can harm individual citizens and corporations, public organizations, and the national security of the entire state.

The experts highlight that proper data regulation can have beneficial effects for security provision and oversight. First, adequate regulation can improve internal processes of data analysis in the security sector and can reduce the intrusiveness of the data collection process, by identifying significant threats more quickly. Proper regulation would equip security sector actors with the legal framework to collect well-targeted data from social media platforms without infringing any privacy rights. Second, data regulation can equip security sector actors with the means to protect human rights by mitigating potential data leaks. At the same time, data regulation would provide more visibly to the security sector in the field of human rights protection, which would help to generate social trust and allow law enforcement to respond objectively and transparently to any requests. Third, proper data regulations would improve the accountability and transparency of security sector actors with the public as well as with other security institutions and stakeholders.

[179] Kavanagh, C., 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?' (Washington, D.C.: Carnegie Endowment for International Peace, 2019).

Security sector actors and their oversight

The experts participating in this research have underlined the various legal lacunae with regard to how traditional security sector actors can or should use digital technologies, further stressing the need to create and adopt regulations that can keep pace with technological developments. In this case, the experts agreed that governments have the opportunity to develop a stable legislative and regulatory environment, by adopting operational plans for promoting standardization, and creating tools for safe use both for security sector actors and the wider public. Executive and government ministries can enact better regulation of big tech companies and ensure proper legislation of government agencies, actors, and intelligence services, as well as work towards decreasing the politicization of digital space. As one expert argued, 'the digital space is non-kinetic in nature, it is the responsibility of governments to enact relevant legislation'.[180] The experts also suggested that government ministries and oversight bodies could regularly review and reassess the conduct of security providers to ensure that relevant laws and procedures were being followed and that any misuse or abuse of power was prevented and subject to disciplinary actions.

Experts argued that digitalization is a new development for many security sector institutions and some institutions – such as the government or parliament – have not internally integrated digital security in decision-making. Digitalization and digital security are, instead, a boardroom topic. So, it is a challenge to decipher what role the government has in protecting the public sector. There are currently various approaches, for instance the development of national cyber security centres (NCSC) or national cyber emergency response teams (CERT). As such, experts claimed that parliaments and their specialized committees have a critical role to play in ensuring that there is a suitable legal framework regulating the digital space. Experts added that it is important that this legal framework keeps pace with technological developments and emerging cybersecurity challenges. This means that parliaments are in a position to recruit technologically capable personnel, develop and implement new investigation methods, and upgrade their own technological capacities to anticipate future challenges. More precisely, parliamentarians can receive training on the challenges posed by cybersecurity for them to ensure that the institutions responsible for combating abuses and crimes committed in the digital arena are able to respond to and anticipate emerging cyberthreats.

In parallel, the experts suggested that big tech companies are in a position to facilitate the development of legislation and digital technologies by cooperating with the security sector to define common standards and set up proper legal frameworks. As big tech companies hold vast amounts of data on civilians and CSOs, these actors can inform the security sector on best data protection methods and practices, upholding rule of law and human rights norms. The lack of guidance on the use of digital tools for security provision activities, however, poses serious risks for human rights standards.

Recommendations: Regulation and oversight

In terms of regulation and oversight, the following three recommendations were developed by synthesizing the insights shared by the experts participating in the current study, as presented in the previous sections:

1. Security sector actors should work in collaboration across the whole sector to ensure the creation of a stable legislative and regulatory environment that keeps pace with and governs the development and use of digital technologies within the security sector.
2. Security sector institutions should proactively standardize oversight approaches and provide uniform, impartial reporting standards to ensure that the principles of good security governance are applied to the oversight of digital technologies.
3. Establish strategic partnerships and cooperation with various stakeholders, including academic and research institutions, corporate entities, and technology experts, to ensure participation.

Thematic area 4: Human rights in the digital age

Digital technologies have considerably contributed to the reshaping of the civic space. The internet and other digital communication tools offer numerous opportunities for promoting the right to freedom of opinion and expression, or to reach a wider audience, including traditionally disenfranchised or marginalized communities, through safe online spaces. There is a general, broad consensus that the same human rights and obligations that

[180] Round 1 Response 6.

apply offline also apply in the digital environment. However, new technologies are creating a fundamentally different paradigm for human interaction, and the current international human rights framework has conceptual gaps when it comes to digital space. As stated by an expert, 'digitalization, AI, and other new technologies hold great promise, but need to be paired with ethical oversight to ensure they don't exacerbate social inequality or lead to human rights violations. We must fully renew the international human rights obligations of states to meet these challenges and overcome the lag of socio-political and legal global processes.'[181]

Nevertheless, mass surveillance, technological biases, digital authoritarianism, hate speech, and disinformation are all developing at an alarming pace. The emergence of AI, facial recognition systems, and social media platforms have substantially expanded the toolkit available for social control. Ubiquitous data collection and data-processing systems allow for accurate and broad tracking and profiling of citizens through the mass collection, analysis, and sorting of data, allowing governments to achieve both granularity and scale in their surveillance operations. Armed with this capacity, authoritarian regimes can more easily stem offline and online dissent and target surveillance at specific groups. Along these lines, one expert participating in this study claimed that 'digitization alone will not solve the problem of placing human rights first in security provision. […] It can be assumed that human rights standards will change under the influence of digitalization, which will inevitably invade people's personal space and privacy. Digitalization will provide greater control over the population, and it will make it possible to predict the behaviour of individuals or communities.'[182] In parallel, another expert added that 'it is a state's obligation to protect and promote human rights and ensure oversight of the security sector. All three concepts – human rights, digitalization, and the security sector – are the domain of the state.'[183]

From this point of view, there is an opportunity for the state to increase the confidence of citizens by ensuring that the security sector does not prejudge its competence in either preventive or repressive measures using digital technologies. Special authorizations (as in the case of the use of force) must be reasonably necessary, proportionate, and subject to circumstances, while the use of big data analysis must be cautious and in accordance with jurisdiction. As stated by an expert, 'there is a thin line between getting the information needed to prevent a big security risk, or not to use technology if there is a potential to overstep regulations and disrupt human rights'.[184] The digitalization of the security sector has increased the pressure to properly balance human rights with the obligation and duty of states to protect their citizens. As such, the experts participating in this study have unanimously agreed that the role of security sector actors and institutions in using digital technologies while upholding human rights is a delicate yet crucial balance that requires careful consideration, ethical principles, and effective governance to avoid any form of abuse.

This fourth thematic area examines the human rights implications of the security sector's digitalization process. The experts analysed different challenges that touch existing human rights norms and principles and provided recommendations for security sector actors to address challenges going forward. The research team has narrowed the disparate strands into three main sub-areas, namely (1) the growth of mass surveillance; (2) the emergence of digital authoritarianism; and (3) the damaging effects of disinformation campaigns on security sector actors, institutions, and human rights. The following sub-sections will expand on these areas and integrate the converging viewpoints provided by the experts. In addition, a spotlight section will provide additional insights into the technological biases found in the digital technologies used by security sector actors, before examining how security sector actors ensure they respect human rights in the digital age.

Mass surveillance

There is broad consensus among the experts that digitalization poses a wide spectrum of risks to human rights protection. As a starting point, there are many issues relating to data protection and privacy, control over one's digital identity, and the use of mass surveillance technology, to mention a few. Oftentimes, the legislation for digital technologies is substandard and undermines privacy rights, especially within the context of mass surveillance conducted by security agencies to accumulate vast amounts of private information and exploit metadata for investigations. Mass surveillance can be briefly defined as a process that uses systems or technologies that collect, analyse, and/or generate data on indefinite or large numbers of people instead of limiting surveillance to

[181] Round 1, Response 9.

[182] Round 1, Response 14.

[183] Round 1, Response 9.

[184] Round 1, Response 9.

individuals about whom there is reasonable suspicion of wrongdoing. Under currently available forms of mass surveillance, governments can capture virtually all aspects of their citizens' lives. As highlighted by an expert, 'the recently developed ability of security agencies to exploit surveillance data is also likely to afford them opportunities to establish the infrastructure of an overreaching police state apparatus that will undoubtedly become a challenge to a rule of law state. This will result in a pressing need to enact specific safeguards that security actors must respect.'[185]

> *'To ease tensions concerning the protection of human rights, [security sector actors] must act professionally, legally, and with the ability to explain their actions. Policymakers must ensure that surveillance is used to the minimal possible extent and in accordance with the legislation. At the same time, policymakers must draft legislation that is understandable to the public and effective to mitigate potential abuses of human rights.'*[186]

In an age where insecurities are even more pervasive, countries often resort to national security arguments to deliberately foreswear or ignore their obligations to human rights. Security services are often guided by the premise that 'the end justifies the means' whereby the means offered to them by modern technological tools lie on a very thin line regarding violation of human rights. There are also major discrepancies between legal provisions for human rights protections and the capacity of the security sector, specifically security overseers, to provide such protections. Violations can include illegal wiretapping, monitoring without warrants on the pretext of imminent threats, or intrusion of private space without targets knowing, such as hacking into private emails, as well as misuse of collected information specific for certain purposes.

For example, the 2013 Snowden revelations detailing how the United States National Security Agency (NSA) was able to collect anyone's personal data via mobile phones, laptops, browser history, Facebook, and other digital communication platforms, represents an instance of global mass surveillance. All this information allowed the NSA to build what it called 'a pattern of life', which is 'a detailed profile of a target and anyone associated with them'.[187] When media worldwide began to dig deeper into the 'Snowden documents', they brought to light the existence of extensive global surveillance programmes by intelligence services. The sheer magnitude of these revelations remains unprecedented, potentially affecting people's privacy around the world even today. Surveillance no longer merely targets state or business secrets but allows for the interception of people's communications on a large scale. This interferes both with the respect for private and family life of individuals and with the right to privacy and data protection. In this instance, one expert argued that 'as societies increasingly progress in the adoption of digital technologies, there are bound to be "systemic shocks" in the way some security actors employ digital tools. […] Policymakers should be better prepared in this regard, focusing on anticipating the effect of adopting new surveillance practices on public opinion.'[188] Another expert added that due to the increasing 'use of facial recognition and other biometric technologies, as well as the automatic gathering of metadata, human rights need to catch up with the contemporary digital reality'.

The availability and accessibility of information and knowledge in the digital age will bring about challenges for the security sector itself. One of these challenges will involve ensuring the legitimate protection of sensitive and confidential defence- and security-related data. While transparency is indeed a value in a democratic setting, digitalization may, in some cases, jeopardise confidential information that can be more easily hacked by adversaries and prone to be leaked on the dark web. Further, wide access to information will also make it more difficult for security institutions to safeguard the secrecy of sources, means, and methods that security sector actors usually rely on to carry out their missions. Another challenge associated with the availability and accessibility of information in the digital age is the increased ability of ordinary actors to manipulate information and harm security sector actors or thwart efforts to reach the legitimate goals of the security sector. The digital exchange of personal data between countries, especially with regard to visas, no-fly lists, and other cases of concern, needs to be streamlined and improved within human rights frameworks. In this vein, there are also

[185] Round 1, Response 11.

[186] Round 3, Response 5.

[187] Macaskill, E. and G. Dance, 'NSA Files: Decoded. What the Revelations Mean for You', *The Guardian* (2013).

[188] Round 3, Response 15.

‘questions surrounding datafication (i.e. data collection, aggregation and use about human activities) by big tech companies, for it provides greater levels of monitoring, surveillance, and targeting capabilities to a range of new actors, as well as the data being available to traditional security actors either through judicial processes or for purchase’.[189]

China’s social credit system is another example of a mass surveillance society system. Unveiled in 2014, China’s social credit system expands the idea to all aspects of life, judging citizens’ behaviour and trustworthiness. An expert argues that ‘many states will (attempt to) adopt the “social credit” system, which China is actively promoting in the world today. It allows uniting the security management information system into a single network, including the criminal information system, the border control system, the traffic control system, and the country management system for senior leaders. Such a system is likely to be able to ensure maximum compliance with the law in the country with a rather low regard for human rights in respect of privacy.’[190] Another expert adds that ‘even though such a multilayered system provides a high level of security, many democratic states are not ready to implement it in their country, because they believe that it violates human rights. However, the development of information technology is forcing even such states to gradually move towards increasing control over the population. Each society will have to decide to what extent state control over the population is acceptable, based on its political, cultural, and other social values.’[191]

One expert warns of the dangers associated with such a ‘social credit’ system: ‘new tensions will arise between human rights and the introduction of new surveillance and law enforcement powers, especially given a continued increase in political radicalization and extremism. Key norms – such as those surrounding data privacy – will evolve considering ever more intrusive digital technology, for instance regarding the use of medical and/or biometric data. Yet, authoritarian centralised political systems might have an “advantage” over those in which the centralised collection, processing and use of data is restricted by standards, laws, and institutions. The attraction of a “technology-backed state”, also known as “digital authoritarianism”, must not be underestimated. […] For societies without traditional, well-established relationships of trust, total surveillance combined with social credit systems of the kind currently being tested in China is an attractive opportunity to establish a functioning community without “troublesome” elements of democratic participation and – particularly – the rule of law. This could further undermine the latter globally.’[192]

Digital authoritarianism

Drawing upon the previous section, many experts stressed the fact that ‘governments can use digitalization to deliberately target certain segments of the public or individuals due to their dissent in political opinions or certain beliefs, either religious or political. This is typically the practice in authoritarian state[s]’.[193] Another expert added that ‘there is a huge risk that digital tools are being used to defend the interests of authoritarian regimes’.[194] As such, more states are deploying sophisticated mass surveillance tools through security institutions, and authoritarian leaders are consolidating their rule by employing digital authoritarian strategies that foster their disillusionment. In this instance, one expert argued that ‘approaches to protect human rights will need to be updated; for example, a multistakeholder approach and public-private partnerships may be more effective for the security sector to work for human rights protection. As technology develops rapidly, there should be an established mechanism to regularly analyse the impact of digitalisation in order to make sure that its further development will not jeopardise human rights.’[195]

[189] Round 1, Response 5.

[190] Round 1, Response 14.

[191] Round 1, Response 14.

[192] Round 1, Response 8.

[193] Round 1, Response 6.

[194] Round 3, Response 1.

[195] Round 1, Response 13.

'[…] the resilience of democratic actors to digital authoritarianism is crucial; without this resilience, countries that are increasing controls on their citizens, expanding their reach abroad, and exporting the tools and tactics of digital authoritarianism today could become the national security concerns of tomorrow.'[196]

Digital authoritarianism can be broadly defined as governments' use of digital information technologies for purposes of social control, repression, and surveillance, as well as enforcing a system of beliefs. Digital authoritarianism repression comprises six techniques: surveillance, censorship, social manipulation and harassment, cyberattacks, internet shutdowns, and targeted persecution against online users.[197] These six techniques are not mutually exclusive. Many governments increasingly allow security sector actors to employ sophisticated digital tools, such as spyware technologies and censorship strategies complemented by expansive 'fake news' statutes that give authorities unbridled discretion to persecute political opponents and civil society activists. When all else fails, states are willing to pull the plug on internet access and plunge their populations into digital isolation for extended periods. This practice is considerably problematic and challenging from a human rights perspective, needing to be thoroughly monitored by oversight bodies. According to a recent statement from the United Nations Office of the High Commissioner for Human Rights (OHCHA), in the past two years alone more than 60 countries around the world have adopted or plan to introduce legislation regulating social media use.[198] For example, Russia and Iran have introduced restrictive media laws applying to social media users, 'designed to curb fake news', and have blocked most foreign media and communication services.[199]

In addition, some authoritarian states have been increasingly drawn to the capabilities of spyware applications, allowing them to exert control over their populations in ways previously unimaginable. These governments often use spyware to stifle political opposition, gather intelligence on perceived threats, and maintain tight control over the flow of information within their borders. Spyware refers to software designed to infiltrate and monitor the activities of a target's device, often without their knowledge or consent. For example, the Pegasus spyware, developed by the Israeli company NSO Group, is one of the most notorious examples of spyware used by authoritarian states.[200] Pegasus has gained notoriety for its advanced capabilities, allowing it to compromise a wide range of devices, smartphones, or tablets, in particular. It operates by exploiting vulnerabilities in the target's device, often through phishing attacks or malicious links, and then gains full access to the device's data, communications, and even its camera and microphone.[201]

This level of intrusion has far-reaching implications, as it enables authoritarian states to monitor political dissidents, human rights activists, and journalists, undermining freedom of speech and press freedom, while allowing these governments to identify and suppress opposition movements before they gain momentum. For example, it was revealed that the Mexican government had allegedly used Pegasus to target journalists and activists critical of the regime, while the murder of journalist Jamal Khashoggi raised suspicions of Saudi Arabia's use of Pegasus in monitoring and targeting critics of the regime.[202] As stated by an expert participating in the current study, 'the security sector will have to guarantee that they respect human and civil rights in digital space, by countering major threats, such as data leaks, cyber-espionage, and disinformation'.[203]

[196] Round 3, Response 9.

[197] Feldstein, S., 'When it comes to Digital Authoritarianism, China is a Challenge – But Not the Only Challenge', *War on the Rocks* (2020).

[198] United Nations Human Rights Office of the High Commissioner, 'United Nations Human Rights Report 2022' (2022).

[199] Ibid.

[200] Pegg, D. and S. Cutler, 'What is Pegasus Spyware and How Does It Hack Phones?', *The Guardian* (2021).

[201] Ibid.

[202] *The Washington Post*, 'A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months Before His Murder, New Forensics Show' (2021).

[203] Round 3, Response 8.

Disinformation campaigns

The proliferation of digital technologies has exacerbated the growing trend of disinformation, posing a massive challenge to human rights. Disinformation can be defined as the deliberate and intentional spread of false news with the aim of manipulating public opinion, interfering with democratic processes, and causing harm to individuals.[204] It is not an easy task to always identify disinformation for what it is. Sometimes, information is completely made up; other times, it is intentionally taken out of context, exaggerated, or with essential information omitted. Disinformation can be spread in multiple formats, be it text, images, videos, and other multimedia content. The actors engaged in disinformation range from malicious individual actors, state-financed cybercriminal groups, and even states via their national security sector. As stated by an expert, the 'awareness about vast possibilities of spreading disinformation on social media and other channels in order to mobilize mass movements needs to be further documented. Policymakers should pay more attention to disinformation practices and hate speech, and demand regular estimates and reports by security sector institutions about such potential events and developments.'[205] Along the same lines, another expert adds that 'the increased ability to manipulate information can lead to damaging effects that harm the legitimacy of security actors or thwart their efforts to reach legitimate national security goals'.[206]

> *'… disinformation […] can be misleading, and even incite to violence. Yet, while new technologies facilitate the spread of false information, digitalization can equip security actors with the tools to contain and combat disinformation campaigns.'*[207]

Disinformation campaigns often target marginalized and vulnerable communities, exacerbating discrimination and having devastating effects on freedom of expression and access to information. An expert highlighted that 'the government's use of data for surveillance, profiling, disinformation, and media manipulation raises urgent new concerns for digital governance and democracy. The rapid pace of technological change makes the need for further research in digital work and frontier technologies an ongoing priority.'[208] Another expert claims that 'access to information and freedom of speech are some of the most contentious human rights violations and a prime example. Societies all around the globe struggle with striking the right regulatory balance between guaranteeing freedom of expression in the digital sphere on the one hand and enforcing existing laws against hate speech or the dissemination of false information with malicious intent on the other. A key question in this regard is about the responsibility and identity of platform providers – are they merely tech companies providing communication infrastructure, or have they evolved into media companies responsible for the online content they host on their platforms?'[209]

For example, in Myanmar, the military's use of disinformation on social media platforms contributed to the fuelling of hatred towards the Rohingya Muslim minority. The military exploited Facebook's wide reach in Myanmar, where it is broadly used by the country's 18 million internet users.[210] According to Amnesty International and *The New York Times*, actors linked to the Myanmar military and radical Buddhist nationalist groups flooded the platform with anti-Muslim content, posting fake content portraying the Rohingya as 'invaders'.[211] After months of reports about anti-Rohingya propaganda, Facebook acknowledged that it had been too slow to act in Myanmar. More than 700,000 Rohingya had fled the country in a year, in what UN officials called 'a textbook example of ethnic cleansing'.[212] The consequences were catastrophic, with lives that were disrupted and entire communities

[204] Fallis, D., 'What Is Disinformation?', *Library Trends*, Vol. 63: No. 3 (2015), pp. 401-26. Available at: https://muse.jhu.edu/article/579342

[205] Round 1, Response 13.

[206] Round 1, Response 11.

[207] Round 1, Response 13.

[208] Round 3, Response 9.

[209] Round 1, Response 8.

[210] *The New York Times*, 'A Genocide Incited on Facebook, with Posts from Myanmar's Military' (2018).

[211] Ibid.

[212] *UN News*, 'UN Human Rights Chief Points to "Textbook Example of Ethnic Cleansing" in Myanmar' (2017).

displaced, underscoring the grave implications of disinformation campaigns. As another example, an expert highlighted that 'in South Korea, the ruling Democratic Party attempted to enact the Press Arbitration Act to punish accredited media outlets for intentionally publishing false information'. According to the expert, this is a 'deplorable attempt to gag the media [and] is considered a severe threat to the liberal democracy of South Korea'.[213]

Efforts to counter disinformation within the security sector must prioritize the protection of human rights. This entails strengthening legal frameworks that safeguard freedom of expression, supporting independent journalism, and promoting digital literacy to equip citizens with critical thinking skills. Moreover, security sector institutions themselves must commit to transparency, accountability, and respect for human rights, fostering an environment where disinformation has no place and where rights are upheld even in the most challenging security contexts. In doing so, we can ensure that disinformation does not become a tool for oppression but rather a force that is countered through the promotion of human rights and democratic values. However, an expert stated that digitalization enables the security sector actors with technological tools, such as AI and machine learning, 'to better protect human rights by removing potential risks, for example, to shift through the millions of posts generated each day to identify and remove "hate speech", propaganda, or disinformation online'.[214] As such, safeguarding human rights in the face of disinformation is not just a matter of principle; it is imperative for the preservation of democracy, the protection of vulnerable communities, and the dignity of all individuals. This approach recognizes that the battle against disinformation is intimately linked to the broader struggle for human rights and the values that underpin democratic societies.

Spotlight: Technological biases and their impact on human rights

Technological biases, stemming from algorithmic decision-making, profiling, and surveillance, can have a significant impact on human rights within the security sector. Algorithms employed in various security applications, such as facial recognition or predictive policing systems, are trained on data that may reflect historical discrimination or societal prejudices. As a result, these algorithms can perpetuate existing biases and inadvertently discriminate against certain groups. This violation of the principle of equal treatment erodes human rights and widens social inequalities. Moreover, relying solely on automated systems without proper human oversight can lead to false positives or false negatives, potentially undermining individuals' rights to fair treatment and due process. In Germany, concerns have been raised about the potential biases in algorithmic decision-making systems used by law enforcement agencies.[215] Predictive policing algorithms have been criticized for perpetuating biases present in historical crime data, leading to over-policing in certain areas and potential profiling based on characteristics such as ethnicity or socio-economic status. These biases raised significant concerns about fairness, equal treatment, and the potential violation of human rights, to the extent that the German Federal Constitutional Court declared the use of the Palantir predictive policing and surveillance software by law enforcement forces in Hesse and Hamburg unconstitutional.[216]

Profiling individuals based on race, ethnicity, religion, or gender can result in discriminatory practices that violate human rights. Such profiling can lead to the targeted surveillance, enhanced scrutiny, or invasive security measures disproportionately affecting marginalized communities. The reliance on technology-driven profiling undermines the principles of equality, non-discrimination, and the presumption of innocence, and may exacerbate societal divisions, and the extensive use of advanced surveillance technologies raises significant privacy concerns. Mass surveillance programmes, pervasive monitoring systems, and the collection of personal data without proper consent or oversight encroach upon individuals' right to privacy. Widespread surveillance has a chilling effect on freedom of expression and association, inhibiting individuals from fully exercising their rights. The erosion of privacy rights within the security sector is incompatible with democratic principles and human rights standards. For example, journalists and human rights defenders from countries such as Bahrain to Morocco have their phones tapped and their emails read by security services.[217] Facebook takes down wall posts after states complain of 'subversive material'.[218] Google hands over user data to law enforcement authorities that includes IP addresses,

---

[213] Round 1, Response 3.

[214] Round 1, Response 13.

[215] Killeen, M., 'German Constitutional Court Strikes Down Predictive Algorithms for Policing', *Euractiv* (2023).

[216] Ibid.

[217] Privacy International, 'Two Sides of the Same Coin – the Right to Privacy and Freedom of Expression' (2018).

[218] Ibid.

location data, and records of communications.[219] The US government conducts mass surveillance of foreign phone and internet users.[220] Each of these acts threatens both an individual's freedom to express themselves and their right to maintain a private life and private communications.

In the US, studies have shown that facial recognition technologies used by law enforcement agencies exhibit bias, particularly against people of colour. For example, a study by the National Institute of Standards and Technology (NIST) found that facial recognition algorithms had higher rates of false positives for Asian, African American, and Indigenous individuals compared with white individuals.[221] This bias can lead to discriminatory outcomes, contributing to racial profiling and potential violations of civil rights. In parallel, the use of predictive policing algorithms in the UK has raised concerns about bias and discriminatory practices. A report by the human rights organization Liberty highlighted how such algorithms can perpetuate existing biases and disproportionately target marginalized communities.[222] The algorithms rely on historical crime data, which may reflect biased policing practices and over-policing in certain neighbourhoods, leading to a cycle of discrimination and disproportionate surveillance.

Technological biases in the security sector can infringe upon the freedom of assembly and protest. Crowd monitoring and control technologies, such as facial recognition or social media monitoring, pose risks to these fundamental rights. The excessive use of surveillance technologies to monitor peaceful demonstrations can intimidate participants, create a climate of fear, and deter people from engaging in legitimate forms of protest. Preserving the freedom to assemble and protest is essential for the healthy functioning of democratic societies and the protection of human rights. Transparency and accountability are vital in addressing technological biases and upholding human rights in the security sector. However, the opaqueness of security technologies and the algorithms behind them hinders the ability to assess their accuracy, fairness, or potential biases. The lack of transparency obstructs individuals' capacity to challenge decisions that may affect their rights. To ensure accountability, rigorous testing, auditing, and independent oversight of security technologies should be implemented. Public disclosure of methodologies and audit outcomes fosters transparency and enables individuals to hold security sector actors accountable.

Addressing these biases requires a comprehensive approach that combines ethical frameworks, data quality, transparency, and legal protections. By integrating fairness, non-discrimination, and respect for human rights into the development and deployment of security technologies, biases can be mitigated. For example, researchers at Stanford University used natural language processing to analyse how police officers spoke to people they stopped on the street.[223] This AI program was incorporated into police body cameras in test groups. Security technology like this can help enforce the fair treatment of everyone law enforcement interacts with, ensuring that all community members are treated equally and that human rights are upheld.[224] Safeguarding privacy, protecting against profiling, and preserving the freedom of assembly and protest are essential for upholding human rights in the face of technological advancements. By striking a balance between security objectives and human rights principles, we can build a more inclusive, equitable, and rights-respecting security sector.

To mitigate biases in security technologies, the experts participating in this study stressed that it is crucial to ensure that the data used for training algorithms is diverse and representative of the population. This can involve collecting data from a wide range of sources and taking steps to address underrepresented groups or marginalized communities. By ensuring diverse data inputs, algorithms can have a better chance of producing fair and unbiased outcomes. Moreover, regular testing and evaluation of security technologies are essential to identify and rectify biases. Independent auditing and evaluation by experts can help uncover potential biases and assess the fairness and accuracy of algorithms. It is crucial to have transparent and standardized testing methodologies that measure the impact of technologies on different demographic groups. Incorporating ethical design principles into the

---

[219] Ibid.

[220] Ibid.

[221] National Institute for Standards and Technology, 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software' (2019).

[222] European Union Agency for Fundamental Rights, 'Bias in Algorithms – Artificial Intelligence and Discrimination' (2022).

[223] Voigt, R., et al., 'Language From Police Body Camera Footage Shows Racial Disparities in Officer Respect' (2017).

[224] Knight, W., 'If Done Right, AI Could Make Policing Fairer', *WIRED* (2020).

development of security technologies can help minimize biases. This includes promoting transparency, accountability, and fairness as core principles throughout the design and implementation process. Engaging diverse stakeholders, including CSOs and impacted communities, can contribute to more inclusive and ethical design practices. While automation can offer efficiency, human oversight and decision-making are essential to ensure the fair and just use of security technologies. Human intervention can provide checks and balances, addressing cases where biases may emerge and ensuring that individual rights are respected. Human experts should be involved in reviewing and validating algorithmic decisions to prevent unfair outcomes.

At the same time, the experts participating in the study highlighted that promoting digital literacy and providing training on the use and implications of security technologies are crucial for security personnel and the public. Education and training programmes can raise awareness about biases, foster critical thinking, and enable individuals to understand and challenge discriminatory practices. This empowers individuals to assert their rights and hold security sector actors accountable. Robust legal and policy frameworks are essential to guide the development and use of security technologies. Governments should establish clear regulations that prohibit discriminatory practices and ensure accountability. Privacy laws, data protection measures, and anti-discrimination legislation can provide a legal basis to safeguard human rights and address biases in the security sector. By adopting these different strategies and working towards a multi-stakeholder approach that involves governments, technology developers, CSOs, and impacted communities, it is possible to address and improve technological biases in the security sector. This ensures that security technologies are deployed in a manner that respects human rights, promotes fairness, and enhances public safety.

Security sector actors and human rights

The experts participating in this research have assessed how security sector actors employing digital technologies have an impact on human rights. For example, the experts stated that, to ensure national security, intelligence agencies have become more invasive. Such behaviour may be accused as infringing upon the privacy of citizens. Moreover, the use of facial recognition and other biometric technologies, as well as the automatic gathering of metadata, can lead to violations of human rights when and where they are used without the consent of individuals concerned. Human rights protection needs to catch up with the digital contemporary reality. The same applies to law enforcement. Experts suggested that law enforcement will be required to maintain a proper balance between the need to access and use information they can obtain and the systems they possess to examine massive data sets, as well as the proper handling, differentiation, and protection of information to ensure privacy and improve human rights. At the same time, the experts highlighted that judicial authorities could play a critical role in interpreting harmful online content and create inclusive procedures of the law respecting universal human rights, indicating how laws are enforced, setting precedents, and overturning government decisions where there is discrepancy with or contravention of existing laws. The judicial branch can bring about course correction as well as preventing abuses of power by security sector actors, so to uphold the rule of law.

The same actors added that in terms of emerging actors, big tech companies must adopt a ‘do not harm’ policy towards all users and security sector actors. They can provide effective technology that empowers citizens to learn about their rights and can conduct training, collect appeals from representatives of minorities and citizens on human rights violations on the web, and publish data on complaints received and on measures taken to correct these deficiencies. Big tech companies can leverage digital technologies to reach out to marginalized communities and enable them to become part of the digital space, and big tech can also play a major role in educating and training the marginalized sections to identify harmful online content and understand the opportunities that are available to them by opening the doors to greater mobility, development, and changes in life for those who have been discriminated against and left behind by social and political systems.

Recommendations: Human rights

In terms of human rights in the digital space, the following three recommendations were developed by synthesizing the insights and opinions of the participating experts, as presented in the previous sections:

1. Security overseers should enact safeguards based on legal and ethical guidelines to ensure that security providers respect privacy rights when conducting any form of mass surveillance.
2. Security sector actors should adopt a multi-stakeholder approach and collaborate with public organizations and the private sector to enhance the protection of human rights to avoid any form of digital authoritarianism.

3. Security sector actors should strengthen legal frameworks, support independent journalism, promote digital literacy initiatives, ensure transparency and accountability within security institutions, and utilize emerging technology (such as AI) to protect human rights in the face of disinformation.

Thematic area 5: Digital divide

One of the most pressing concerns in today's increasingly interconnected world is the digital divide, which can be broadly defined as the discrepancies between individuals with or without access to digital technologies. However, the digital divide is multifaceted, including many factors such as access, affordability, and quality. It is considerably influenced by other social factors, such as literacy levels, gender, income, urban vs rural, and religion, to mention just a few. According to a recent report from the International Telecommunications Union (ITU), in 2022, only 36 per cent of individuals in 46 developing countries were using the internet, in comparison to the 87 per cent of users in developed countries.[225] It is estimated that nearly 2.7 billion people are not connected to the internet.[226] These figures suggest that universal and meaningful connectivity – the possibility for all individuals to enjoy a safe, productive, and affordable online experience – remains a distant prospect for certain populations. Limited internet access, inconsistent connectivity and electricity supply, alongside low digital literacy and education levels, all contribute to increasing exclusion of already disadvantaged groups and communities.

As everything goes online today, those who wish to but cannot get information are therefore situated in a socially disadvantaged position where they cannot make their needs heard. Governments rarely translate official documents into languages that are used by marginalized populations, and hence digitization will likely further contribute to exacerbating such marginalization. In this vein, it is known that access to technology is not equal between men and women in all countries, with women less likely than men to have mobile internet access due to a lower average income. As girls have less access to education than boys, they are more likely to be more illiterate, thus their ability to take advantage of online resources is reduced. For example, when measured in terms of internet use, the digital gender gap in developing countries remains rather significant, with no sign of narrowing. In 2022, 43% of the male population in developing states was online, in comparison to only 28% of the female population.[227] As for developing states, a discrepancy can still be observed: 70% of the male population has access to the internet, compared to only 63% of the female population. An expert highlighted that the 'inaccessibility to digital technologies, especially in the developing world, can be a tool for authoritarian governance. […] One cannot talk about a reformed security sector with limited access to digital technologies and raising awareness of possible threats. In an increasingly digital world, all individuals should be able to use digital technologies to access health and education information, financial inclusion, and digital pathways to economic and political empowerment.'[228]

As for the impact of the digital divide on the security sector, an expert participating in the research mentioned that 'it negatively impacts the overall digitalization process and the access to digital technologies to provide equitable security services'.[229] As stated by another expert, 'the impact of the digital divide on the digitalization process initiated by security sector actors in developing states will affect citizens differently, depending on their circumstances. […] Some individuals will risk increasing profiling and harassment in these spaces while being excluded due to the lack of infrastructure. Unethical use of data could see exclusionary and discriminatory practices applied to marginalized groups. Individuals not equipped with appropriate technology or access to data, connectivity, or electricity will be disadvantaged in accessing services increasingly made available online.'[230] Moreover, the increasing pressure on the digitalization of the security sector will result in institutions that are able to keep up with the pace of the constantly evolving digital landscape and those who are not. The digital divide prevents some security providers and overseers in other parts of the world acquiring equitable access to digital

[225] International Telecommunication Union, 'Digital inclusion of all' (2022).

[226] Ibid.

[227] International Telecommunication Union, 'Internet Use' (2022).

[228] Round 3, Response 9.

[229] Round 1, Response 15.

[230] Round 1, Response 10.

technologies, posing a significant problem that may weaken the transparency of decision-making processes for security sector actors.

The final thematic area focuses on the digital divide in our societies and explores how the security sector can address this gap through digitalization. The experts analysed different patterns and issues further deepening the existing digital divide and provided recommendations for security sector actors to address challenges going forward. The research team has narrowed the disparate strands into three main sub-areas, namely (1) closing the digital literacy gap; (2) ensuring citizen participation in the security sector and access to information; and (3) implementing a gender-sensitive approach to security provision and oversight. The following sub-sections will expand on these areas and integrate the converging viewpoints provided by the experts. In addition, a spotlight section will provide additional insights into the role digital communication platforms can play in closing the digital divide, before examining the impact the existing digital divide has on security sector actors.

Closing the literacy gap

Digital literacy concerns all nations and regions across the globe to a varying degree. It encompasses the ability to find, evaluate, and use digital information in an effective and responsible manner. While the speed of digitalization in the last couple of decades has improved the living standards and conditions for a variety of individuals living in various geographies across the globe, there are still some groups of people who are left outside the current wave of innovation. This shows that the rapid evolution of technology often outpaces individuals' ability to keep up. The security sector itself is experiencing this challenge and it has a crucial role to play in addressing digital literacy. As stated by an expert, 'digital technologies change rapidly, leaving those who cannot catch up with these changes behind. Thus, digital literacy (the ability to acquire and understand information) and digital poverty have been significant social issues in recent times.'[231] Another expert added that 'keeping in mind that already disadvantaged groups are overrepresented in the offline population, which is disproportionately female, rural, poor, composed of older persons, and/or with limited education and low literacy levels, security sector actors in cooperation with relevant stakeholders need to develop a commonly agreed framework for closing the digital divide'.[232] There seems to be an emerging consensus among the experts participating in this research that the digital divide can only be effectively addressed if it is clearly understood, defined, and measured through a commonly agreed framework. More precisely, as recommended by an expert, 'such a framework could inform evidence-based policymaking and allow governments to understand who the individuals being digitally excluded are, why they are excluded, and to guide digital inclusion efforts'.[233]

> *'… very basic challenge is digital literacy, both in the wider society and in the security sector [of developing states]. At least in my country, there's little reason to assume that they [security sector actors] are able to operate at a high professional standard in the digital sphere.'*[234]

In recent years, the lens through which the digital divide is understood has widened: shifting from a focus on physical access (ICT infrastructure) and affordability (cost of internet connection and devices) to a multifaceted understanding of the causes of the digital divide, including digital literacy skills, and the awareness/relevance of the internet for marginalized communities. These different dimensions of the digital divide need to be tackled together, with digital literacy at the forefront of all efforts. Literacy and education levels vary from country to country. Extensive participation in decision-making and security provision is constrained where sections of the population have low levels of education and basic literacy. Experts unanimously agreed that the establishment of 'universal digital literacy programmes have the opportunity to provide free access to educational programmes for marginalized communities to acquire digital capabilities so that they can be better integrated into our contemporary interconnected societies'.[235] Along the same lines, the experts added that 'the security sector may also collaborate with the public sector and big tech companies, to create public accessible spaces, where digital resources and

[231] Round 1, Response 3.

[232] Round 3, Response 9.

[233] Round 3, Response 9

[234] Round 1, Response 8.

[235] Round 3, Response 2.

courses are freely accessible. This partnership could lead to specifically seek out members of marginalized communities to empower them to be advocates for their communities in digital literacy and provide them with resources to introduce their fellow members to how digital skills can help with their careers and other commercial activities.'[236]

As processes are implemented and the security sector improves data literacy both internally among its own staff and externally in the general population, it is possible that accountability, rule of law, and governance will significantly improve. As an expert added, 'the security sector, by its very nature, must contribute to the development of digital literacy, not limit it – because every entity within the society is important. Policymakers should never forget that citizens are their partners.' For example, the Smart Africa Digital Academy (SADA) provides courses, webinars, and opportunities for exchange to policymakers and regulators to promote an inclusive digital transformation in Africa. SADA reaches a wide audience, ranging from state officials, entrepreneurs, and normal citizens with the aim of improving their digital literacy, to ensure that all individuals can benefit from the potential benefits offered by emerging technologies.[237] In recent years, several educational models for digital literacy have been developed. One of these is the Digital Navigator model – individuals with robust digital skills take on the role of offering guidance to their community on different topics, such as connectivity, devices, and digital literacy.[238] As such, the experts have unanimously agreed that a population with a high digital literacy level 'can proactively participate in security provision and oversight'[239], as it would 'allow security actors to collect feedback from citizens about how they use their security services'.[240]

Promoting participation and engagement

The global availability of digital technologies combined with an increasing rate of digital literacy and connectivity enables security sector actors to reach almost anybody at any time online. According to an expert, 'this allows for a powerful channel to curate online sentiment, get information about the wants and needs of specific target populations, and better tailor activities to the specific needs of persons or groups'.[241] In parallel, as digitalization will increase the skills of security sector actors, for example in law enforcement, it is likely to also increase the skills of many other citizens (and oversight organs), who will be empowered to keep security sector actors 'on their toes' as claimed by another expert.[242] This will translate in better SSG since security institutions will be constantly aware that they are being watched, by better-informed constituents. This, in turn, enhances accountability, transparency, and the rule of law.

> *'Depending on how the term "security sector" is viewed, the risk of exclusion or lack of online presence of certain groups in society should be carefully considered. If we traditionally see the security sector as taking care of the defence and security of a country, then the exclusion of certain groups can be regarded as a risk in terms of susceptibility of these groups to various negative influences and security practices, for example. If we look at the security sector as a construction on which the well-being of a country is built, then such exclusion leads to the risk of regression of the state, in terms of economic, educational, and scientific capacity. The exclusion of women and other marginalized groups from access to information carries risks of misbehaviour in various crisis situations, lack of opportunity to report potential threats or accidents (from natural disasters to abuse of this category of population). […] This would mean that states have irresponsibly given up on that category of population that has the absolute right – and the state has the responsibility – to access information for more appropriate inclusion and participation in society.'*[243]

[236] Round 3, Response 8.

[237] Smart Africa Digital Academic, Home page (2023). Available at: https://sada.atingi.org/.

[238] Digital Inclusion, 'The Digital Navigator Model' (2023).

[239] Round 1, Response 8.

[240] Round 1, Response 8.

[241] Round 1, Response 2.

[242] Round 1, Response 11.

[243] Round 3, Response 9.

Full equitable and inclusive participation in the digital space and access to digital information is impacted by the available infrastructure, the costs, and the digital literacy of the user. Additionally, access to the technology to enable digital participation might not be so easily available. Access is further impacted by connectivity and electricity supply in certain regions of the world. Access to infrastructure to enable participation might also not be equally available across the demographics of the community and may be exacerbated by cultural practice. This could affect the participation of the elderly, of youth, and of women. The language in which the digital information is made available and where it takes into consideration hearing and sight impairment, or other disabilities, can also have an impact on participation. In this context, an expert stated that 'information about the security sector can be made more accessible by converting official documentation and other information into different formats, such as audio and video. This will contribute to more informed understanding amongst populations of how and why decisions are made.'[244] Documentation available online can provide opportunities for the translation of this material into other languages by individuals/groups with an interest in promoting greater participation in decision-making and service provision, while allowing for better searchability of documentation and other resources, which makes finding relevant information easier, and is highly beneficial for those looking to undertake research on the security sector.

In addition, new meeting technologies and the increased use of online meetings allow individuals to participate in safe spaces from which they were previously excluded due to the costs and logistics of attending. The video recordings and minutes of such meetings remain available to facilitate future gatherings, and documentation and the ability to access relevant parts of documents are more easily available via online facilities. At the same time, digitalization has empowered some marginalized communities to provide their input into research studies or to conduct their very own research. This has allowed for the priorities and concerns of previously marginalized communities to be easier understood and brought to the forefront in the planning of the security sector. Likewise, complex data has been made more accessible through easier mapping and visualisation of the data. This facilitates participation in understanding results and trends, the review of results and in decision-making. According to an expert, 'gathering different actors into online meetings can bring new people and new ideas or solutions to some societal issues. In this way, the security sector itself will develop an awareness of seeing itself in a broader social context and will identify factors (which it may not have assumed) that may contribute to the advancement of security as a whole. The security sector can be trapped in the traditional view of itself and its tasks. Enabling the participation of more diverse entities using meeting technology can help the security sector to change its self-image.'[245]

Policymakers will need to ensure that online platforms managed by the security sector do not purposely omit, or as a result of lack of serious studies or design, any segment of the population. Further efforts can and should be made by including all segments of the population concerned with security provision. In addition, these platform designs must be tested to uncover any features that may be exclusionary or discriminatory. For example, countless cyber communities engage in producing and exchanging security-related information in the internet space.[246] An expert suggested that 'governments can certainly introduce policies to ensure equitable online participation, especially in public forums sponsored by local and national authorities. For instance, a certain percentage could be set aside on the basis that it can ensure equitable participation by all parts of the population, ensuring that it is representative of its ethnic, religious, and gender diversity.'[247]

For example, the city of Madrid uses the platform Decide Madrid to enable citizens to submit ideas for solidarity, connect with businesses in their neighbourhood, and ask municipal experts questions about any crisis situation.[248] An expert added that 'in Brazil, during the pandemic, the senate provided legislative responses to COVID-19 questions proposed by citizens through the e-Citizenship Portal, while in Scotland, local authorities held an online consultation to enable the public to submit and rate comments on the government's COVID-19 response'.[249] Policymakers must insist upon proper training of security sector actors to ensure that they act professionally and

[244] Round 1, Response 12.

[245] Round 3, Response 9.

[246] Round 1, Response 3.

[247] Round 3, Response 12.

[248] Participedia, 'Decide.Madrid.es Online Participatory Budgeting' (2023).

[249] Round 1, Response 13.

meet the objectives in developing this digital space and using new technologies. As highlighted by an expert, security sector actors 'must have firm rules that call for constant supervision and performance evaluation of the actors. They should also consider provisions that seek to punish the actors who exclude specific populations on online platforms.'[250]

As such, digitalization offers the opportunity for a more active civilian engagement with the oversight and accountable governance of the security sector. As stated by an expert, 'there is likely to be increased public participation in security provision in democracies where diversity and differing views are respected (and mechanisms of effective oversight exist). In such contexts, it is likely that robust public debates will address the security sector and its role in society.'[251] As digitalization can be used as a tool for security sector actors to engage in direct contact with citizens via social media, the checking of information, and reports on a homepage, and other communication channels, citizens could therefore have a safe space to access and broaden their knowledge about security issues. However, as stressed by another expert, 'many countries around the world are categorised as authoritarian or hybrid regimes. In such countries, digitization is unlikely to have a significant impact on participation, as meaningful public engagement is not encouraged and oversight mechanisms are weak or absent. Nonetheless, such information may contribute to building momentum amongst pro-democracy movements in such countries.'[252]

Implementing a gender-sensitive approach

As the world is increasingly moving online, opportunities for business and education are not equal for all. Women and girls face a range of barriers to equal access to the internet, many of them being extensions of longstanding discrimination and repression. Once online, they face a range of virtual harassment and abuse. It is necessary to address this to ensure that women and girls are not left behind or excluded from using available digital technologies. The term 'digital gender divide' is frequently used to refer to these types of gender differences in resources and capabilities to access and effectively utilize digital technologies within and between countries, regions, sectors, and socio-economic groups.[253] On a global scale, there are 259 million more men than women using the internet, according to the ITU.[254] This gap has significant implications for women's participation in the digitalized security sector.

> *'[…] access to technology is not equal between men and women in all countries. Females are less likely than males to gain access to the internet in many parts of the world. […] . Cost is the biggest barrier to mobile phone ownership for many people, and cost typically affects women more because their average income is lower than men's. Education is another serious issue; in many countries, girls have less access to education than boys. Limited literacy surely leads to lack of digital skills and thus reducing women's ability to take advantage of online resources.'*[255]

Some root causes of the digital gender divide include barriers to access, affordability, poor education, technological illiteracy, inherent biases, and socio-cultural norms. Women often face disproportionate challenges due to their role in unpaid care and domestic work, leaving them with less time to develop digital skills and careers.[256] Negative social perceptions, lack of acceptance by family members, and family opposition can deter women from embracing digital technologies. Girls' lower confidence in emerging technologies, maths, and science is also influenced by societal and parental biases, impacting their engagement in these fields. Addressing the digital gender divide requires the implementation of a gender-sensitive approach throughout the society, starting with the state and the security sector.

[250] Round 3, Response 13.

[251] Round 1, Response 12.

[252] Round 1, Response 12.

[253] OECD, 'Bridging the Digital Gender Divide – Include, Upskill, Innovate' (2018).

[254] International Telecommunication Union, 'The Gender Digital Divide' (2022).

[255] Round 1, Response 16.

[256] OECD, 'Bridging the Digital Gender Divide – Include, Upskill, Innovate' (2018).

Digitalization can open new windows of opportunity for security sector actors in terms of offering, managing, and overseeing the specific needs of women. As described by an expert, 'digitalization and relevant technologies offer women the potential to bypass some of the traditional cultural and mobility barriers, particularly in developing countries'.[257] An expert suggested that, to 'deliver gender-sensitive security and justice, security actors should strive to foster female digital literacy; and encourage more women to participate in tertiary education and STEM (science, technology, engineering, and mathematics) occupations and jobs. Having in mind that already disadvantaged groups are overrepresented in offline populations, which is disproportionately female, […], governments, in cooperation with relevant stakeholders, need to develop a commonly agreed framework for closing the digital gender divide. This divide is thwarting opportunities and raises risks, exacerbating inequalities inside the community by negatively impacting the life prospects of women.'[258]

Over the past decades, the UN system, nation states, and other international actors have recognized that the security sector needs to be gender responsive.[259] With the adoption of the 2030 Agenda for Sustainable Development by the UN member states in 2015, digital technologies have gained increasing importance in meeting Goal 5: Gender Equality.[260] In this context, initiatives for gender mapping in the field of ICT have been launched in order to accelerate the global process of bridging the gender divide.[261] For example, the International Telecommunication Union (ITU) produces global and regional gender equality scorecards that assess the digital gender divide. These scorecards provide data and analysis on the participation of women and men in the information and communication technologies (ICT) sector, internet access, and digital skills development.[262] The UN Women's WEPs initiative encourages businesses to adopt principles that promote gender equality and women's empowerment in the workplace, marketplace, and community. It includes a focus on promoting women's participation and leadership in the ICT sector.[263] Moreover, various mentorship programmes connect experienced women in the tech industry with aspiring women in ICT. In parallel, given the gender gap in the cybersecurity field, initiatives such as 'Women in Cybersecurity' programmes aim to map gender disparities and create strategies for increasing female representation in this critical ICT sector.[264]

In this context, the reduction of the digital gender divide will occur if policies go beyond access and focus more on decision-making and capacity-building processes. Usually, CSOs and activists are the ones who engage the public and eventually encourage people to follow administrative procedures. Women suffer from not having control over the finance and economic administration of their household. As such, an expert suggested that 'the security sector actors must be trained to be gender sensitive and understand that in the digital space gender issues take different forms and may even exacerbate the situation. Policymakers must incorporate training for their security actors to find effective ways of empowering women. Part of the training should develop the understanding of security sector actors on how specific digital tools are effective methods to empower women and enable them to bypass obstacles created by traditional social and cultural barriers.'[265] Another expert added that 'policymakers need to be aware of the technological barriers encountered by women and devote proportional percentages of investments and quotas in hiring and training'.[266] Policymakers have the opportunity to employ digital communication tools and online mechanisms to ensure the involvement and participation of women community representatives. And finally, an expert stressed the fact that 'all efforts should be made to reinforce gender mainstreaming and strengthen women's participation in law enforcement'.[267]

---

[257] Round 1, Response 16.

[258] Round 1, Response 16.

[259] UN Political and Peacebuilding Affairs, 'Women, Peace and Security' (2023).

[260] Sustainable Development Goals, 'Goal 5: Achieve Gender Equality and Empower All Women and Girls' (2023).

[261] Ibid.

[262] International Telecommunication Union, 'The Gender Digital Divide' (2022).

[263] Women's Empowerment Principles, About (2023). Available at: https://www.weps.org/about.

[264] International Telecommunication Union, 'Women in Cyber Mentorship Programme' (2023).

[265] Round 1, Response 16.

[266] Round 3, Response 10.

[267] Round 3, Response 9.

Spotlight: Using digital communication platforms to bridge the digital divide

The digital divide, characterized by unequal access to ICT, remains a pressing global challenge. In addition, from a socio-technical perspective, the digital divide can be regarded as consisting of existing differences in terms of knowledge and skills due to lack of digital education, different perceptions of technology, costs, and both social and cultural norms. Experts argue that it is not a matter of connectivity – as more and more individuals are nowadays able to access the internet through the proliferation of smartphones – but rather of digital literacy, cultural differences, and cost barriers. Other experts argued that digital communication platforms hold significant potential in reducing this divide by facilitating connectivity, fostering the exchange of knowledge, and promoting inclusion. Digital communication platforms have become important pathways to reduce the digital divide and help vulnerable communities build safe online spaces, access information, promote human rights, and exchange on relevant themes. These platforms range from email, instant messaging applications, social media, blogs, meeting technologies, and forums.

For example, social media, messaging apps, and video conferencing tools provide avenues for individuals and communities to connect across geographical barriers. They enable real-time communication, facilitating knowledge sharing, collaboration, and access to educational resources. Facebook's initiative Internet.org (now Free Basics) aims to provide free access to selected online services, including educational content, health information, and communication tools, in underserved regions.[268] These digital platforms offer a wealth of educational materials, e-learning platforms, and Massive Open Online Courses (MOOCs) that can be accessed remotely. By educational resources being made available online, individuals in underserved areas can overcome physical barriers to education and acquire knowledge and skills. Moreover, platforms such as Fiverr or Upwork connect freelancers from around the world with clients seeking their services. These platforms enable individuals, regardless of their location, to access global job opportunities and generate income.

However, some individuals on digital platforms might act with hidden and malicious intentions that are dangerous to the security of the state. Experts believe that communication platforms can sometimes lead to 'information pollution'. Information pollution can be briefly defined as disinformation, fake news, and propaganda campaigns that aim to destabilize confidence in government and security institutions. At the same time, other experts argue that some authoritarian governments might use communication platforms and digital technologies to curb opposition and to manipulate political narratives. It is thus becoming increasingly difficult in modern societies to distinguish between true and false news. As an expert has explained 'the authorities are able to determine the political moods of the society and manipulate them through the use of communication technologies'.[269]

Human rights defenders communicate about abuses and advocate for change using social media, forums, or blog posts. Vulnerable populations use such chat groups on various applications to keep themselves informed but also to denounce human rights violations to CSOs. The experts argue that the anonymity enabled by communication platform networks allows users to express their opinions and beliefs free from any burden. The free flow of information, free expression, and free debate in digital space are requisites for good governance over security sector actors. The experts warn that digitalization itself 'may not lead to the best protection against abuse of state power'.[270] Breaches of security systems can result in private information leaks and hence harms to human rights protection. Governments can use digitalization to deliberately target certain segments of the public or individuals due to their dissent in political opinions or certain beliefs, either religious or political. This is typically the practice in authoritarian states where security authorities use digitalization to monitor citizens, to prevent and suppress any activities deemed unfavourable to the official views.[271]

In parallel, to ensure the safety of citizens in the digital space, new security measures might conflict with human rights principles. Some experts believe that there is a silent compromise between national security and the right to privacy and protection of personal data. Experts add that big tech companies have a major impact in bringing new technologies and means of communications to the people.[272] Accordingly, they can focus upon developing those

---

[268] Dredge, S., 'Facebook's internet.org Initiative Aims to Connect "the Next 5 Billion People"', *The Guardian* (2013).

[269] Round 1, Response 11.

[270] Round 1, Response 3.

[271] Shahbaz, A., 'The Rise of Digital Authoritarianism', *Freedom House* (2018).

[272] Round 3, Response 9.

technologies that respect human rights and empower vulnerable communities. Big tech as a major employer can play a proactive and significant role in training its own employees to understand societal biases and discrimination, and to seek ways to address it positively. Most importantly, big tech companies can enhance security by levelling the opportunities for everyone and proactively reaching out to those who have been historically discriminated against.

The experts stress the fact that new communication technologies have proven their ability in increasing the efficiency of national security institutions to be more inclusive and reach marginalized individuals in remote parts of society. For example, law enforcement can communicate quickly on events that have an impact on the population (e.g., demonstrations, concerts, sports events, or road accidents causing disruption). It is essential to increase communication channels between all stakeholders, including the public and the government. Digitally enabled communication and crowd-sourcing solutions might help with creating checks and balances against security actor overreach and strengthen the trust of citizens in security sector institutions. Moreover, experts highlight that communication platforms allow for better intra-governmental coordination, by sharing critical operation data so all government agencies involved can minimize knowledge gaps. Security sector actors can publish stories about their operation to keep the population informed.

Digital communication platforms present immense opportunities in bridging the digital divide by increasing connectivity, providing access to educational resources, and creating economic opportunities. However, challenges such as infrastructure limitations, digital literacy gaps, language barriers, information pollution, and affordability issues must be addressed in a sustainable manner to ensure safe, equitable, and inclusive access.

Security sector actors and the digital divide

The experts participating in this study examined how security sector actors employing digital technologies can address and close the digital divide. For example, experts stressed the fact that public law enforcement has a responsibility to be aware of the digital divide, to ensure that vulnerable groups are not done a disservice. This could include ensuring that information is disseminated in various formats, including for those with disabilities and learning difficulties, as well as tailored to various linguistic groups. However, as explained by an expert, a major challenge remains the fact that internet access is severely limited in many countries in the Global South, either due to availability or data prices. Digitalization enables security sector actors to reach almost anybody at any time online. This allows for a powerful channel to curate online sentiment, obtain information about the wants and needs of specific target populations, and better tailor activities to the specific needs of individuals or groups. As such, police forces can better engage with the public by inviting them to participate in events via the new means of communication, by creating digital meetings on themes that affect their activities, thus affirming a desire for transparency and accountability.

The experts added that in most countries official documents are usually only published in one or possibly two languages, even though multiple languages are spoken. Governments rarely translate such documents into languages that are used by marginalized populations. Information about the security sector can be made more accessible by converting official documentation and other information into different formats, such as audio and video for people with disabilities. This will contribute to better understanding among populations of how and why decisions are made. The digitization of sector documentation can provide opportunities for the translation of this material into other languages by individuals or groups with an interest in promoting greater participation in decision-making and service provision. Experts argued that the government can use technology to develop adequate measures for monitoring policy implementation, to ensure that it is meeting its targeted goals, to assess performance of various units implementing their policies, and to use the digital space to inform and receive constant feedback from the people who are the recipients of these policies.

The experts also highlighted that big tech companies have a major impact in bringing new technologies and means of communications to the people. Accordingly, they can focus upon developing those technologies that empower women and raise awareness about gender-related issues. Big tech also is a major employer and hence can play a proactive and significant role in training its own employees to understand the gender discrimination prevailing in society and seek ways to address it positively. Most importantly, big tech companies can enhance gender security by levelling opportunities for everyone and proactively reaching out to those who have been historically discriminated against.

Recommendations: Digital divide

In terms of addressing the digital divide, the following three recommendations were developed by synthesizing the opinions of the experts participating in this study, as presented in the previous sections:

1. Security sector actors should collaborate with the public sector and big tech companies to create accessible public spaces where digital resources and courses are freely accessible, with a focus on empowering marginalized communities. Improving digital literacy can lead to better accountability, rule of law, and governance.
2. Security sector actors should use online platforms and technologies to engage with citizens, ensure digital inclusion, and promote public participation in security provision and oversight to leverage greater transparency, accountability, and participation in the security sector.
3. Security sector actors should develop a commonly agreed framework for closing the digital gender divide, while reinforcing gender mainstreaming and strengthening women's participation in law enforcement.

Conclusion and recommendations

Digitalization has made its way into many security-related domains, such as the armed forces, intelligence services, and law enforcement, to mention a few. This results in a digitally interwoven security sector, giving rise to a more complex security ecosystem that is exposed to continuous organizational, institutional, and regulatory transformation. This renders the digitalization process highly dynamic and complex, and thus challenging for public security policies insofar as it requires constant adaptation. Thus, as digitalization can be regarded as a multi-layered security challenge that – through its dual nature – can affect the governance, provision, and oversight of security services, it is evident that SSG/R has a key role to play in defining the fair use of new technologies and in exploring how to strengthen digital governance frameworks. As such, this Delphi study has sought to address the overarching impact of digitalization on the security sector and it has reached the following conclusions.

First, the experts participating in this research have reached a consensus illustrated in the form of the five thematic areas explored in the Analysis chapter. These five thematic areas range from new technologies, technical capacity, regulation and oversight, human rights in the digital age, and the digital divide. The experts unanimously agreed that new technologies enable security sector actors to use a plethora of new tools to improve their accountability, transparency, and effectiveness in security provision. Nonetheless, these technologies require continuous human control and evaluation to uphold the rule of law, while security sector actors need to develop the appropriate technical capacities and skills to use such tools safely and efficiently. Furthermore, security institutions and policymakers need to propose and promote robust regulations that keep up with the rapid pace of technological developments, while paying close attention to the implications of digital technologies on human rights, to ensure the responsiveness of security oversight when facing any form of abuse. Security institutions and actors play a paramount role in the quest to close the digital divide and ensure inclusive participation in the sector for groups that have previously been marginalized or excluded.

Second, this study has identified the main challenges and opportunities digitalization poses to good SSG. While new technologies, such as AI, have huge potential to assist security providers and overseers in improving their operations and decision-making processes based on huge amounts of data, this might risk intensifying existing power asymmetries, especially for citizens in vulnerable situations. To avoid such risks, security personnel need to develop an awareness of digital threats and the technical capacity to use such tools in their daily duties. The experts recognize, though, that current regulatory frameworks are outpaced by technological advancements. At the same time, the experts agree that the digitalization of the security sector has increased the pressure to properly balance individual human rights, such as the freedom of expression or the right to privacy, with the obligation and duty of states to protect their citizens, while access to digital space is not equitable across regions or social groups.

While the challenges posed by digitalization are substantial, it is essential to recognize the numerous opportunities it brings to the security sector. Digitalization enables the creation of accessible digital records, aiding investigations to keep track of multiple security-related incidents. Enhanced communication channels, made possible by digital platforms, foster efficient information sharing among security agencies. Advanced analytical tools, such as AI, process vast data sets bolstering disaster response capabilities, enabling real-time data analysis and equipping security sector actors with predictive insights and the capacity to respond to threats as they emerge. Automation streamlines routine tasks, reducing errors and freeing up resources for strategic roles. Furthermore, digitalization underscores the importance of robust cybersecurity measures, while also offering opportunities to safeguard civil liberties through improved oversight and data transparency.

Third, by exploring the thematic areas outlined above, this study has illustrated the extent to which key security providers and overseers have adapted to the transition towards the increasing digitalization of their work, and how this adaptation has created spaces for the emergence of new actors. These actors have all adapted to digitalization in their own ways, depending on their needs. For example, the armed forces are at the forefront of harnessing the potential of digital technologies to enhance their operations. From utilizing advanced communication systems to employing drones for reconnaissance and surveillance, armed forces have integrated digital tools to improve their situational awareness, response capabilities, command and control, and overall efficiency. Military organizations increasingly rely on AI and data analytics for strategic planning and decision-making, enabling them to adapt swiftly to the evolving security landscape. Similarly, law enforcement agencies have incorporated digital technologies into various aspects of their operations, such as predictive policing algorithms to allocate resources effectively, body-worn cameras for transparency and accountability, and digital

forensics for cybercrime investigations. The use of digital platforms for information sharing and intelligence collaboration has also become commonplace among law enforcement agencies, facilitating joint efforts in combating crime and terrorism.

Finally, this study provides three specific recommendations per thematic area for policymakers to consider when addressing and adapting to the challenges and opportunities posed by emerging digital technologies:

New technologies:

- The security sector needs to ensure oversight of its spending on digital resources to ensure transparency and accountability in the allocation of resources for updating legacy systems.
- Security sector actors should adopt digital tools to improve traceability of processes, sharing of information, and record-keeping within the security sector, to ensure better responsiveness, effectiveness, and efficiency.
- New technologies, such as AI, need to be implemented with careful consideration of their ethical and legal implications. Security sector actors should ensure that human judgement remains a central component of decision-making to ensure the prevalence of rule of law.

Technical capacity:

- Prioritize and invest in the education and training of security sector personnel to enhance their technical capacities in digital technologies (including cybersecurity, AI, data analytics, digital forensics, and information management), while reinforcing the principles of good SSG.
- Security sector actors should actively seek out individuals with technical expertise and digital skills to meet the growing demand for such talent in the sector.
- Prioritize cooperation, information sharing, and collaboration both domestically and internationally. By working together and sharing best practices, security sector institutions can enhance the skills and knowledge of their personnel, develop innovative strategies, and improve overall security.

Regulation and oversight:

- Security sector actors should work in collaboration across the whole sector to ensure the creation of a stable legislative and regulatory environment that keeps pace with and governs the development and use of digital technologies within the security sector.
- Security sector institutions should proactively standardize oversight approaches and provide uniform, impartial reporting standards to ensure that the principles of good security governance are applied to the oversight of digital technologies.
- Establish strategic partnerships and cooperation with various stakeholders, including academic and research institutions, corporate entities, and technology experts, to ensure participation.

Human rights in the digital age:

- Security overseers should enact safeguards based on legal and ethical guidelines to ensure that security providers respect privacy rights when conducting any form of mass surveillance.
- Security sector actors should adopt a multi-stakeholder approach and collaborate with public organizations and the private sector to enhance the protection of human rights in order to avoid any form of digital authoritarianism.
- Security sector actors should strengthen legal frameworks, support independent journalism, promote digital literacy initiatives, ensure transparency and accountability within security institutions, and utilize emerging technology (such as AI) to protect human rights in the face of disinformation.

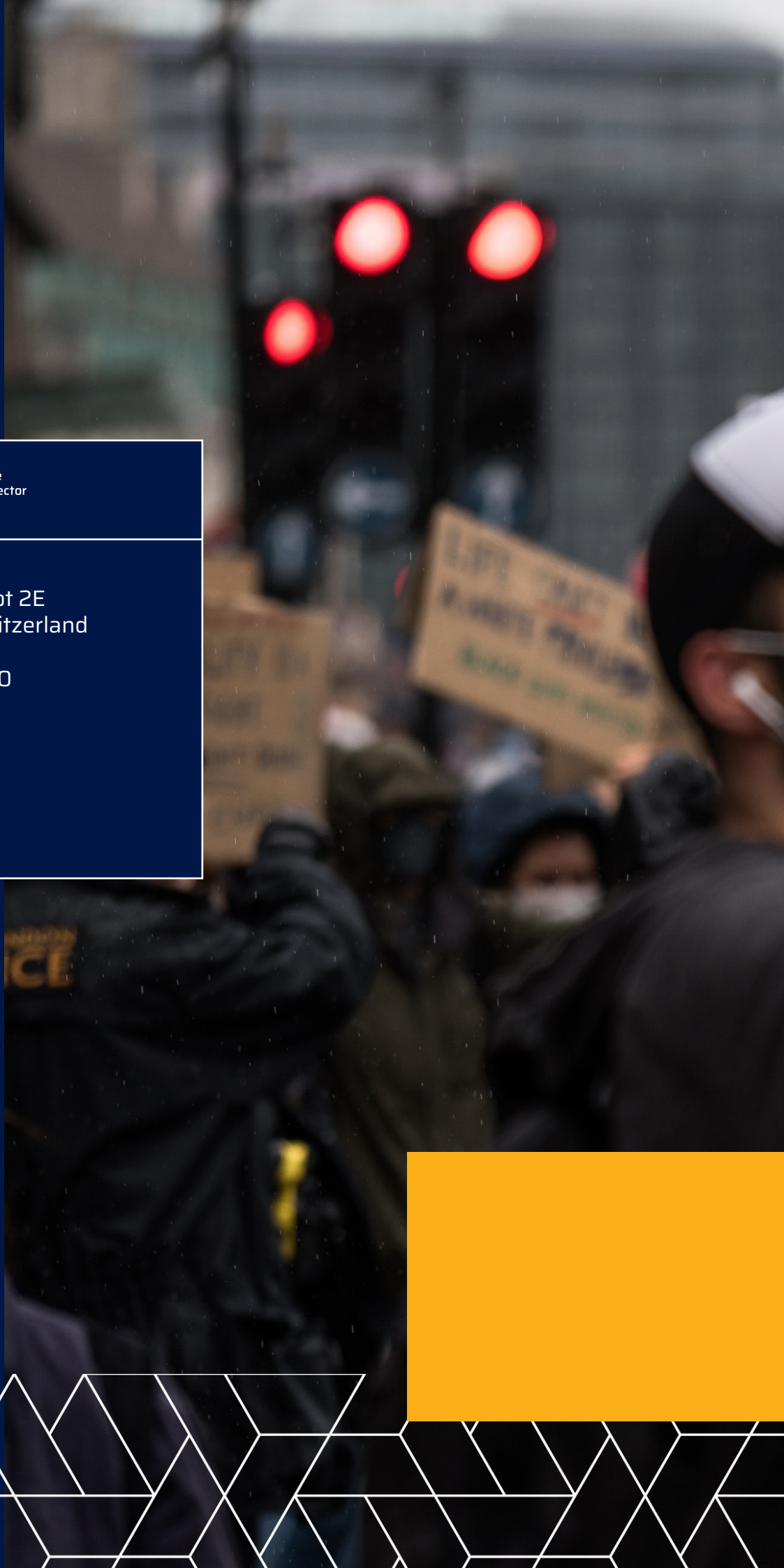
Digital divide:

- Security sector actors should collaborate with the public sector and big tech companies to create accessible public spaces where digital resources and courses are freely accessible, with a focus on

empowering marginalized communities. Improving digital literacy can lead to better accountability, rule of law, and governance.

- Security sector actors should use online platforms and technologies to engage with citizens, ensure digital inclusion, and promote public participation in security provision and oversight to leverage greater transparency, accountability, and participation in the security sector.
- Security sector actors should develop a commonly agreed framework for closing the digital gender divide, while reinforcing gender mainstreaming and strengthening women's participation in law enforcement.

Building upon the current study, for future research it would be beneficial to conduct a comprehensive mapping study on the integrations of AI technologies in defence and military operations. More precisely, this future research could investigate how AI is transforming decision-making processes, while exploring the ethical, legal, and strategic dimensions of lethal autonomous weapons systems (LAWS). In addition, future research could delve deeper into the cybersecurity challenges faced by security sector institutions and actors as they embrace the process of digitalization and adopt emerging technologies, such as AI, into their operations.



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
www.dcaf.ch

@DCAF_Geneva