

Accountability in cybersecurity

Edited by Franziska Klopfer

December 2024

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](https://twitter.com/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

info@dcaf.ch

www.dcaf.ch

Twitter [@DCAF_Geneva](https://twitter.com/DCAF_Geneva)

Contributors

Editor: Franziska Klopfer

Design & Layout: Elmæ Muslija

Cover image: Geralt on Pixabay

Disclaimer

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

Table of contents

Introduction

by Franziska Klopfer.....4

CHAPTER 1

Parliamentary oversight of cybersecurity policies:

comparative analysis of Germany, Switzerland, and the UK

by Nele Achten.....7

CHAPTER 2

Unrealized potential:

ombuds institutions and oversight of cybersecurity in the Western Balkans

by Luka Glušac.....25

CHAPTER 3

Seeking accountability for cyber-attacks:

challenges of attribution and subsequent responses

by Rebecca Mikova.....44

CHAPTER 4

Cybersecurity and its challenges:

an introduction for members of parliament

by Teodora Fuior.....71

CHAPTER 5

Safeguarding digital democracy:

the evolving role of non-public actors in Albania

by Megi Reçi and Sara Kelmendi.....106

Conclusion

by Franziska Klopfer.....134

As more and more aspects of our lives are becoming digitalised, it is important to think about how to protect digital services and the systems and networks running those services.

In recent years, high-profile cyber-attacks have shown how vulnerable digital services are. The Western Balkan region is no exception. Smaller and bigger cyber incidents and attacks occur repeatedly. At the same time there is an increase in cybercrime targeting private individuals and companies.¹

Another set of threats to digital security relate to the content that is distributed online. Online harm and disinformation can have profound impact on the safety of individuals and the stability of societies. A definition of cybersecurity therefore must not only include the protection of networks, infrastructures and services but also the safety of those using online services.² The Freedom Online Coalition defines that cybersecurity aims “to enhance the security of persons both online and offline[.]”³

Many different actors are involved in cybersecurity, and they need tools, cooperation mechanisms, regulations, in order to be able to provide cybersecurity.⁴ Individuals, organisation and companies can do a lot to protect themselves online, for example by adopting sensible gestures (‘cyber hygiene’) and using IT security tools. They need to be supported by the state, which is also in charge of the overall cyber defence of the country. Some of the cybersecurity activities that states provide include: setting cybersecurity standards and roles in enforcing them in procedures and laws (state legislator); preventing, investigating and prosecuting cyber-crime (police, protectors, judiciary); providing support with cyber incidents (computer emergency response teams (CERTs)).⁵

A discussion on roles and responsibilities of different actors in cybersecurity needs to be followed by a discussion on accountability: What happens when these roles and responsibilities are not fulfilled?

¹ See, for example, ENISA Cyber Threat Landscape (2024).

<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>

² The European Union (EU) defines cybersecurity as “the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats” EU Cybersecurity Act: Art. 2.1

³ <https://freeandsecure.online/> This definition was developed in reference to the UN Human Rights Council’s 2012 resolution in which UN member states (A/HRC/20/8) “affirm that the same rights that people have offline must also be protected online.”

⁴ The International Telecommunications Union (ITU), the United Nations specialized agency for information and communication technologies explains what these cybersecurity ‘activities’ are and lists: “...the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment and organization and users’ assets”. ITU Recommendation X.1205 (04/08) ITU-T X.1205, Overview of cybersecurity; <https://www.itu.int/rec/T-REC-X.1205-200804-I>

⁵ The exact definition of different actors roles and responsibilities need to be defined by law. While general best practices exist (such as EU Network in Information Security Directive), in practice roles and responsibilities are still defined and re-defined. See for example “Roles in Cybersecurity: CSIRTs / LE / others”. Available at Lendl, Otmar (CERT.AT): [CERT.at Roles in Cybersecurity: CSIRTs / LE / others](https://cert.at/roles-in-cybersecurity-csirt-le-others)

In particular, how can the state be held accountable? In discussions on cybersecurity, accountability is often defined as holding those perpetrating malicious cyber-attacks to account. The 11 norms of responsible state behaviour in cyberspace, which are part of the United Nation's framework of responsible state behaviour in cyberspace, are one of the guiding documents that aim to shape international cybersecurity. They define what states should do or avoid doing in cyberspace and aim at promoting interstate cooperation, "respecting human rights and privacy, protecting critical infrastructure, safeguarding global supply chains, providing assistance when required and preventing the malicious use of digital technologies on states' national territories."

However, accountability should not only be concerned with state's negative obligations to not do harm but also their positive obligations to prevent harm as best as possible. Security Sector governance (SSG) has long been concerned with how security is provided. Effectiveness and efficiency are two major principles of good governance in the security sector. Applied to the cybersecurity field, SSG is concerned with whether the cybersecurity activities of the state are actually effective and efficient. Is the state doing enough to ensure the cybersecurity of data and of systems to avoid that data is misused and that digitalised services are safe and available?

Another principle of good governance is responsiveness. Applied to cybersecurity, this principle looks at whether cybersecurity as a whole is responsive to the real security needs of all. It is based on the premise that the state has to ensure the security of all members of society equally. This then includes a duty to provide security online to all citizens. Do cybersecurity plans understand and respond to specific vulnerabilities that different members of society have? Are the right priorities set in national cybersecurity strategies?

In practice, few actors currently are consistently holding states to account on how they deliver cybersecurity to their citizens. This book aims to look at some of the oversight actors that aim to ensure accountability in the traditional security sector: parliaments, independent state bodies (such as ombuds-institutions) and civil society.

By far the most powerful oversight actors should be the national parliament. They have a legal mandate to oversee the work of government and state security actors. They usually have the power to call state security providers to give account of their work. They can start inquiries, demand regular reports and can declare that actions of that state were illegal.

There are other mechanisms: for example independent state bodies, such as human rights ombuds institutions or national audit offices. They can investigate issues of concern and also have the right to demand access to a certain number of official documents. They can however only condemn possible illegal activities and then bring a complaint before a court.

Civil society organisations have no legal powers but can play a critical role in fostering accountability. While they have no legal mandate to oversee and have a more limited access to official documents; they cannot convoke any state official. But they are in principle not dependent on government money or parliamentary approval of their budget. They decide on their own agenda and can focus on topics that they consider important. They are potentially more flexible in acquiring new knowledge and expertise. Think tanks in particular, with trained researchers can provide important insights into the functioning of the cybersecurity system, and examining the adherence to human rights standards.

This book examines different aspects of accountability by exploring the potential of oversight actors in ensuring accountability of state cybersecurity actors.

Parliamentary oversight of cybersecurity policies: comparative analysis of Germany, Switzerland, and the UK

by Nele Achten, independent consultant¹

¹ This background paper is part of the three-year project 'Good Governance in Cybersecurity in the Western Balkans' (June 2021–March 2024) implemented by the Geneva Centre for Security Sector Governance (DCAF) and funded by the UK government's Foreign, Commonwealth and Development Office (FCDO).

Table of contents

	Key insights	9
1.	Introduction	9
2.	Parliamentary oversight	10
2.1	Forms of parliamentary oversight.....	11
2.2	Implementation of the parliaments oversight function.....	12
3.	Oversight of cybersecurity policies	13
3.1	Evaluating the success of proactive oversight activities.....	14
3.2	Examples of proactive oversight activities of cybersecurity policies.....	14
4.	Parliamentary committees overseeing cybersecurity policies	18
4.1	Types of parliamentary oversight committees.....	19
4.2	Oversight of national cybersecurity agencies and policies.....	21
5.	Summary conclusion	23
6.	Annexes	24

Key insights

- The collection of information pertinent to governmental actions and policies is the most relevant tool for parliamentary oversight of cybersecurity policies.
- The collection of information related to cybersecurity policies can have different objectives: 1) to make more informed decisions about the adequacy of existing policies versus the need for new legislation, 2) to evaluate the allocation of budgets, and 3) to influence foreign policy and diplomatic responses to specific issues.
- The collection of information related to cybersecurity policies can have different objectives: 1) to make more informed decisions about the adequacy of existing policies versus the need for new legislation, 2) to evaluate the allocation of budgets, and 3) to influence foreign policy and diplomatic responses to specific issues.
- Cybersecurity is a cross-sectional topic that falls within the oversight responsibility of a wide number of parliamentary committees. This makes it difficult to gain a full picture of existing oversight activities related to cybersecurity topics. In contrast, a single parliamentary committee is generally responsible for oversight over national cybersecurity agencies. It is thus easier for parliamentarians to get a comprehensive understanding of governmental actions and policies that fall under the responsibility of a national cybersecurity agency.

1. Introduction

If one were to ask a politician or policymaker about the role of parliaments in strengthening cybersecurity, they would most likely begin by discussing the legislative function of parliaments. In the field of cybersecurity, however, this function may seem limited and insufficient to establish effective governance of the most relevant issues. In several countries, many aspects of cybersecurity are indeed not regulated by legislation. Governmental agencies instead rely on frameworks for voluntary cooperation with the private sector.¹

Nevertheless, in addition to their legislative function, parliaments also play an oversight role. They are responsible for overseeing governmental policies, programmes, and responses to specific issues. The present background paper analyses the oversight function of parliaments in Germany, Switzerland, and the United Kingdom (UK) regarding different issues related to cyber-

¹ Legislation has been identified as an inadequate tool of governance by several states regarding problems related to cybersecurity policy, including disinformation, the exchange of information between the public and private sector on cyber incidents, and comprehensive mandatory security requirements for consumer products.

security policy. The paper aims to support cybersecurity actors in the Western Balkans, in particular parliamentary staffers and members of parliament, to understand how they can contribute to more effective and accountable cybersecurity governance.

In Section 2, the paper outlines the key forms of parliamentary oversight and the parliamentary bodies that usually exercise these functions. Forms of oversight range from an ex post assessment of government performance in relation to proactive activities aiming to collect information about governmental policies and responses to specific issues. These proactive oversight activities have been the most relevant form of oversight regarding cybersecurity policy problems. Ad-hoc investigations on specific issues, in contrast, have not yet played a significant role in the oversight of governmental cybersecurity policies.

In Section 3, the paper discusses oversight of cybersecurity policies and related governmental responses. Proactive parliamentary oversight is particularly important in evolving and complex policy fields, such as tech and cybersecurity policy. Effective proactive oversight activities should be defined more clearly to maximize the benefits of oversight. In addition, different oversight tools allow parliamentarian to invest only a certain amount of their time in related activities, depending on the scope of the investigation they are conducting. This section provides examples of different levels of parliamentary investigations in the field of cybersecurity policy.

Finally, the paper outlines the oversight role of parliamentary committees in Germany, Switzerland, and the UK. Section 4.1 briefly outlines the different types of committee in each of the analysed jurisdictions and the legal basis for their creation. Section 4.2 then provides an overview of parliamentary committees overseeing national cybersecurity agencies and other issues related to cybersecurity policy.

2. Parliamentary oversight

Parliamentary oversight can be defined as parliament's responsibility and capacity to be informed about governmental policies, programmes, and responses to specific incidents, and to intervene when deemed necessary. This form of oversight is, and always has been, a fundamental element of the balance of power. Parliamentary oversight is a mechanism to prevent the abuse of governmental power² and is 'at the heart of the relationship between the executive and the legislative powers'.³

² Griglio, Elena. 2020. 'Introduction: Oversight of the Executives. A European Approach', in *Parliamentary Oversight of the Executives: Tools and Procedures in Europe*, ch. 1, p. 3.

³ Ibid., p. 4.

2.1 Forms of parliamentary oversight

Parliamentary oversight may come in many forms – reactive or proactive (ex post or ex ante), adversarial or supportive. Ex post oversight can be carried out either to respond to a particular incident or situation or to ensure the regular monitoring of budget spending. An investigation into a particular incident is generally conducted on an ad-hoc basis by so-called inquiry committees. Budget control, in contrast, usually falls under the responsibility of a permanent parliamentary committee, which verifies that allocated budgets have been spent for their determined purpose.⁴

In addition, oversight can also take place before the government has conducted or finished a particular activity (ex ante oversight). One form of ex ante oversight is parliamentary approval, which may be required for military deployment abroad, a declaration of war, or the appointment of high-level ministerial positions. Finally, there is a proactive form of ex ante oversight, which involves the collection of information for several different purposes.⁵

Chart 1: Key forms of parliamentary oversight⁶

Forms of oversight	Purpose
Reactive (ex post)	In-depth investigation of a particular issue
Budget control (ex post)	Monitoring how the allocated budget has been spent
Approval (ex ante)	Approval of military deployment abroad/war Appointment of high-level ministerial positions
Proactive (ex ante)	Collection of information for a variety of purposes

In the field of cybersecurity, proactive oversight activities have played a far more significant role. The purpose of proactive activities can be adversarial (e.g. information gathering by the opposition to challenge governmental responses) or supportive (e.g. to identify the need for legislation). Before analysing the meaning and examples of ex ante oversight of cybersecurity policy problems, the following section briefly outlines who is usually responsible for each of the forms of oversight outlined above and why ad-hoc inquiry committees have not yet been relevant to the oversight of specific governmental actions related to cybersecurity issues.

⁴ This type of oversight relates to an ex post assessment and must be distinguished from the proactive collection of information to evaluate the allocation of budgets.

⁵ See Section 3.2 on 'Examples of proactive oversight activities of cybersecurity policies'.

⁶ For another overview of parliamentary oversight tools, see: Griglio, Elena. 2020. 'Classifying Oversight Tools According to Parliamentary Practice', in *Parliamentary Oversight of the Executives: Tools and Procedures in Europe*, ch. 3, p. 81.

2.2 Implementation of the parliaments oversight function

Parliamentary oversight can be exercised by the plenary, permanent committees, and ad-hoc inquiry committees, although their oversight tools may vary. Typically, the plenary and permanent and ad-hoc committees may conduct hearings of experts or members of the government.⁷ Parliamentarians may also sometimes pose written questions to clarify or discuss government policies. Inquiry committees have the right to request information from public bodies, including the government, and may have the power to mandate the appearance to a committee hearing.⁸ The following chart shows which organ usually exercises the forms of ex post and ex ante oversight outlined above.

Chart 2: Who conducts the different forms of parliamentary oversight?

Forms of oversight	Who?
Reactive (ex post)	Ad-hoc inquiry committees
Budget control (ex post)	Permanent oversight committees
Approval (ex ante)	Parliamentary plenary
Proactive (ex ante)	Parliamentary committees

So far, ad-hoc inquiry committees have not played a significant role in the oversight of specific governmental actions related to cybersecurity issues. In Germany, one inquiry committee has been in charge of investigating the background and scope of foreign secret service activities within the country (also called the NSA inquiry committee).⁹ It is the only existing inquiry committee within the analysed jurisdictions that is close to cybersecurity policies. In Switzerland, a parliamentary investigation committee has only been deployed four times – the last time being in 1996.¹⁰

While most member states of the European Union provide for the appointment of inquiry committees within their constitution, Malta, Sweden, and the UK are notable exceptions.¹¹ The UK system of select committees has, to a certain degree, similar objectives and procedures to inquiry committees in other countries in continental Europe.¹² The difference, however, is that they have

⁷ There are other oversight tools, including a vote of mistrust towards the government, available to parliaments. They are intentionally not outlined here because of their irrelevance to the selected key forms of parliamentary oversight.

⁸ Pavy, Eeva. 2020. 'Committees of Inquiry in National Parliaments – Comparative Survey'. Document requested by the European Parliament's Committee on Citizens' Rights and Constitutional Affairs. March, p. 6.

⁹ Deutscher Bundestag. 2014. Fraktionen CDU/CSU, SPD, Die Linke. Und Bündnis 90/Die Grünen 'Antrag auf Einsetzung eines Untersuchungsausschusses' (18.03.2014) Drucksache 18/843.

¹⁰ Organisation des Parlements: <https://www.ch-info.swiss/edition-2021/das-parlament/organisation-des-parlements>.

¹¹ Lehmann, Wilhelm. 2010. 'Parliamentary Committees of Inquiry in National Systems: A Comparative Survey of EU Member States'. Document requested by the European Parliament's Committee on Citizens' Rights and Constitutional Affairs. October, p. 5.

¹² Ibid., p. 5.

open-ended mandates, and inquiries conducted by select committees in the UK are not limited to the investigation of governmental actions or policies on a specific past issue. They may also investigate a particular issue to shape a future government policy.¹³ This only reaffirms the relevance of ex ante oversight conducted by parliamentary committees when it comes to problems related to cybersecurity policy.

3. Oversight of cybersecurity policies

While members of parliament (MPs) might agree that oversight is an important part of their job, their engagement in oversight activities is in practice often limited.¹⁴ The MP's constituency may not see the direct benefit of oversight activities and, as a result, MPs may find it challenging to prioritize their engagement in oversight.

The second Global Parliamentary Report, jointly published in 2017 by the Inter-Parliamentary Union and the United Nations Development Programme, however, clearly concludes that:

*'Parliamentary oversight helps to deliver many outcomes that are valued highly by citizens [...] By holding government to account, identifying problems and seeking corrective measures in legislation, budget allocations, policy and administration, parliament provides a vital service to society.'*¹⁵

The parliamentary role of proactive oversight is particularly important when it comes to problems related to cybersecurity policy. Legislative responses are often considered inadequate or insufficient to address these problems; it is thus crucial for parliaments to understand the contribution of governmental policies, programmes, and responses to policy-related issues. Some MPs may be willing to engage more in oversight activities if they are convinced of the effectiveness of their oversight activities. The key question is therefore how to define the success of proactive oversight activities.

The parliamentary role of proactive oversight is particularly important when it comes to problems related to cybersecurity policy. Legislative responses are often considered inadequate or insufficient to address these problems; it is thus crucial for parliaments to understand the contribution of governmental policies, programmes, and responses to policy-related issues. Some MPs may be willing to engage more in oversight activities if they are convinced of the effectiveness of their oversight activities. The key question is therefore how to define the success of proactive oversight activities.

¹³ See, for example, an inquiry on hate speech, mis- and disinformation conducted by the Democracy and Digital Technologies Select Committee in 2019-2020. For more details about this inquiry, see Section 3.2 (for examples of comprehensive policy analyses).

¹⁴ IPU (Inter-Parliamentary Union) and UNDP (United Nations Development Programme). 2017. *Parliament's Power to Hold Government to Account: Realities and Perspectives on Oversight*. Global Parliamentary Report, p. 11.

¹⁵ Ibid., p. 11.

3.1 Evaluating the success of proactive oversight activities

As outlined above, the principal goal of proactive oversight activities is to collect information. This may be for a variety of purposes, including:

1. to make decisions about the adequacy of existing policies versus the need for new legislation;
2. to evaluate the allocation of budgets; and
3. to influence foreign policy and diplomatic responses to specific issues.

To ensure successful proactive oversight, the collection of information must support one of these three objectives. It is therefore considered a successful form of oversight if it leads to more rational and well-informed decisions by the government and the parliament itself.¹⁶ Rational and well-informed decisions by the executive and the legislator, developed through a dialogue between both powers, will most likely lead to better policy solutions.

In other words, the collection of information is a successful form of oversight if it supports a dialogue between the parliament and the government and thereby leads to rational and well-informed decisions. A dialogue between the parliament and its government requires, *inter alia*, that parliamentarians have a good understanding of governmental policies and related challenges.¹⁷ The following section illustrates efforts by German, Swiss, and UK parliaments to increase their understanding of problems related to cybersecurity policy and their governments' policy responses.

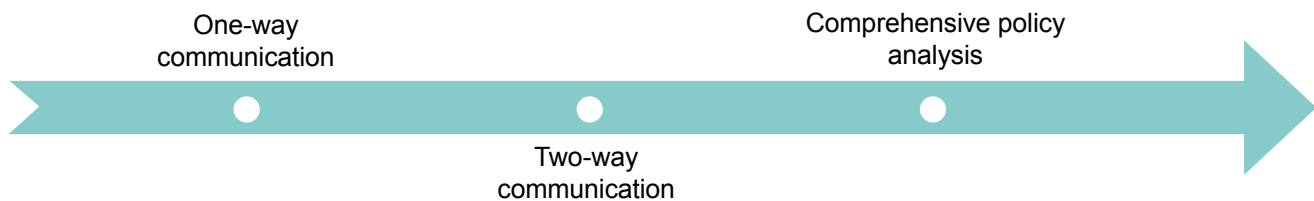
3.2 Examples of proactive oversight activities of cybersecurity policies

The following proactive oversight activities aim to acquire different levels of knowledge. Parliamentarians use different investigative tools depending on the level of information required. A parliamentary question might, for example, only aim to understand the position of the government on a particular policy problem, while a parliamentary committee might aim to understand how this problem can be addressed by different stakeholders, including the government, parliament, and actors from the private sector.

¹⁶ 'Improvement in the democratic process as a result of effective oversight can be measured by, for example: Recommendations made by committees or other parliamentary organs being evaluated on their merits, and accepted or rejected by government on the basis of rational and publicly-articulated responses' (Ibid., p. 15).

¹⁷ 'Benefits of oversight include increased knowledge and understanding of government policies' (Ibid., p. 16).

Chart 3: Level of investigation



One-way communication can take the form of a parliamentary question or hearing. Many proactive oversight activities are implemented through one-way forms of communication. The objective of this oversight tool is to gain information about governmental activities without providing feedback or engaging in any further dialogue – at least for the time being.

Example: Parliamentary questions about specific cyber incidents and potential responses of the German federal government ('Kleine Anfrage' 2018)¹⁸

- Does the federal government have insights into who the actors are behind the 'Not-Petya' cyber-attack?¹⁹
- Does the federal government consider reacting militarily (conventional and/or digital) to cyber-attacks?²⁰ In the event of potential 'hackbacks', how does the federal government intend to ensure that uninvolved actors, such as hospitals or power grids, do not become collateral victims of a cyber counterattack initiated by the Federal Republic of Germany?²¹
- What procedures do the federal ministries and their subordinate authorities and bodies have in place for dealing with IT security gaps or IT vulnerabilities that they identify, or become aware of, in the course of their work?²²

Two-way communication entails feedback from the receiver, and oversight tools may trigger a more in-depth dialogue between parliament and government. The following example shows how a form of communication originally intended as 'one way' can evolve into a two-way dialogue, as well as the limits of this type of oversight.

¹⁸ The government generally responds to 'Kleine Anfragen' in writing (§104 (2) GOBT) and without a discussion in the plenary. Another important oversight tool is referred to as 'Grosse Anfrage' – it requires a minimum ... and it is Note as well that all of these questions were asked before the German federal government has published its position paper '[On the Application of International Law in Cyberspace](#)' (March 2021).

¹⁹ Deutscher Bundestag. 2018. Kleine Anfrage, [BT-Drucksache 19/2009](#) (04.05.2018): 'Liegen der Bundesregierung Erkenntnisse vor, wer hinter dem Cyber-Angriff "NotPetya" steckt?'

²⁰ Deutscher Bundestag. 2018. Kleine Anfrage, [BT-Drucksache 19/2009](#) (04.05.2018): 'Behält sich die Bundesregierung vor, auf Cyber-Angriffe auch militärisch (konventionell und/oder digital) zu reagieren?'

²¹ Deutscher Bundestag. 2018. Kleine Anfrage, [BT-Drucksache 19/2032](#) (07.05.2018): 'Wie gedenkt die Bundesregierung im Falle einer potentiellen Einführung von Hack Backs sicherzustellen, dass unbeteiligte Akteure, wie z. B. Krankenhäuser oder Stromnetze, sowie alle anderen ausländischen informationstechnischen Systeme, die in Deutschland zur kritischen Infrastruktur gehören würden, nicht zu Kollateralschäden eines von der Bundesrepublik Deutschland initiierten Cybergegenangriff werden?'

²² Deutscher Bundestag. 2021. Kleine Anfrage, [BT-Drucksache 20/262](#) (14.12.2021): 'Welche Routinen existieren in den Bundesministerien und ihren nachgeordneten Behörden und Stellen zum Umgang mit IT-Sicherheitslücken bzw. IT-Schwachstellen, die sie gefunden haben oder die ihnen in Ausübung ihrer Tätigkeit zur Kenntnis gelangt sind?'

Example: Question about Switzerland's neutrality policy on cyberwar ('Interpellation' 2021)²³

- ◇ 31 May 2021 - written questions asked by an MP:
 - Has the Federal Council carried out an in-depth clarification as to how the neutrality law is to be applied in cyberspace and in cyber warfare?
 - Which forms and intensity of international cooperation in this area are compatible with permanent neutrality?²⁴
- ◇ 1 September 2021 - written response received from the Federal Council²⁵
- ◇ 30 September 2021 - oral feedback received from the MP, along with a request for a debate.²⁶

The MP expressed his partial satisfaction with the response of the Federal Council. While he does not expect the government to have a final answer to all his questions, the MP highlights the need to reflect on these topics now and to connect 'technical, security policy, and international law aspects'. He argues that the government cannot expect to find solutions from international consultations and specifies questions that require further attention, including the following:

- Which agreements with other states are permissible in terms of neutrality policy?
- How does the Federal Council ensure that the Swiss infrastructure is not used for cyber-attacks and how does it react?'

He asks the Federal Department of Foreign Affairs (FDFA) to lead the policy development process in this regard.

- ◇ 30 September 2021 - oral response from Federal Council Ignazio Cassis, FDFA:²⁷

The Federal Council agrees on the importance of cybersecurity foreign policy and highlights that the Swiss Strategy of Digital Foreign Policy 2021-2024 includes a focus on cybersecurity policy. In addition, the FDFA has created a new department of digitalization that shall also address cybersecurity foreign policy. Regarding the protection of critical infrastructure, the Federal Council states that this is outside the responsibilities of the FDFA.

The example shows that two-way communication oversight tools support a dialogue between parliament and government. Foreign policy is, however, a core function of the government, and this

²³ Note that an interpellation is a parliamentary question of important inner or foreign policy events or issues. The written response of the Federal Council may be discussed orally in one of its sessions. In addition, written and oral oversight tools are available regarding all other governmental policies. For further details in German, see the website of the Swiss confederation '[Organisation des Parlements](#)'.

²⁴ [Interpellation MP Damian Müller, 21.3614](#) (31.05.2021): 'Hat der Bundesrat eine vertiefte Abklärung vorgenommen, wie das Neutralitätsrecht im Cyberraum und in der Cyberkriegsführung anzuwenden ist? Welche Formen und Intensität der internationalen Zusammenarbeit sind (...) mit der dauernden Neutralität vereinbar?'

²⁵ Ibid., Stellungnahme des Bundesrates (01.09.2021).

²⁶ [Votum MP Damian Müller, 21.3614](#) (30.09.2021): 'Welche Absprachen mit anderen Staaten sind neutralitätspolitisch zulässig? (...) Wie stellt der Bundesrat sicher, dass die schweizerische Infrastruktur nicht für Cyberangriffe genutzt wird, und wie reagiert er?'

²⁷ [Votum Federal Council Ignazio Cassis, 21.3614](#) (30.09.2021).

example demonstrates the limits of parliamentary oversight in this regard. It also illustrates that a coherent and comprehensive public policy development of cybersecurity requires many public entities to work together. A dialogue is needed not only between parliament and government, but also between governmental departments responsible for different aspects of cybersecurity. This is a frequent challenge for issues related to cybersecurity policy.

Parliaments could play an important role in overcoming this challenge by creating cross-sectional committees that investigate cybersecurity policy problems in depth. This leads to the last category of proactive parliamentary oversight activities: parliamentary investigations that aim to ensure a comprehensive policy analysis. A comprehensive analysis of a given policy problem may be conducted by the governmental department themselves²⁸ or by parliamentary committees.

Example: Inquiry on hate speech and mis- and disinformation conducted by the Democracy and Digital Technologies Lords Select Committee in 2019-2020²⁹

Over the course of almost ten months, the committee collected oral and written evidence from expert witnesses. The in-depth analysis included a variety of policy issues and concepts, including the accountability of technology platforms, transparency, digital literacy, informed citizens, and elections. Based on this analysis, the report concludes with 45 recommendations for future parliamentary actions, governmental policies, and other activities.

The example shows that the most comprehensive oversight is thus conducted by parliamentary committees. While there is sometimes scepticism about whether the UK select committees really matter for governmental policy decisions, academic research shows that, in the past, numerous policy recommendations have been implemented and instigated major policy changes.³⁰ The UK select committee system is different from the parliamentary committee system in Germany and Switzerland; however, parliamentary committees in all of these jurisdictions play a pivotal role in parliamentary oversight.³¹

²⁸ The decision to ban Huawei 5G equipment from the network was taken by the UK prime minister. The related policy analysis for this decision was conducted by the UK Department for Digital, Culture, Media and Sport. The Telecommunication Security Bill obliging telecom providers to completely exclude Huawei by 2027 was also introduced by the Department for Digital, Culture, Media and Sport. See Intelligence and Security Committee of Parliament. 2021. *Annual Report 2019-2021*, para. 37. While it was originally the UK Intelligence and Security Committee

²⁹ UK Democracy and Digital Technologies Select Committee. 2021. *Digital Technology and the Resurrection of Trust*. Report of Session 2019-21.

³⁰ Benton, Meghan and Meg Russell. 2012. 'Assessing the Impact of Parliamentary Oversight Committees: The Select Committees in the British House of Commons', *Parliamentary Affairs*, Vol. 66, Iss. 4, September, pp. 772-797.

³¹ Griglio, Elena. 2020. 'Classifying Oversight Tools According to Parliamentary Practice', in *Parliamentary Oversight of the Executives: Tools and Procedures in Europe*, ch. 3, p. 86.

4. Parliamentary committees overseeing cybersecurity policies

The following section briefly summarizes the different types of parliamentary oversight committees. It concludes by outlining parliamentary committees overseeing national cybersecurity agencies and highlighting other key issues related to cybersecurity policy.

4.1 Types of parliamentary oversight committees

Most parliaments have permanent and temporary committees. The responsibilities of permanent committees often mirror those of governmental departments or are limited to highly sensitive issues of national security and defence. They are often defined in either the constitution or the parliaments rules of procedure. In addition, some parliaments have temporary committees that may be established to investigate a specific policy area.³²

Examples: In Germany, the parliament establishes permanent committees at the beginning of each legislative period. Four committees are mandatory according to the constitution.³³ The others can be established based on the parliament's stated priorities. In addition, the parliament may establish temporary committees (so-called Enquete-Commissions) to investigate specific policy issues in a comprehensive manner.³⁴

In Switzerland, the standing committees are determined in the rules of procedure of the National Council and the Council of States.³⁵

The distinction between the functions of parliamentary committees is even more relevant to this paper. Some countries have a hybrid committee system, meaning that the same parliamentary committee is responsible for preparing legislation and collecting information about governmental policies. The collected information then flows directly into the draft legislation. In hybrid committee systems, no single parliamentary committee has exclusive responsibility for conducting oversight of the executive.

³² These should not be confused with ad-hoc committees of inquiry, which are established to investigate a particular governmental performance or issue (ex post).

³³ The German constitution determines four standing committees: the Committee for the Affairs of the European Union (art. 45), the Foreign Affairs Committee (art. 45a), the Defence Committee (art. 45a), and the Petitions Committee (art. 45c).

³⁴ Note that these committees may consist of parliamentarians and subject-matter experts.

³⁵ Art. 10 of the [Standing Orders of the National Council](#) (03.10.2003) and Art. 7 of the [Standing Orders of the Council of States](#) (20.06.2003).

Example: In Germany, the principal function of permanent committees is to prepare for the legislative negotiations of the plenary.³⁶ This function entails extensive evidence-gathering and exchange with the government.³⁷ No parliamentary committees are exclusively responsible for overseeing governmental policies or financial budgets.³⁸

Another type of committee system locates the oversight function in specific non-legislative committees.

Examples: In Switzerland, standing supervisory committees are responsible for overseeing the financial budget and conduct of business of the Confederation.³⁹

In the UK, select committees deal with executive oversight, whereas general committees are concerned with legislation. The Commons Select Committees shadow government departments⁴⁰ and examine their spending, policies, and administration.⁴¹

Finally, parliamentary committees may also have the exclusive role of investigating specific policy areas or problems. These types of committees rely heavily on subject-matter experts and are particularly relevant in the field of tech and cybersecurity policy.

Examples: In the UK, the Lords Select Committees investigate special policy subjects, taking advantage of the Lords' greater amount of time (compared with the MPs on the Commons Select Committees).⁴² The above-mentioned Lords Select Committee on Democracy and Digital Technologies and its inquiry on hate speech and mis- and disinformation is one example of an investigation into a special tech and cybersecurity subject.⁴³

³⁶ § 54 Parliamentary Rules of Procedure (GOBT).

³⁷ See also: Griglio, Elena. 2020. 'Classifying Oversight Tools According to Parliamentary Practice', in *Parliamentary Oversight of the Executives: Tools and Procedures in Europe*, ch. 3, p. 90.

³⁸ Note that the Budget Committee has the hybrid role of preparing the financial plan for the upcoming year and controlling the expenses of the past year.

³⁹ See the definition of 'Supervisory Committees' in the Lexicon of Parliamentary Terms. Each chamber – the National Council and the Council of States – has one finance and one control committee. Supervisory committees are different from [specialist committees](#), which exclusively follow developments and consult on topics related their specific responsibilities (this may, but does not have to, include the drafting of legislation). See the Swiss Confederation's [Organisation des Parlements](#) website.

⁴⁰ There are a total of 26 ministerial departments. See the UK government [Departments, agencies and public bodies](#) website.

⁴¹ See the UK parliament's [Select Committees](#) website. For an example of the oversight of cybersecurity expenditures, see House of Commons Committee of Public Accounts. 2019. *Cyber Security in the UK*. Ninety-Ninth Report of Session 2017-19. 15 May.

⁴² See the UK parliament's [Select Committees](#) website.

⁴³ UK Democracy and Digital Technologies Select Committee. 2020. *Digital Technology and the Resurrection of Trust*. Report of Session 2019-21.

In Germany, the above-mentioned temporarily established Enquete-Commissions also investigate special policy subjects. While there are usually no more than one or two of these committees established in each legislative period, they have proven to be particularly relevant for tech policy topics. A recent Enquete-Commission, for example, investigated the challenges and opportunities of artificial intelligence.⁴⁴ Previously, another commission considered the impact of the internet on society, the economy, and politics.⁴⁵

4.2 Oversight of national cybersecurity agencies and policies

Parliamentary oversight is a difficult concept to capture given its different forms (ex post versus ex ante) carried out by divergent types of parliamentary committees. Oversight of cybersecurity policies is particularly complex because of the diversity of parliamentary committees dealing with different elements. This final section provides an overview of parliamentary committees overseeing national cybersecurity agencies and other key issues related to cybersecurity policies in Germany, Switzerland, and the UK.

Over the past decade, all these states have established a national cybersecurity agency. They have grown out of different ministerial departments. The parliamentary committee responsible for the oversight of the national cybersecurity agency depends on the agency's historical origin.

The **German Federal Office of Information Security (BSI)** was originally created in 1990. As a federal agency under the Ministry of the Interior, it was primarily responsible for supporting federal agencies and law enforcement to strengthen their information technology (IT) security.⁴⁶ Since 2015, it has been responsible for IT security in general, in addition to that of the federal administration.⁴⁷ In the German hybrid committee system, oversight is conducted by the parliament's Internal Affairs Committee.

The **Swiss National Cyber Security Centre (NCSC)** was established only recently in 2020.⁴⁸ It is the overarching organization of the Swiss Confederation in the area of cyber risks.⁴⁹

⁴⁴ The Committee on 'Artificial Intelligence: Societal Responsibility and Economic, Social and Ecological Potentials (2018-2020)': see Einsetzungsantrag Enquete-Kommission 'Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale', [BT-Drucksache](#) 19/2978 (26.06.2018).

⁴⁵ The Committee on 'Internet and Digital Society (2010-2013)': see Einsetzungsantrag Enquete-Kommission 'Internet und digitale Gesellschaft', [BT-Drucksache](#) 17/950 (03.03.2010).

⁴⁶ § 3 BSI-Errichtungsgesetz (17.12.1990).

⁴⁷ Law for Increasing the Security of Information Technology Systems (IT Security Act/IT Sicherheitsgesetz) (15.07.2015).

⁴⁸ The Cyber Risks Ordinance from May 2020 is the legal basis for the creation and expansion of the NCSC, and regulates 'the organisation of the Federal Administration for its protection against cyber risks as well as the tasks and responsibilities of the various offices in the cyber security domain' (Ordinance on Protection against Cyber Risks in the Federal Administration (Cyber Risks Ordinance) (27.05.2020), art.1).

⁴⁹ <https://www.ncsc.admin.ch/ncsc/en/home/ueber-ncsc/organisation.html>

The NCSC coordinates the work of public agencies and ministerial departments in the cyber-security domain.⁵⁰ In the Swiss parliament, the security policy committee is responsible for following developments and consulting on cybersecurity and cyber defence.

The **UK National Cyber Security Centre (NCSC)** was launched in 2016 and is part of the Government Communications Headquarters (GCHQ) – the UK’s intelligence and security organization.⁵¹ The NCSC assists the public and private sector in addressing cybersecurity risks.⁵² As part of the UK intelligence organization, the UK Intelligence and Security Committee of Parliament conducts oversight of the NCSC.⁵³

In addition to overseeing national cybersecurity agencies, parliaments also carry out oversight activities related to other key cybersecurity policy issues – which are often relevant to a wide variety of other policies. The following chart provides an overview of topics that are particularly relevant to cybersecurity policies and the parliamentary committees responsible for overseeing them.

Key topics for cybersecurity ⁵⁴	Responsible parliamentary committee ⁵⁵
Similar type of parliamentary oversight committee	
<ul style="list-style-type: none"> – Arms exports – Military cyber capabilities (defensive or offensive) 	DE: Defence Committee CH: Security Policy Committee UK: Common Select Defence Committee
<ul style="list-style-type: none"> – Relations with international organizations (NATO, UN, EU) – International law 	DE: Foreign Affairs Committee CH: Foreign Affairs Committee UK: Common Select Foreign Affairs Committee
<ul style="list-style-type: none"> – Law enforcement coordination – Criminal law (including cross-border cooperation) 	DE: Internal Affairs Committee CH: Security Policy Committee (for law enforcement coordination) and Legal Affairs Committee (for cross-border cooperation on criminal law matters) UK: Common Select Home Affairs Committee

⁵⁰ Art. 12, [Cyber Risks Ordinance](#) (27.05.2020)

⁵¹ NCSC, [‘The Launch of the National Cyber Security Centre: A Snapshot of the Past, Present and Future of Cyber Security’](#).

⁵² Website of the UK National Cyber Security Centre [‘About the NCSC – What we do’](#).

⁵³ See Intelligence and Security Committee of Parliament. 2021. ‘Annual Report 2019-2021’. HC 877 (10.12.2021). The Intelligence and Security Committee of Parliament is a joint committee with nine members from both houses of parliament (see the [committee’s website](#)).

⁵⁴ Additional topics not covered in this generic overview include consumer protection, competition rules, the protection of financial institutions, and support for small and medium-sized companies.

⁵⁵ The responsibilities of the respective parliamentary committees are based on the following resources: for Germany, the hybrid permanent committee’s responsibilities regarding the shadowing of ministries – there are often several committees involved but only one leading committee; for Switzerland, the websites of the committees that enlist their support; and for the UK – regarding the Commons Select Committees – the responsibilities of UK ministerial departments.

Significantly different parliamentary oversight committee	
Protection of critical infrastructure	DE: Internal Affairs Committee CH: Security Policy Committee (as civil protection is part of the Department of Defence, Civil Protection and Sport) UK
IT security of products	DE: Internal Affairs Committee CH: Economic Affairs and Taxation Committee UK: Common Select Digital, Culture, Media and Sport Committee
Disinformation	UK: Lords Select Committee on Democracy and Digital Technologies Note: In Germany, the EU Commissions Code of Practice on Disinformation is more relevant than debates within the national parliament.

5. Summary conclusion

The present report has shown that the collection of information is the most relevant form of oversight in the field of cybersecurity policies. Challenges related to cybersecurity policies are relatively new, and governments are still experimenting with different responses. Policy solutions also require a comprehensive analysis of the responsibilities of all actors from the public and private sector. Parliamentary oversight plays a key role in this regard.

While MPs understand the importance of oversight activities, they do not always prioritize those that are considered particularly time intensive. This is understandable given the challenges of assessing the impact of certain oversight activities, particularly proactive activities that aim to improve understanding of a specific policy issue. This paper, however, has shown that MPs have tools to engage in oversight activities of different depth and consequently as well different time commitments. One-way communication tools, including simple questions or interpellations, can already increase understanding and awareness of certain cybersecurity policies or governmental actions.

Finally, the paper highlights the fundamental importance of parliamentary committees in conducting oversight. It may seem irrelevant to compare oversight committees in different countries since parliamentary committee systems differ between states and cybersecurity policy issues are addressed under a variety of other policy issues; however, the diverse functions of oversight committees can also help parliaments with less developed oversight activities to develop their own approach to overseeing cybersecurity policies.

6. Annexes

The following annexes summarize the key points for each country:

Annex 1: Summary of Germany case study

- The parliament establishes four permanent committees at the beginning of each legislative period, which conduct extensive evidence-gathering and exchange with the government.
- Based on structure of the hybrid permanent committee's shadowing responsibility of ministries, there are often several committees involved but only one leading committee.
- Other committees can be established based on the parliament's stated priorities, including temporary committees (so-called Enquete-Commissions) to investigate specific policy issues.
- While there are usually no more than one or two Enquete-Commissions established in each legislative period, they have proven particularly relevant for tech policy topics. A recent Enquete-Commission investigated artificial intelligence (2018-2022) and another considered the internet and digital society (2010-2013).
- There has been one inquiry committee on the background and scope of foreign secret service activities within Germany (also referred to as the NSA inquiry committee).
- The Internal Affairs Committee oversees the BSI, which was created in 1990 – under the Ministry of the Interior – to strengthen IT security within federal agencies and law enforcement.

Annex 2: Summary of Switzerland case study

- The standing committees are determined in the rules of the country's two parliamentary structures: the National Council (lower house) and the Council of States (upper house). These committees oversee the financial budget and conduct of business of Switzerland.
- In relation to cybersecurity, the Security Policy Committee oversees military cyber capabilities, critical infrastructure protection, and law enforcement coordination (which also involves the Legal Affairs Committee); the Foreign Affairs Committee oversees relations with international organizations; and the Economic Affairs and Taxation Committee oversees the IT security of products.
- The Security Policy Committee also oversees the Swiss NCSC, which was created in 2020 as the overarching organization of the Swiss confederation in the area of cyber-risks and

coordinates public agencies and ministerial departments in the cybersecurity domain.

- Conversely, specialist committees are exclusively responsible for following developments and consulting on topics within their specific responsibilities. This may, but does not have to, include the drafting of legislation.
- A parliamentary investigation committee has only been deployed four times for cybersecurity-related issues, the last time being in 1996.

Annex 3: Summary of UK case study

- Select committees deal with executive oversight, whereas general committees are concerned with legislation. The Commons Select Committees shadow government departments and examine their spending, policies, and administration.
- Unlike most European states, the UK's constitution does not provide for inquiry committees. The UK system of select committees has, to a certain degree, similar objectives and procedures to inquiry committees in other European states. The difference, however, is that they have open-ended mandates, and inquiries conducted by select committees in the UK are not limited to the investigation of governmental actions or policies on a specific past issue. They may also investigate a particular issue to shape a future government policy.
- The Lords Select Committees investigate special policy subjects, taking advantage of the Lords' greater amount of time (compared with the MPs on the Commons Select Committees). The above-mentioned Lords Select Committee on Democracy and Digital Technologies and its inquiry on hate speech and mis- and disinformation is one example of an investigation into a special tech and cybersecurity subject.
- The UK Intelligence and Security Committee of Parliament forms part of the GCHQ – the UK's intelligence and security organization – and oversees the NCSC, which was launched in 2016 to assist the public and private sector in addressing cybersecurity risks.

Annex 4: Resources

Studies and reports on parliamentary oversight

- Inter-Parliamentary Union (IPU) and United Nations Development Programme (UNDP). 2017. [Parliament's Power to Hold Government to Account: Realities and Perspectives on Oversight](#). Global Parliamentary Report.
- Pavy, Eeva 2020. [Committees of Inquiry in National Parliaments: Comparative Survey](#). Document requested by the European Parliament's Committee on Citizens' Rights and Constitutional Affairs. March.

Parliamentary databases

- Germany: [Dokumentations- und Informationssystem für Parlamentsmaterialien \(DIP\)](#) – only available in German
- Switzerland: [Curia Vista - Database of parliamentary proceedings](#) (e.g. for interpellations) – most documents are only available in German and French); [Official Bulletin](#) (for oral statements and debates)
- UK: Parliamentary committees' [background and documents](#)

Unrealized potential: ombuds institutions and oversight of cybersecurity in the Western Balkans

by Luka Glušac¹

¹ Assistant Director and Research Fellow at the Institute for Philosophy and Social Theory, University of Belgrade, and former Senior Adviser in the Office of the Protector of Citizens (Ombudsman) of Serbia and Programme Manager at DCAF – Geneva Centre for Security Sector Governance. Email:

Table of contents

1.	Introduction.....	27
2.	The ‘Triple A’ framework.....	28
3.	Authority: normative preconditions.....	29
4.	Ability: technical expertise.....	34
5.	Attitude: developing a culture of oversight.....	37
6.	Gaps and opportunities.....	41

1. Introduction

This chapter looks at how Western Balkan² ombuds institutions can oversee cybersecurity and human rights in cyberspace. It explores their mandate, powers, and functions, and argues that the current legal framework of ombuds institutions in the region allows them to perform these tasks successfully. It notes, however, that this potential remains largely untapped, due to a lack of commitment and technical expertise. The paper explores the steps needed to enable ombuds institutions to work more systematically and consistently in this area, including by cooperating with the legislature and other independent oversight bodies, such as equality bodies and information commissioners.

In the context of this chapter, cybersecurity is defined as both the state of being protected in cyberspace and the measures taken to achieve this. As such, cybersecurity requires not only technical solutions to protect information and communications technologies (ICTs) and services against attacks and incidents, but also a system of governance that sets out the roles and responsibilities of those involved in providing, managing, and overseeing cybersecurity.³

In this chapter, ombuds institutions are defined as independent oversight bodies that receive complaints and investigate matters pertaining to the protection and promotion of human rights and the prevention of maladministration.⁴ This definition is consistent with the modern notion of an ombuds institution as an independent public authority overseeing the work of public administration as well as a human rights institution. With its unique position, independent of the three traditional branches of government (the executive, legislature, and judiciary), ombuds institutions can play an auxiliary role by ensuring checks and balances between state powers. They are therefore increasingly described as forming part of a fourth branch of government, together with other independent constitutional (expert) oversight bodies.

The chapter begins by presenting the analytical framework, based on the ‘three As’ – authority, ability, and attitude – which is then applied to ombuds institutions in the Western Balkans in the context of cybersecurity and human rights in cyberspace.

² The Western Balkans comprise Albania, Bosnia and Herzegovina, Kosovo,* Montenegro, North Macedonia, and Serbia.

* The designation of Kosovo is without prejudice to positions on status, and is in line with UN Security Council Resolution 1244 and the International Court of Justice Opinion on the Kosovo declaration of independence.

³ DCAF. 2021. *Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach*. Geneva: DCAF, p. 6.

⁴ The term ‘ombudsman’ is gender-neutral, since it is derived from a Swedish word and the ‘man’ suffix is gender-neutral in Swedish. It therefore applies correctly to both male and female ombudsmen. Many states, however, use a different term for female incumbents (such as ‘ombudswoman’, ‘ombudsfrau’, or ‘médiatrice’). When referring specifically to a head of institution, the paper uses gender-sensitive terminology. The study uses the term ‘ombuds institutions’ when referring to these institutions in general. When referring to a specific institution, the official legal names are used, such as the People’s Advocate (Albania) or the Protector of Human Rights and Freedoms (Montenegro).

2. The ‘Triple A’ framework

To assess the legal and practical potential of ombuds institutions in the Western Balkans to oversee cybersecurity, this paper uses the so-called ‘Triple A’ framework. The framework was developed to be apply to parliaments and their role in security sector governance,⁵ but has been adapted here for ombuds institutions.

The underlying logic of this framework is that the role of ombuds institutions in overseeing cybersecurity is contingent upon its powers, capacity, and willingness to hold the government to account for its actions – that is, to oversee cybersecurity institutions and protect human rights in cyberspace. Powers, capacity, and willingness are translated into three categories: ‘authority’, ‘ability’, and ‘attitude’.⁶

In general, authority refers to the formal powers needed to hold the government accountable. Ability means having the resources, staff, and expertise required to do so, while attitude refers to the willingness and commitment to fulfill the mandate. Table 1 applies this framework to the specific case of ombuds institutions.

Table 1: The Triple A framework

Authority	Ability	Attitude
Ombuds institutions must have sufficient normative and legal authority to oversee the security sector, including cybersecurity. Most countries have constitutions, basic laws, regulations, or statutes that confer this authority formally, but in practice this authority is not always exercised or respected.	Ombuds institutions must have sufficient resources to effectively fulfil their constitutional and legal roles, including institutional support, access to information, analytical and research capacity, specialized skills, and working relationships with security institutions, other state authorities, and civil society.	Ombuds institutions must maintain a strong commitment to exercising their mandate vis-à-vis the security sector, particularly when such activities encounter resistance from within and outside the security institutions.

⁵ Born, H., ed. 2003. *Parliamentary Oversight of the Security Sector: Principles, Practices and Mechanisms*. Geneva: DCAF and IPU; Born, H. and H. Hänggi. 2005. ‘Governing the use of force under international auspices: deficits in parliamentary accountability’, in *SIPRI, SIPRI Yearbook 2005: Armaments, Disarmament and International Security*, pp. 199-222. Stockholm: SIPRI; Reimers, D. 2021. ‘Strengthening the Role of Parliaments in SSG: Challenges and Remedies from Selected Case Studies’, in DCAF, *Strengthening the Role of Parliaments in SSG – Challenges and Opportunities from Selected Case Studies*. Geneva: DCAF, pp. 6-21.

⁶ George, B. and J. Morgan. 1993. *Parliament and national security*. Paper presented at the Conference on Redefining Society-Military Relations from Vancouver to Vladivostok, Birmingham, 16-18 April 1999.

Combined, these three elements constitute the necessary conditions for effective oversight and enable ombuds institutions to contribute to good (cyber)security sector governance; yet, on their own, none are sufficient.⁷ While having the mandate and powers to oversee the security sector is a necessary precondition for effective oversight, formal powers may be strong but not exercised in practice – either due to a lack of institutional capacity or resources, or a lack of commitment to focusing on the security sector.

The following section applies this framework to ombuds institutions in the Western Balkans in the context of cybersecurity.

3. Authority: normative preconditions

Ombuds institutions must have sufficient normative and legal authority to oversee the security sector, including cybersecurity. Most countries have constitutions, basic laws, regulations, or statutes that confer this authority formally. In practice, however, this authority is not always exercised or respected. This is the case in the Western Balkans. Legally, nothing prevents ombuds institutions from playing an active role in cybersecurity. In fact, they have a myriad of powers and functions that allow them to employ a comprehensive preventive and reactive approach to protecting and promoting human rights in cyberspace and overseeing cybersecurity.

All Western Balkan economies have general national parliamentary ombuds institutions with similar designs, mandates, and powers. They are all established by the constitution and/or international agreements (in the case of Bosnia and Herzegovina and Kosovo) and therefore have the strongest guarantees of independence.

All ombudspersons are appointed by their respective national parliaments, to which they are accountable and report to. The parliament should be a key interlocutor and partner of the ombuds institution. The impacts of the ombuds institution's final decisions or recommendations are not based on coercion but rather on consent, or even persuasion. In other words, ombuds institutions rely on the power of authority – that is the power of their arguments and findings to make public administration bodies comply with their recommendations – rather than on the authority of power. However, when that does not happen, the parliament should get involved, to push the public authorities to comply with ombuds' recommendations, exercising its essential function: oversight of the executive.⁸

⁷ Reimers, D. 2021. 'Strengthening the Role of Parliaments in SSG: Challenges and Remedies from Selected Case Studies', in DCAF, *Strengthening the Role of Parliaments in SSG – Challenges and Opportunities from Selected Case Studies*. Geneva: DCAF, p. 10.

⁸ Glušac, L. 2019. *Assessing the relationship between parliament and ombudsman: evidence from Serbia (2007–2016)*. *The International Journal of Human Rights*, Vol. 23, Iss. 4, p. 534.

An ombuds institution is an independent oversight authority, however, the parliament must not interfere with the work of this body or give it specific instructions or orders. The concept of independence presupposes that ombuds institutions are free from the influence of any political authority, including the parliament.

The independence of ombuds institutions is not 'a privilege established for anyone's comfort, but a requirement and a necessity needed to ensure that human rights protection does not depend on daily politics'.⁹ Independence is indeed an essential characteristic of ombuds institutions; without independence, it is no longer an ombuds institution.¹⁰ The institution's independent status means that its decisions are not influenced by any external entity. This applies not only to the executive, but also to the other branches of the state, as well as to any other public or private entity – such as private companies, civil society organizations (CSOs), and citizens (including complainants).

Ombuds institutions are *de jure* (formally) independent to the degree that legislation forbids any external influence on their work, such as instructions, inducements, threats, or considerations of political or other preferences. *De facto* (actual) independence refers to the degree to which the agency makes day-to-day decisions without any external interference from political parties, the authorities they oversee, the media, or citizens. Ombuds institutions must make decisions without taking into consideration any explicit or implicit, or expressed or intended, wishes or interests of external entities.

All Western Balkan ombuds institutions are so-called hybrid ombuds institutions, meaning they have a dual mandate: (1) to fight maladministration by controlling the work of public administration; and (2) to protect and promote human rights.

There is no generally accepted definition for the 'protection' and 'promotion' of human rights. Even the most elaborated international standards in this area – the Venice Principles on the Protection and Promotion of the Ombudsman Institution¹¹ and the Paris Principles Relating to the Status of National Human Rights Institutions (NHRIs)¹² – do not define the 'protection' and 'promotion' of human rights. The Subcommittee on Accreditation of the Global Alliance of NHRIs (GANHRI SCA), the expert peer body in charge of the NHRI accreditation, does however provide useful guidelines in this regard. The GANHRI SCA understands 'promotion' to include functions

⁹ OHCHR (UN Human Rights Office of the High Commissioner). 2012. *Strengthening the Bond between Parliaments and National Human Rights Institutions*. 2 April.

¹⁰ Glušac, L. 2021. *A Critical Appraisal of the Venice Principles on the Protection and Promotion of the Ombudsman: An Equivalent to the Paris Principles?* *Human Rights Law Review*, Vol. 21, Iss. 1, p. 45.

¹¹ Council of Europe Venice Commission. 2019. *Principles on the Protection and Promotion of the Ombudsman Institution* ('The Venice Principles'). CDL-ad(2019)005. 3 May.

¹² United Nations General Assembly. 1993. *Resolution 48/134 on the Principles relating to the Status of National Institutions* (The Paris Principles). 20 December.

that seek to create a society where human rights are more broadly understood and respected. Such functions may include education, training, advising, public outreach, and advocacy – or, more generally, those that address and seek to prevent actual human rights violations. Tasks may include monitoring, inquiring, investigating, and reporting on human rights violations, as well as handling individual complaints.¹³ A comparative overview of the powers and functions of ombuds institutions in the Western Balkans is given in the table below.

Table 2: Overview of functions and powers of Western Balkan ombuds institutions

	Albania	Bosnia and Herzegovina	Kosovo	Montenegro	North Macedonia	Serbia
Monitoring	x	x	x	x	x	x
Unhindered access to documents, premises, and people	x	x	x	x	x	x
Investigating						
Upon complaint	x	x	x	x	x	x
On own initiative	x	x	x	x	x	x
Issuing recommendations following investigations	x	x	x	x	x	x
Issuing opinions to parliament, government, and public administration bodies	x	x	x	x	x	x
Reporting to the parliament	x	x	x	x	x	x
Annually	x	x	x	x	x	x
Special (periodic)	x	x	x	x	x	x
Providing mediation and good services			x			x
Legislative advice						
Submitting parliamentary bills						x
Submitting amendments to the parliament or the government						x

¹³ Global Alliance of National Human Rights Institutions (GANHRI). 2018. *General Observations of the Sub-Committee on Accreditation*. 21 February.

Advising competent authorities to prepare amendments	x	x	x	x	x	x
Providing opinions on draft legislation to the government or ministries	x		x	x	x	x
Initiating proceedings before the constitutional court for the assessment of the constitutionality and legality of laws, other regulations, and general acts	x		x	x	x	x
Education and training	x	x	x	x	x	x
Awareness raising	x	x	x	x	x	x
Public outreach and advocacy	x	x	x	x	x	x

As shown in Table 2, ombuds institutions from the region have very similar powers and functions. The key difference between them relates to the right of legislative initiative, as only the Serbian Protector of Citizens is given an explicit (constitutional) right to propose laws and submit amendments directly to the parliament. Other ombuds institutions may only ‘recommend’ or advise competent authorities to do so. Another difference concerns mediation and good offices, which are explicitly mentioned only in the cases of Kosovo and Serbia.

To comply with the human rights protected and promoted by ombuds institutions in the Western Balkans, national laws all stipulate that these institutions act in accordance with their respective constitutions, laws, and ratified international treaties; the Serbian Law on the Protector of Citizens also explicitly includes ‘generally accepted rules of international law’¹⁴ – that is, international customary law.

Regarding the application of human rights in cyberspace, it is widely accepted that ‘many of the international human rights, whether found in customary or treaty law, that individuals enjoy “offline” are also protected “online”’.¹⁵

All of the functions and powers of ombuds institutions mentioned above also apply to the security sector, because security institutions – such as the police, armed forces, and security or

¹⁴ Serbia. 2021. *Law on the Protector of Citizens*, art. 3.

¹⁵ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 179.

intelligence services – are all elements of public administration, which ombuds institutions have the power to oversee. The security sector therefore falls within the mandate of ombuds institutions, even though neither it nor cybersecurity is explicitly mentioned in the founding legislation of ombuds institutions. In some countries of the region, specialized laws and strategic documents provide for an explicit role for ombuds institutions in the security sector, particularly in terms of oversight. For instance, in North Macedonia, Article 56 of the Law on Interception of Communications gives the ombuds institution a specific role in overseeing the legality of interceptions, with regards to protecting human rights and freedoms.¹⁶

Regarding cybersecurity, it should be noted that national cybersecurity documents of Western Balkan economies do not explicitly recognize the role of ombuds institutions and other oversight bodies in the area of human rights, such as those responsible for ensuring equality, access to information of public importance, and/or personal data protection.¹⁷ This does not, however, legally prevent them from having an active role in protecting and promoting human rights in cyberspace and overseeing the implementation of cybersecurity-related legislation.

Before exploring the capacities and attitudes of ombuds institutions in order to determine whether they fulfill this role in practice, it is important to consider their role as security sector actors. The widely adopted holistic approach to security sector reform (SSR) distinguishes four groups of security sector reform (SSR) actors: (1) state actors that have the right to use force; (2) non-state actors that have the right to use force; (3) state actors that do not have the right to use force; and (4) non-state actors that do not have the right to use force.¹⁸

Ombuds institutions play a particular role among state actors that do not have the right to use force.¹⁹ This is because they are well placed to: (1) contribute to the effective protection of the human rights and freedoms of citizens in the context of security services' activities; (2) reinforce the framework for democratic civilian oversight; and (3) strengthen the democratic foundations underlying security services' operations, thereby improving their work and consequently increasing the public's trust in them.²⁰

¹⁶ Fuior, T. 2021. *Guidelines for Intelligence Oversight: for parliamentary committees in the Assembly of the Republic of North Macedonia*. Geneva: DCAF, p. 129.

¹⁷ DCAF. 2021. *National Cybersecurity Strategies in Western Balkan Economies*. Geneva: DCAF.

¹⁸ Ball, N. 1998. *Spreading Good Practices in Security Sector Reform: Policy Options for the British Government*. London: Saferworld; Edmunds, T. 2002. 'Security Sector Reform: Concepts and Implementation', in W. N. Germann and T. Edmunds, eds., *Towards Security Sector Reform in Post Cold War Europe: A Framework for Assessment*. Baden-Baden: Nomos, pp. 15-31; Hänggi, H. 2004. 'Conceptualizing Security Sector Reform and Reconstruction', in A. Bryden and H. Hänggi, eds., *Reform and Reconstruction of the Security Sector*. Berlin: Lit Verlag, pp. 1-11.

¹⁹ IPU (Inter-Parliamentary Union) and DCAF. 2003. *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices*.

²⁰ Janković, S. 2006. *Democratic Civil Control of Intelligence: Security Services in Serbia* (in Serbian). Belgrade: Belgrade Centre for Security Policy.

Nevertheless, empirical evidence on the activities of ombuds institutions in SSR is, with a few exceptions²¹, notably scarce. The fact that the status of ombuds institutions is rarely acknowledged in the literature can be attributed to the rather modest successes of ombuds institutions and/or the failure to advertise success stories²². Indeed, comparative experiences have shown that ombuds institutions often do not exploit opportunities to oversee the security sector effectively – to the extent possible²³. This also applies to Western Balkan ombuds institutions, which have remained largely inactive in this regard. For instance, ‘despite this strong legal authority for oversight, the North Macedonian Ombudsperson has not been an active human rights defender between citizens and the security and intelligence sector’²⁴. The same could be said for other Western Balkan ombuds institutions. A rare exception was the Serbian Protector of Citizens during the mandate of Saša Janković (2007–17), who was widely recognized as ‘a notable example of an ombudsperson that plays an active role in the oversight of security services’.²⁵ The reason ombuds institutions have such a poor track record of effectively overseeing the security sector in the Western Balkans, including cybersecurity, lies in the other two ‘As’ of the framework: ability and attitude.

4. Ability: technical expertise

Expert knowledge is a key precondition for successful (independent) oversight of the security sector. ‘If ombudspersons do not have expert technical knowledge of security-related issues, experts should be employed to allow substantive activities to be included in their oversight.’²⁶

Ombuds institutions in the Western Balkans do not generally have the capacity to comprehensively oversee the security sector. They primarily lack technical expertise. Some institutions, such as the Montenegrin Protector of Human Rights and Freedoms, have acknowledged this and underlined the need to strengthen institutional capacity and internal systems to be able to effectively oversee the security sector. The donor community has been relatively supportive when ombuds institutions have demonstrated an interest in strengthening their capacity to oversee the security sector. For instance, the Montenegrin Protector of Human Rights and Freedoms joined forces with civil society and the international donor community to improve their capabilities in this

²¹ Kinzelbach, K. and E. Cole, eds. 2007. *Monitoring and Investigating the Security Sector: Recommendations for Ombudsman Institutions to Promote and Protect Human Rights for Public Security*. Geneva: UNDP and DCAF; Born, H., and A. Wills (eds). 2012. *Overseeing Intelligence Services: A Toolkit*. Geneva: DCAF.

²² Glušac, L. 2018. ‘National Human Rights Institutions and Oversight of the Security Services’, *Journal of Human Rights Practice*, Vol. 10, Iss. 1, p. 60.

²³ Council of Europe Commissioner for Human Rights. 2015. *Democratic and Effective Oversight of National Security Services*. Issue Paper. Prepared by Aidan Wills.

²⁴ Fuior, T. 2021. *Guidelines for Intelligence Oversight: for parliamentary committees in the Assembly of the Republic of North Macedonia*. Geneva: DCAF, p. 39.

²⁵ Council of Europe Commissioner for Human Rights. 2015. *Democratic and Effective Oversight of National Security Services*. Issue Paper. Prepared by Aidan Wills, p. 51.

²⁶ Glušac, L. 2018. ‘National Human Rights Institutions and Oversight of the Security Services’, *Journal of Human Rights Practice*, Vol. 10, Iss. 1, pp. 65-66.

area. In 2018, the Centre for Democracy and Human Rights (CEDEM) – in cooperation with the Protector of Human Rights and Freedoms and with the support of the Embassy of the Federal Republic of Germany – implemented the project ‘Strengthening the Institutional Capacities of the Ombudsman for Supervision of the Security Sector’. The results have yet to be observed, however.

The Serbian case is even more illustrative, as the Protector of Citizens has gone from being an exceptional institution to one that shows very little interest in security sector oversight. Petrović argues that the 2017 appointment of Zoran Pašalić as the new Protector of Citizens has had a very detrimental effect on the control and oversight of the security services.²⁷ In contrast to Janković, Pašalić lacks the knowledge and skills required to oversee the security services. This should not, however, have prevented the new Protector of Citizens from effectively exercising oversight of the legality and propriety of security services’ activities.²⁸ With sufficient motivation, the new Protector of Citizens could have tried to retain and drive the employees who had acquired the relevant knowledge – and, in doing so, bridge the gap between knowledge and skills. Instead, the opposite has happened. The new Protector of Citizens’ lack of interest in continuing to work on security sector oversight has pushed in-house experts to leave the office, including those with the highest security clearance.

It is important to note that the Serbian Protector of Citizens did continue two work streams related to the security sector more broadly – torture prevention and general maladministration issues (such as delays in issuing personal documents by the Ministry of Interior or labour disputes in the Ministry of Defence). The Protector of Citizens has, however, experienced serious problems in attracting reputable CSOs to apply for its National Preventive Mechanism against Torture (NPM) roster²⁹, due to a loss of trust and credibility. Despite this, the NPM has continued to perform announced and unannounced visits to possible places of detention, including military facilities, which represents a new and important shift in the context of Serbia which was an important novelty in the Serbian context. The Albanian People’s Advocate has also recently refocused on inspecting the infrastructure used for disciplinary restrictions in military installations – including their physical structure, the provision of basic services, and respect for human rights of military personnel under disciplinary confinement.³⁰

The situation is even more challenging when it comes to cybersecurity and human rights in cyberspace, because overseeing the security sector in cyberspace requires a particular and sought-after

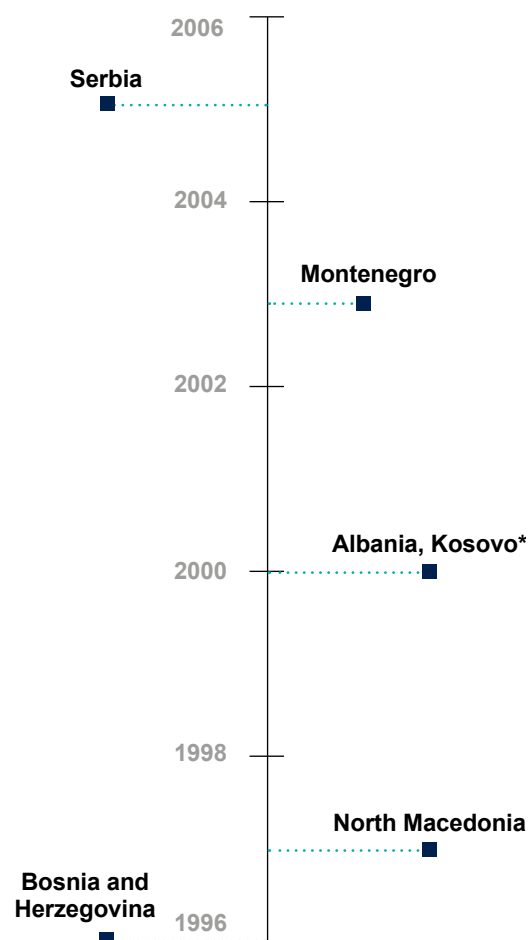
27 Petrović, P. 2020. *The Anatomy of Capturing Serbia’s Security: Intelligence Sector*. Belgrade: Belgrade Centre for Security Policy, pp. 65-67.

28 Ibid.

29 National Preventive Mechanisms (NPMs) are independent visiting bodies, established at the domestic level and composed of one or more bodies, for the prevention of torture and other cruel, inhuman, or degrading treatment or punishment, adopted under the Optional Protocol to the UN Convention against Torture. In Serbia, the role of NPMs is performed by the Protector of Citizens together with the Provincial Ombudsman of Vojvodina and CSOs, which are chosen following a public call for candidates.

30 Dafa, Alban. 2021. *(Un) Democratic Control of the Albanian Armed Forces Centralisation of Defence Policy and Ineffective Oversight*. Tirana: Institute for Democracy and Mediation, p. 32.

ter set of skills. While ombudspersons and their deputies have among the highest salaries in the public sector – usually equivalent to those of the judges of the constitutional courts – the employees in their offices do not. This makes it very difficult to attract highly skilled and experienced staff, particularly from the ICT sector. Furthermore, the oversight of online activities may require a different set of skills than those needed for traditional ‘offline’ oversight measures. For ‘online’ cases, the investigative procedure conducted by an ombuds institution remains the same: ombuds institutions determine – by reviewing documents, undertaking interviews with the public authorities in question, and visiting their premises when necessary – whether public authorities have fulfilled their role legally and properly in the most efficient, effective, and ethical way.. While this is straightforward for some cases of online violence, for others – depending on the specificities of the case – the ombuds investigators may require specialized knowledge of, for instance, the functioning of social media channels or the applicable law when the owner and/or servers of the hosting company are located abroad. Furthermore, it should be underlined that ombuds institutions (usually) do not have jurisdiction over private entities, be they natural or legal persons.



Thus, in cases where a private citizen is threatened by another private citizen on a social media platform owned by a private company, an ombuds institution can only oversee the work of public authorities (such as the police) to assess whether they did everything in their power to investigate the case.

Ombuds institutions can establish working relationships with big private companies in this field – even if they cannot oversee their work. Ombuds institutions have the potential to serve as bridges between private enterprises and the state when it comes to human rights issues, such as protecting the personal data of users. Big companies (such as Google, Meta, or Apple) and smaller ones active at the national level that collect a massive amount of data about their users are known to be reluctant to share this data with the state, citing the need to protect the privacy of their users. However, in specific legal circumstances – that is, as part of criminal proceedings – they are obliged to share it. There are also companies that predominantly sell data collected online through various methods. Ombuds institutions could bring their expertise to the table to shed more light on human rights concerns in this area. This could benefit both the state and private enterprises. The former could better understand the importance of the right to privacy and personal data protection, including data kept by private entities. The latter could use ombuds’ expertise to fine-tune their policies and terms and conditions, with the ultimate goal of preventing, to the extent possible, online harassment and other forms of violence on their media channels. Ombuds

institutions could work with both sides to develop the most efficient procedures for prosecuting those who use social media to harass or threaten other users.

CSOs are another key actor for ombuds institutions. Ombuds institutions should join forces with CSOs to raise awareness, educate, or even develop joint legislative proposals if needed. In some parts of the region, cooperation with civil society is explicitly stipulated in the ombuds laws, as in Serbia, Kosovo, and North Macedonia.³¹ This engagement is beneficial for ombuds institutions because they can draw on the knowledge and experience of CSOs when conducting joint awareness-raising and education campaigns. It also enables them to learn about the most recent developments in the field from specialized CSOs, as well as to use their expertise and follow up on policy recommendations to the government.

CSOs submit cybersecurity-related policy recommendations to the ministry of telecommunications, interior, or defence – depending on which ministry is responsible for overseeing cybersecurity. When an ombuds institution is preparing to establish a cybersecurity oversight programme, the ministry in charge should ideally have a solid track record in ‘traditional’ oversight of the security sector so as to facilitate the process of establishing a cybersecurity oversight programme. They will thus have prior experience of working with ombuds institutions and general procedures already in place. A much-needed level of trust will also have been established. This leads into the third ‘A’: attitude or the level of commitment to overseeing the security sector.

5. Attitude: developing a culture of oversight

As indicated, ombuds institutions in the region do not have a strong culture of security sector oversight and their activities to protect human rights in cyberspace have been sporadic rather than part of a well-designed programme. There are several reasons for this situation.

In the early years of their work (see Figure 1), ombuds institutions understandably had to concentrate on positioning themselves in the state hierarchy and raising awareness of their role among citizens, whose rights they are supposed to protect and promote.

Given their broad mandate and the extent and nature of systemic human rights and governance problems faced by public administrations in the region, ombuds institutions needed to choose their priorities wisely. They therefore opted to pay particular attention to the most vulnerable groups, such as children, women, persons with disabilities, national minorities, and persons deprived of their liberty. Another reason for this focus is that most of the initial employees came

³¹ Serbia, Law on the Protector of Citizens, Official Gazette of the Republic of Serbia”, No. 105/2021, Art. 42; Kosovo, Law on Ombudsperson, No. 05/L-019, Art 16.1.9; and North Macedonia, Law on the People’s Advocate, Art. 2.

from human rights CSOs, with expertise in those issues. As vast structural problems have been identified in various public sectors – such as tax administration, cadastre, state pension funds, and social services – ombuds institutions have concentrated primarily on these urgent matters that have the potential to affect the lives of hundreds of thousands of people, leaving the security sector on the margins.

Due to the authoritarian past of the region, security institutions in the region, particularly intelligence and security services, were unused to being regulated and have traditionally been highly secretive, lacking external controls, and prone to human rights violations. Since the late 1990s and early 2000s, there have been many efforts to invest in reforming and democratizing the security apparatus of the Western Balkans, including by developing a comprehensive system of democratic civilian control of the security sector, comprising parliamentary, judicial, governmental, and independent expert control. Despite being given strong mandates to oversee the security sector, ombuds institutions had neither the experience nor the expertise to perform these tasks, while security institutions were reluctant to allow external bodies to ‘intrude’. It is largely this lack of experience and trust on both sides that has hindered the much-needed independent expert oversight. As new entities, ombuds institutions have had to build their credibility.

Credibility is particularly important for ombuds institutions because, as suggested by Neave³², their impact is not derived from binding, coercive, or determinative powers, but from the rigour, objectivity, and independence with which they conduct their activities. Ombuds institutions are seen through the lenses of their mandate-holders. Hence, ‘the role of individual leadership should not be overlooked, since many NHRIs – like any organization – thrive under the independent-mindedness or perseverance of particular commissioners or, alternatively, flounder in the face of passive leadership’³³. The success of ombuds institutions, therefore, ‘depends overwhelmingly on the strength of their mandate-holder(s) and their ability to position themselves as an objective, rigorous and credible authority’.³⁴

Building credibility in other areas of work should have helped ombuds institutions to establish a full-fledged oversight programme over the security sector, including cybersecurity, but this has not been the case. Ombuds institutions are often hesitant to involve themselves in sensitive security-related issues, particularly if there is the potential for confrontation with security institutions. Furthermore, ombuds institutions could make a far more active and strategic contribution to protecting human rights in cyberspace, particularly in the cases of cyberbullying and online violence against women.³⁵

³² Neave, C. 2014. ‘Exploring the Role of the Commonwealth Ombudsman in Relation to Parliament’. Senate Occasional Lecture Series at Parliament House, Canberra, 28 November, p. 31.

³³ Cardenas, S. 2012. ‘National Human Rights Institutions and State Compliance’, in R. Goodman and T. Pegram, eds., *Human Rights, State Compliance, and Social Change: Assessing National Human Rights Institutions*. Cambridge: Cambridge University Press, p. 49.

³⁴ Glušac, L. 2018. ‘National Human Rights Institutions and Oversight of the Security Services’, *Journal of Human Rights Practice*, Vol. 10, Iss. 1, pp. 65-66.

³⁵ Cyber violence can be defined as a cybersecurity threat characterized by ‘the use of computer systems to cause, facilitate, or threaten

The use of digital means for technology-facilitated abuse can range from online violence, (sexual) harassment, sexting, revenge-porn, image-based abuse, stalking, and tracking. The use of cyber violence thereby also acts as an enabling tool leading to the perpetration of a variety of further crimes, with serious human rights consequences, such as human trafficking and child sexual exploitation and abuse.³⁶ Furthermore, domestic violence is often linked to the use of cyber means to stalk, track, and harass female victims, since the victim of domestic violence can frequently be further intimidated, controlled, followed, harassed, and bullied into submission through technological means and by acts of online abuse.³⁷

Ombuds institutions from the region have all invested considerable efforts in fighting domestic violence, but have yet to devote more attention to cyberspace. Recent research indicates that online gender-based violence is increasing in the Balkans.³⁸ Some ombuds institutions from the region have conducted campaigns to raise awareness of the issue. For instance, the Montenegrin Protector of Human Rights and Freedoms has published comic strips about online violence against women and girls to educate the public and raise awareness.³⁹

The study conducted by the Balkan Investigative Reporting Network identifies four main reasons for increased online gender-based violence: 'inadequate legislation and an already poor institutional response to discrimination and hate speech; lack of response from big tech companies in implementing their own community policies related to digital violence; media enforcing gender stereotypes and failing to punish violations of professional ethical guidelines; and deep-rooted patriarchal norms on a societal level that legitimize and normalize violence and discrimination against women'.⁴⁰ Interestingly, the media is not only one of the indirect contributors to increased online violence, but also the target, since journalists are among the most frequently affected by this phenomenon.⁴¹

While he has been notably inactive in overseeing the security sector, Serbian Protector of Citizens Pašalić did initiate the creation of an online platform for protecting journalists against all forms of violence and offer his support to associations of journalists. The platform's impact, including its overall usefulness and success, has yet to be seen, as a similar platform – run by one of the associations of journalists – already exists and records all online and offline acts of violence against journalists. Pašalić has also publicly announced that he had proposed amend-

violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering, and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities' (Council of Europe. 2018. '[Cybercrime Convention Committee \(T-CY\) Mapping study on Cyberviolence](#)').

³⁶ DCAF. 2021. *Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach*. Geneva: DCAF, p. 9.

³⁷ Ibid.

³⁸ Karic, S. and M. Ristic. 2022. '[How Online Violence Against Women Goes Unpunished](#)', *Balkan Insight*. 11 May.

³⁹ Montenegrin Protector of Human Rights and Freedoms. n.d. [Zaštita od nasilja na internetu](#).

⁴⁰ Ibid.

⁴¹ Mastracci, M. 2021. '[Online Intimidation: Controlling the Narrative in the Balkans](#)', *Balkan Insight*, 16 December.

ments to the Law on Public Peace and Order,⁴² which would classify threats and insults on social networks as misdemeanors, and see legal proceedings in cases of spreading hate speech, threats, and verbal attacks on social networks conducted under an expedited procedure with the immediate execution of judgment. Irrespective of the ultimate success of this initiative, the Protector of Citizens (Ombudsman) of Serbia could certainly intensify its activities in overseeing efforts by the police to investigate cases of online violence.

Collaboration between ombuds institutions and equality bodies on online hate speech and other anti-discriminatory acts could also be strengthened in countries of the region where the protection of equality is designated to a separate body, as in Albania, North Macedonia, and Serbia.⁴³

Ombuds institutions could also cooperate with personal data protection and information commissioners. The collaboration between the Serbian Protector of Citizens and the Commissioner for Information of Public Importance and Personal Data Protection on the surveillance of citizens' communications from 2012 is a good example of how this can be achieved. At the time, there were four telecommunications companies in Serbia, three of which also provided mobile telephone services. 'According to the Commissioner, of those four, only one company had used database (listing) access control software (allowing them to count the number of external visits to telecommunications databases, that is, by police and security services)' ⁴⁴— although they all have a duty to keep that information for one year and to register any such access.⁴⁵ 'In his oversight visit, the Commissioner found that over the course of one year, one telecommunications company alone had registered more than 4,000 accesses on request and more than 270,000 direct (online) accesses to the company's listings database. Of those 4,000 requests to access listings, more than half did not quote any legal grounds or court orders.'⁴⁶ For these reasons, the Protector of Citizens and the Commissioner have suggested integrating 'the existing parallel technical capacities of various agencies and the police into a single national agency, which would act as a provider of technical services necessary for the interception of communications and other signals to all authorized users.'⁴⁷ Despite this, no such agency has been created to date.

Evidence from Albania also suggests that enhancing inter-institutional cooperation is one of the most effective ways to improve synergies effects and increase the individual capacities of each

42 RTS. 2022. [Pašalić: Utvrditi pojedinačnu odgovornost za širenje govora mržnje na internetu](#). 6 May. Interestingly, these amendments are not available on the Protector of Citizens' website, where all other legal initiatives are listed.

43 In Bosnia and Herzegovina, Kosovo, and Montenegro, ombuds institutions subsume the function of national equality bodies.

44 Glušac, L. 2018. 'National Human Rights Institutions and Oversight of the Security Services', *Journal of Human Rights Practice*, Vol. 10, Iss. 1, pp. 58-82. See also Commissioner. 2012. [Press Conference of the Commissioner for Information of Public Importance and Personal Data Protection and Ombudsman with regard to 14 Measures](#) (in Serbian).

45 Commissioner. 2012. [Press Conference of the Commissioner for Information of Public Importance and Personal Data Protection and Ombudsman with regard to 14 Measures](#) (in Serbian).

46 Ibid.

47 Glušac, L. 2018. 'National Human Rights Institutions and Oversight of the Security Services', *Journal of Human Rights Practice*, Vol. 10, Iss. 1, p. 73.

institution. Alban Dafa argues that strengthening cooperation between the Supreme State Audit Institution, the Ombuds Institution, and the Information and Data Protection Commissioner would improve the effectiveness of their actions and overall impact as independent oversight institutions vis-à-vis the security sector, particularly regarding the right to information, the protection of personal data, and increasing transparency and procedural fairness.⁴⁸

In sum, there is an intrinsic interdependence between ability and attitude in this context. When it comes to exercising strong oversight over the security sector, Western Balkan ombuds institutions lack the necessary commitment (that is, attitude) to develop a culture of oversight and are therefore not motivated to develop or acquire the required technical expertise (that is, ability). As mentioned above, they already possess sufficient understanding and knowledge of some cyber-related issues; however, they have yet to build interest and capacity in other areas – particularly those requiring highly technical knowledge, such as the effect of artificial intelligence on human rights.⁴⁹

6. Gaps and opportunities

Carver correctly observed that ‘the security sector provides a particularly striking example of the difficulties of enforcing accountability’.⁵⁰ This applies even more to cybersecurity and other aspects of the security sector that require specific technical expertise. Oversight and accountability mechanisms in these areas always lag behind those of security institutions, as the latter are constantly evolving and acquiring new equipment, developing new methods of work, and so on.

This study has shown that, in the context of cybersecurity and human rights in cyberspace, ombuds institutions in the Western Balkans already have a solid legal framework. What they lack, however, is a commitment to devoting more time and resources to overseeing the security sector.

Since their establishment, ombuds institutions in the region have often struggled with limited budgets and insufficient staff. It is difficult to determine whether and how strongly this has affected their commitment to focus more on security sector oversight. Arguably, not so much, because these activities do not require excessive funds, compared to other lines of work. Furthermore, the donor community has traditionally invested significantly in supporting both democratic oversight of the security sector and ombuds institutions. Whenever ombuds institutions demonstrated an interest in making improvements, as in the cases of Serbian or Montenegrin institutions in the past, support was provided. Commitment and political will seem to be bigger factors.

⁴⁸ Dafa, Alban. 2021. *(Un) Democratic Control of the Albanian Armed Forces Centralisation of Defence Policy and Ineffective Oversight*. Tirana: Institute for Democracy and Mediation, p. 41.

⁴⁹ See FRA (EU Fundamental Rights Agency). 2020. *Getting the Future Right: Artificial Intelligence and Fundamental Rights*. Vienna: FRA.

⁵⁰ Carver, R. 2012. ‘National Human Rights Institutions in Central and Eastern Europe’, in R. Goodman and T. Pegram, eds., *Human Rights, State Compliance, and Social Change: Assessing National Human Rights Institutions*. Cambridge: Cambridge University Press, p. 201.

Once there is a strong will for change, it will be easier to identify and develop capacities, in the form of technical staff, equipment, internal procedures, and so on. As far as the triple 'A' framework is concerned, ombuds institutions have 'authority', but are largely lacking in 'ability' and 'attitude'. Their involvement in cybersecurity could therefore be described as unrealized potential, because their activities are sporadic activities, and they lack a comprehensive programme of work.

This should not be a surprise, since the region still suffers from complex human rights challenges – some inherited from former Yugoslavia, and others caused by economic and political transitions or resulting from rising autocratization. Operating in such a context, ombuds institutions are in a difficult position and must pick their battles strategically, given their limited resources and particular institutional position.

While ombuds institutions may gain knowledge from each other, they are also affected by the experiences of their peers in attempting to influence the very heart of the security sector, as Janković did during his mandate; he encountered a full-fledged public campaign, led by the ruling majority, security services, and government-controlled media.⁵¹ Such a development has hardly motivated other regional ombuds institutions to focus on overseeing the security or intelligence services. Nevertheless, given the complex and dispersed nature of the security sector, there is still significant room for improvement.

The area of human rights in cyberspace has great potential for encouraging a more active role for ombuds institutions. All ombuds institutions in the region have well-developed programmes for the protection and promotion of human rights of the most vulnerable groups. Given the current state of play, in the short term, ombuds institutions could continue to concentrate on protecting the human rights of these groups, such as women and girls, by integrating an online dimension into their work. As part of these efforts, they could focus more on overseeing the police by ensuring that reported cases of online violence are fully investigated. This could help build confidence and trust, among both citizens and the police. In the medium term, ombuds institutions could turn to more advanced topics, which require expert knowledge in terms of technology or processes.

Developing partnerships is crucial as a means to increase knowledge and expand institutional reach. Ombuds institutions should establish strategic cooperation with the parliament so as to better coordinate the resources at the disposal of each oversight institution. They should provide advice to the parliament and government on policy and legislation regarding online civic space that complies with international human rights standards and laws. Ombuds institutions play a central role in holding the government accountable to its human rights obligations, both offline and online.

⁵¹ See Glušac, L. 2018. 'National Human Rights Institutions and Oversight of the Security Services', *Journal of Human Rights Practice*, Vol. 10, Iss. 1.

Joining forces with other independent oversight bodies, such as equality bodies, personal data protection, and public information commissioners is also a particularly rewarding strategy, due to the synergies it offers. This study has identified some examples of good practices, which could be revived or replicated.

Currently, in the Western Balkans, civil society and the private sector have more expertise in overseeing cybersecurity than ombuds institutions. Developing stronger ties and cooperation agreements with these actors is therefore highly advisable. The media and CSOs media should be key partners of ombuds institutions.

CSOs in the region have grown more vocal on cyber-related issues, particularly with the recent purchase of new surveillance systems. Governments have seen the expansion of registration and identification systems as a useful tool for border and movement controls and counterterrorism but also for the suppression of opposition and activists in increasingly authoritarian regimes. Hence, CSOs have assessed the potential for abuse of identification systems and advocated for robust data protection legislation and privacy safeguards. Ombuds institutions should contribute more actively to these discussions.

The media is particularly crucial for the ultimate success of ombuds' efforts. It serves as not only a megaphone for the findings of ombuds institutions but also a means to apply pressure. Public officials often only react to ombuds' requests and recommendations as a result of pressure following media reports. Cooperation with media outlets (traditional and electronic) is essential to enable ombuds institutions to conduct large-scale advocacy, awareness-raising, and educational campaigns. In return, ombuds institutions should pay particular attention to protecting the rights of media workers (such as journalists and editors) and other human rights defenders, as they are often subject to online threats and verbal attacks.

Seeking accountability for cyber-attacks: challenges of attribution and subsequent responses

by Rebecca Mikova

Table of contents

1.	Introduction.....	46
2.	Challenges to the attribution of cyber-attacks.....	48
2.1	International norms governing attribution of cyber-attacks.....	48
2.2	Approaches and challenges to cyber-attack attribution.....	51
2.3	Attribution of cyber-attacks.....	54
2.4	Public attribution of cyber-attacks by states.....	55
2.5	Case study on Ukraine.....	58
3.	Responses to cyber-attacks.....	61
3.1	Has the cyber-attack been attributed to a state?.....	61
3.2	Was the attribution public?	62
3.3	What is the scale and nature of the cyber-attack?	62
3.4	Diplomatic protests.....	65
3.5	Retorsion.....	66
3.6	Legal measures.....	67
4.	Role of parliaments in cyber-attack attribution and subsequent responses.....	68
5.	Recommendations.....	69

Introduction

Cyberspace constitutes a new frontier, which – although crucial for the functioning of modern societies – remains largely unregulated under international law. Following the emergence of cyberspace, the international community accepted that the traditional norms and principles of international law would continue to apply to this domain.¹ While in general this provided clarity on the application of international law in cyberspace, it did not address the specificities of cyberspace that complicate this. One of these key areas is the norms and standards for the attribution of cyber-attacks. Under international law, attribution is an important prerequisite for establishing state responsibility for an internationally wrongful act.² An act or omission can be attributed to a state if it is committed either by a state organ³ or by persons or entities exercising elements of governmental authority.⁴ The ability or inability to attribute a cyber-attack therefore has various political and legal implications, such as whether a given state is entitled to conduct counter-measures and, if so, the standards they must conform to.

Understanding how the attribution of cyber-attacks can be determined and its limitations, as well as how this affects the state's response, is crucial for policymakers for the following reasons:

- ◇ **Increasing prevalence of cyber-attacks:** As more and more aspects of our daily lives and critical infrastructure become digitized, the risks posed by cyber-attacks and their potential consequences are also increasing. It is important for policymakers to understand how to adequately respond to such attacks to ensure national security and public safety.
- ◇ **Challenges of attribution:** The attribution of cyber-attacks can be a complex process and involve many technical, legal, and political considerations. Policymakers must therefore understand its limitations—including technical factors, such as the use of proxy servers or false flag operation—to prevent misattribution and adverse consequences.
- ◇ **Importance of international law:** The attribution of cyber-attacks is governed by international law, which is both complex and multifaceted. It is important for policymakers to understand the legal framework surrounding cyber-attacks, including the principles of sovereignty, non-intervention, and the prohibition on the use of force.
- ◇ **Deterrence:** Attribution is essential for effective deterrence of cyber-attacks. If attackers believe that they can launch attacks without being identified or facing any consequences, they may be emboldened to carry out more attacks in the future.

¹ See, for example, EU (European Union). 2013. [Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace](#), para. 2.5.

² ILC (International Law Commission). 2001. Responsibility of States for Internationally Wrongful Acts, art. 2(a).

³ Ibid., art. 4(1).

⁴ Ibid., art. 5.

- ◇ **Retaliation:** Permissible responses to cyber-attacks can include a range of measures, from diplomatic protests to military retaliation. It is important for policymakers to understand the appropriate responses to various types of cyber-attacks, as well as their legal limits.
- ◇ **Collaboration:** The attribution of cyber-attacks often requires collaboration between different countries and agencies. Policymakers should therefore understand how to work with other countries to share information and coordinate responses to cyber-attacks, especially as many cyber-attacks originate from foreign countries.
- ◇ **Protection of civil liberties:** Policymakers should know how to balance the need to respond to cyber-attacks with the protection of civil liberties, such as privacy and freedom of expression. Responses to cyber-attacks that involve the collection of personal data or censorship could have unintended consequences on civil liberties, and policymakers should be aware of these potential risks.

Since the international legal norms that apply to cyberspace were developed before its emergence, applying these norms in practice poses a number of challenges. The key reason for this is that while traditional international law is based on the principle of territoriality, cyberspace operates in a 'deterritorialized' manner. For example, information travelling in cyberspace can cross numerous jurisdictions within a fraction of a second and exist simultaneously, wholly, or partially in different jurisdictions. Cyberspace also allows its users to remain anonymous – which makes it very difficult, if not impossible, to determine their geolocation – through the use of virtual private networks (VPNs), specialized browsers (for example, the Tor Browser and the Invisible Internet Project), or other tools (such as anonymous remailers and anonymizers). While this does not preclude states from continuing to apply sovereignty and jurisdictional principles based on territoriality, the incongruity between this domain and traditional regulatory approaches has made establishing accountability for cyber-attacks difficult.

This chapter will begin by exploring the norms and existing challenges to the attribution of cyber-attacks and go on to analyse the limitations and scope of possible responses for states. Cyber-attacks, cyber operations, and intrusion events are referred to interchangeably. The analysis is based on applicable international norms as well as state practice in this regard. Theoretical analysis is complemented by various examples, with a specific focus on the attribution of cyber-attacks related to the war in Ukraine.

2. Challenges to the attribution of cyber-attacks

This section provides an overview of the key challenges concerning cyber-attack attribution, as well as the relevant international norms. While traditional international law continues to apply in cyberspace, a number of gaps remain that the international community has yet to address. The key challenges to attributing and responding to cyber-attacks are the following:

Legal and policy challenges:

- Lack of international evidentiary standards for the attribution of cyber-attacks
- Lack of coherent methodological approaches to, as well as terminology on, the attribution of cyber-attacks, which in turn undermines verification efforts and makes cross comparisons difficult
- Lack of international norms in cases of the misattribution of cyber-attacks
- Strict international norms concerning the attribution of cyber-attacks conducted by non-state actors to states

Security risks:

- High risks associated with the public disclosure of evidence or the methodology on which the attribution is based, which in turn either disincentivize states from publicly declaring the attribution of cyber-attacks or lead to unsubstantiated attribution claims that can be disputed

Political challenges:

- Absence of an internationally accepted and recognized entity to investigate cyber-attacks and make authoritative attribution claims
- Political factors that influence a state's decision to attribute a cyber-attack and result in attributions that have no legal basis, particularly during conflict
- Political instrumentalization of attribution claims in the absence of evidentiary standards and verification processes, which, without an appropriate response, undermine deterrence

2.1 International norms governing attribution of cyber-attacks

International law provides that cyber operations conducted by state organs, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to that state.⁵ This includes intelligence, military, internal security, customs, or other state

⁵ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, rule 15.

agencies, regardless of their function or place in governmental hierarchy.⁶ The International Court of Justice stated that ‘persons, groups of persons or entities may, for purposes of international responsibility, be equated with State organs even if that status does not follow from internal law, provided that in fact the persons, groups or entities act “in complete dependence” on the State, of which they are ultimately merely the instrument’.⁷ In cases where individuals, groups, or entities act beyond the authority granted to them or in contravention to instructions, the key criterion is whether they acted in an apparently official capacity. This excludes instances where individuals have exploited governmental cyber infrastructure for private gains.⁸ The same standard is applied to entities exercising elements of governmental authority. The mere fact that a cyber operation was launched or otherwise originated from governmental infrastructure, or made using private cyber infrastructure in a state’s territory, is usually insufficient evidence for attributing an operation to that state or indicating its involvement.⁹

Furthermore, cyber operations conducted by a non-state actor are attributable to a state either when ‘such operations are engaged in pursuant to the State’s instructions or under the State’s direction or control, or when the State acknowledges and adopts the operations as its own’.¹⁰ This covers individual hacker; informal groups (for example, Anonymous); criminal organizations engaged in cybercrime; legal entities such as commercial IT service and software and hardware companies; and cyber terrorists or insurgents.¹¹ The attribution of a cyber-attack by a non-state actor is considered on a case-by-case basis depending on the factual relationship between them and the state.¹² It should be noted that the non-state actor does not have to be legally empowered to exercise elements of governmental authority, but rather functions as that state’s auxiliary.¹³ This includes instances where, in response to an unanticipated massive cyber-attack, a state instigates private individuals and groups to act as volunteers to help respond to the crisis.¹⁴ The IT Army of Ukraine illustrates the challenges of implementing this in practice. Created out of necessity following Russia’s invasion of Ukraine, the army has evolved into a hybrid contrast that is neither civilian nor military, neither public nor private, neither local nor international, and neither lawful nor unlawful.¹⁵ The International Group of Experts who developed the Tallinn Manual 2.0 considered the appropriate standard for the attribution of conduct of a non-state actor to be the

⁶ Ibid., para. 2

⁷ ICJ (International Court of Justice). *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. Merits. Judgement of 26 February. ICJ Reports 2007, para. 392. See also ICJ. 1986. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Merits. Judgement of 27 June. ICJ Judgment of 27 June. ICJ Reports 1986, paras. 109-110.

⁸ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, rule 15, paras. 6-7.

⁹ Ibid., rule 15, paras. 13-14

¹⁰ This rule, provided in the Tallinn Manual 2.0, is derived from Article 8 of Articles on State Responsibility.

¹¹ Ibid., rule 17, para. 2

¹² Ibid., rule 17, para. 3

¹³ Ibid., rule 17, para. 4

¹⁴ Ibid.

¹⁵ Soesanto, Stefan. 2022. ‘[The IT Army of Ukraine: Structure, Tasking and Ecosystem](#)’. Center for Security Studies.

presence of effective control, developed by the International Court of Justice (ICJ) in the Nicaragua and Genocide judgements.¹⁶ A state is in effective control of a cyber operation by a non-state actor if it determines the execution and course of the operation, and if the cyber activity conducted by the non-state actor is an integral part of that operation.¹⁷ 'Effective control includes both the ability to cause constituent activities of the operation to occur, as well as the ability to order the cessation of those that are underway.'¹⁸ A state's general support or encouragement of a non-state actor's cyber-attack is insufficient to establish attribution. For example, if a state provides malware to a non-state actor, the cyber-attack cannot be attributed to that state in the absence of effective control over specific operations.¹⁹ In cases where a non-state actor operating under the effective control of a state engages in ultra vires acts, the standard to consider is whether the act was incidental to the mission – that is, whether it is an integral, essential part of the operation over which the state exercises effective control.²⁰

International law does not, however, provide a standard for cyber-attack attribution. Instead, states have developed various national positions on this matter,²¹ as a result of which there is no international norm or consensus on what constitutes sufficient evidence for the attribution of cyber-attacks.²² There are therefore only a limited number of instances where states have publicly attributed a cyber-attack to a state.²³ Based on empirical data, it appears that technically capable states tend to use public attribution more frequently against states that they consider adversaries.²⁴ For example, the pace of US government public attributions of cyber-attacks has generally increased over time.²⁵ In recent years, some states have attempted to overcome this obstacle by coordinating their attribution of cyber-attacks. Towards the end of 2017, six countries – Australia, Canada, Japan, New Zealand, the United Kingdom, and the United States – had issued coordinated statements attributing the WannaCry cyber-attack to North Korea.²⁶ In principle, the impact of this type of coordinated attribution is limited – beyond serving as a tool for political persuasion. In the long run, however, such efforts, especially if they include a coordinated assessment of

¹⁶ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, rule 17, paras. 5-6; ICJ. 1986. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Merits. Judgment of 27 June. ICJ Reports 1986, p. 14, para. 115; see also ICJ. 2007. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment of 26 February. ICJ Reports 2007, p. 43.

¹⁷ ILC. 2001. Responsibility of States for Internationally Wrongful Acts, art. 8, para. 3 of commentary.

¹⁸ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, rule 17, para. 6

¹⁹ Ibid., rule 17, para. 8

²⁰ Ibid., rule 17, para. 13

²¹ For further information on national positions on cyber-attack attribution, see CCDCOE (Cooperative Cyber Defence Centre of Excellence). 'Attribution'. n.d. Database. Accessed 16 August 2022.

²² Banks, William. 2021. 'Cyber Attribution and State Responsibility', *International Law Studies*, Vol. 96.

²³ For example, the United States Justice Department indicted five People's Liberation Army Officers in 2014 on economic espionage charges; in 2017 British Minister of Security, Ben Wallace claimed during a BBC interview that North Korea was responsible for the WannaCry cyber-attack.

²⁴ Yang, Fan. 2022. 'The Problem with Ill-Substantiated Public Cyber Attribution: A Legal Perspective', in Ariel E. Levite, Lu Chuanying, George Perkovich and Fan Yang, eds., *Managing U.S.-China Tensions Over Public Cyber Attribution* Carnegie Endowment for International Peace and Shanghai Institutes for International Studies, p. 6.

²⁵ Bateman, Jon. 2022. 'The Purposes of U.S. Government Public Attribution', in Ariel E. Levite, Lu Chuanying, George Perkovich and Fan Yang, eds., *Managing U.S.-China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace and Shanghai Institutes for International Studies.

²⁶ Banks, William. 2021. 'Cyber Attribution and State Responsibility'. *International Law Studies*. Vol. 96, p. 1044

evidence based on specific standards, could serve as evidence of state practice in this area and lead to the development of applicable customary international law.

2.2 Approaches and challenges to cyber-attack attribution

There is no single criterion for determining the origins of a cyber-attack. Instead, each cyber-attack needs to be assessed holistically, including the specific context and evidence available, to establish a high level of confidence. For this purpose, three types of indicators can be distinguished:

- **Technical indicators:** Technical indicators include computing and network components, such as Internet Protocol (IP) addresses, log file analysis, reviews of software executables, and language settings or knowledge of required resources. ‘A regular pattern of a non-state group taking control of governmental cyber infrastructure to launch cyber operations can be a counter-indication that a State launched a particular operation.’²⁷ In many cases, technical indicators may not be sufficient or may mislead the investigator due to the decentralized, dynamic and open nature of the internet, which enables the offender to easily hide their tracks by disconnecting devices, changing IP addresses, or leveraging tactics, techniques, and procedures (TTP) developed by other malicious actors. For example, in a 2013 cyber-attack on Ukrainian government websites, the attacker impersonated the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). They then directed their operations against the NATO CCDCOE website, the Estonian Defence Forces, and the militaries of other NATO states – making it look as though they came from the Ukrainian government.²⁸ As a result, identifying the specific machines and methods involved in an attack does not guarantee that those responsible will be found.²⁹
- **Intelligence indicators:** Intelligence or clandestine indicators comprise classified information produced by intelligence agencies, including political insights. In many cases, human intelligence is required to corroborate technical findings – for example, to pin down the human actors who actually conducted the cyber-attack.³⁰ ‘[R]eliable human intelligence that indicates governmental computers will be or have been employed by non-State actors to conduct operations could augur against a conclusion of State involvement.’³¹

²⁷ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, rule 15, para. 17.

²⁸ Ibid., rule 15, para. 15.

²⁹ Davis, John S. et al. 2017. *Stateless Attribution: Toward International Accountability in Cyberspace*. Rand Corporation.

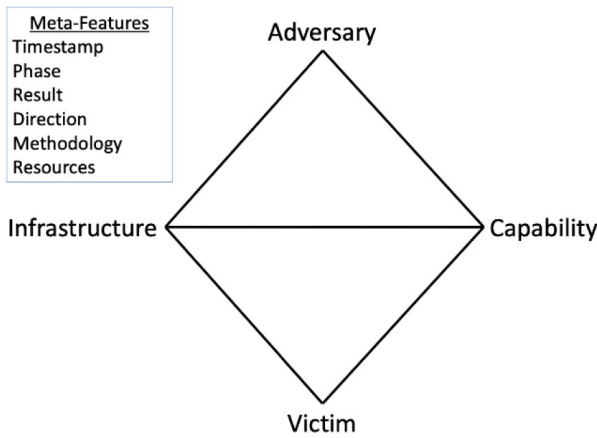
³⁰ Yang, Fan. 2022. ‘The Problem with Ill-Substantiated Public Cyber Attribution: A Legal Perspective’, in Ariel E. Levite, Lu Chuanying, George Perkovich and Fan Yang, eds., *Managing U.S.-China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace and Shanghai Institutes for International Studies, p. 6.

³¹ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, rule 15, para. 17.

- **Political Indicators:** Political indicators include diplomatic knowledge about the motivation of governments and political operatives. For example, the existence of friendly relations between the injured state and the purportedly responsible state would go against the conclusion that the state is the perpetrator.³²

A number of models and frameworks have been developed to standardize approaches to cyber-attack attribution. These models employ different terminology and conceptualize cyber-attacks and cyber intrusion events in different manners. The table below outlines three main attribution models and frameworks.³³

Table 1: Models of cyber-attack attribution

Diamond Model of Intrusion Analysis	
<p>The Diamond Model of Intrusion Analysis was developed by the US Department of Defense in 2013 and considers four components: the adversary, capabilities, infrastructure, and victims. This model is based on the axiom that ‘for every intrusion event, there exists an adversary taking a step toward an intended goal by using a capability over infrastructure against a victim to produce a result’.³⁴ An intrusion event is therefore defined as ‘how the attacker demonstrates and uses certain capabilities and techniques over infrastructure against a target’.³⁵ In practice, this model allows investigators to create profiles of adversaries that outline their cyber capabilities, the cyber infrastructure they use, and the victims targeted. Following a cyber-attack, this information can be used to determine the likely entity responsible for a given cyber operation.</p>	

³² Ibid., rule 15, para. 17.

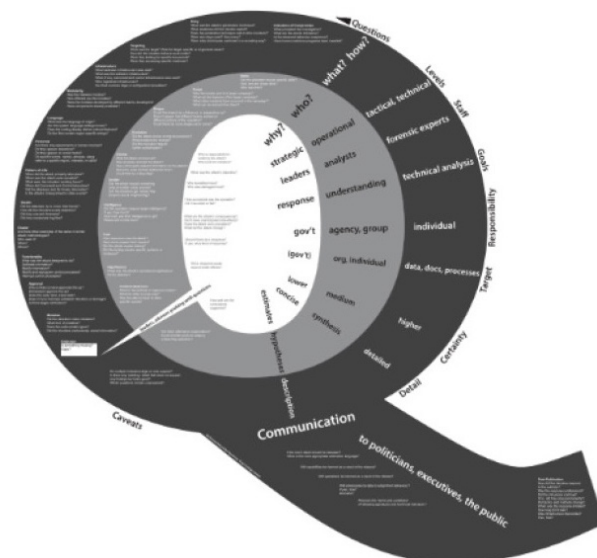
³³ It should be noted that the table does not include models that have a primary objective other than attribution (for example, Cyber Kill Chain, developed in 2013 by Lockheed Martin, and MITRE ATT&CK Navigator are aimed at defending against cyber-attacks rather than their attribution).

³⁴ Carreon, Cris. 2019. ‘Applying Threat Intelligence to the Diamon Model of Intrusion Analysis’. Recorded Future

³⁵ Ibid.

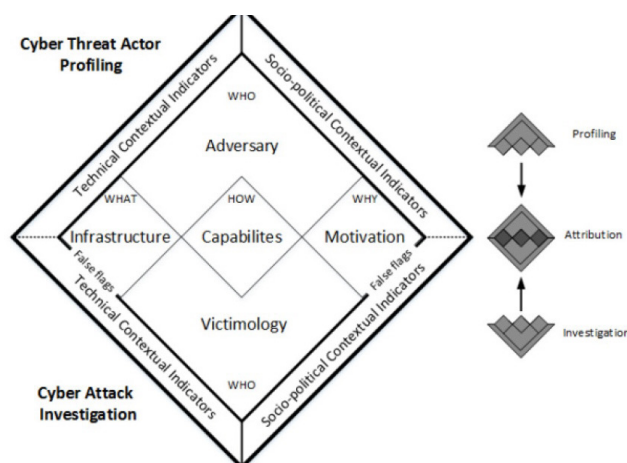
Q-Model

The Q-Model, developed by Rid and Buchana in 2015, is one of the best-known attribution frameworks.³⁶ The model helps analysts to consider the full range of relevant questions and to put the investigation into context. It integrates both technical and non-technical information to enable an analysis of competing hypotheses. The model includes over a hundred indicators divided into more than 30 categories such as functionality and skills. It introduces multiple levels (strategic, operational, tactical, technical, and communication) and roles (from forensic investigators through to national security officers and political leaders).



Cyber Attribution Model

The Cyber Attribution Model (CAM) was developed in 2019 by Pahi and Skopik.³⁷ This model intends to address false flag operations, which frequently result in misattribution, by addressing the interdisciplinary challenges of cyber attribution and the lack of concepts designed to address possible false flag operations on the technical and socio-political side. The model is initially separated into two components – cyber-attacks analysis and threat actor profiling – which are later brought together in the attribution phase.



As the existence of these various models shows, the practice of attribution has been diffuse and discordant –lacking a standard methodology for investigations to assess evidence and a universal measure of confidence to draw conclusions.³⁸

³⁶ Rid, Thomas and Ben Buchana. 2015. 'Attributing Cyber Attacks', *Journal of Strategic Studies*, Vol 38, Iss. 1-2, pp. 4-37.

³⁷ Pahi, Timea and Florian Skopik. 2019. 'Cyber Attribution 2.0: Capture the False Flag'. European Conference on Cyber Warfare and Security (ECCWS) 2019 18th European Conference on Cyber Warfare and Security.

³⁸ Davis, John S. et al. 2017. *Stateless Attribution: Toward International Accountability in Cyberspace*. Rand Corporation.

Another key element that determines the implications of an attribution is the type of entity that conducts the attribution. These can be divided into state actors and non-state actors, the latter of which include both private sector and non-governmental organizations. A growing number of private cybersecurity firms – such as CrownStrike, FireEye, KasperskyLab, Novetta, Symantec, and Trend Micro – also form part of this private sector and carry out cyber attribution investigations.³⁹ If a state organ – or a non-state entity exercising elements of governmental authority to conduct cyber-attack investigations – reaches a conclusion as to who is responsible for a cyber-attack, it may be assumed that the state exercised due diligence in reaching the finding; this can trigger domestic legal mechanisms, such as criminal investigations or various types of international responses. If the entity responsible for the attribution is a non-state actor, this does not prima facie imply the need for a state response. Depending on the company's size and influence, however, its attribution may be viewed as credible and carry significant weight. Due to the difficulty in comparing findings involving different attribution methodologies and actors, if a non-state actor uses its own methodology the findings may be rendered useless by state organs that wish to use them as a basis for their investigations. This also explains why efforts to harmonize cyber-attack attribution methodologies across different actors should be encouraged. While there has been some discussion over the creation of an international entity for cyber attribution (for example, Global Cyber Attribution Consortium proposed by Rand Corporation), no such body has been created to this day. The creation of such a body would imply that its findings automatically obtain international recognition and possibly trigger an international legal or political response.

2.3 Attribution of cyber-attacks

When an actor – whether state or non-state – attributes a cyber-attack, they must decide whether to disclose their findings. In doing so, they have to consider a number of factors, namely the risks of disclosing their findings and whether they affect their wider objective. When reporting on cyber-attack attribution, actors risk revealing the technical vulnerabilities of a particular system, sources of information, and methods of attribution – as well as sensitive sources and methodologies if the investigation includes classified information.⁴⁰ Because of this, the evidence and grounds for attribution of a cyber-attack are rarely disclosed publicly. The reputation of and level of trust in the state or non-state actor is therefore important since their attribution often has to be taken at face value without supporting evidence.⁴¹

Attributing a cyber-attack also implies acknowledging that the cyber-attack took place. Both public and private actors may be hesitant to do so to avoid:

- ◇ admitting vulnerability and losing the trust of citizens, customers, or their digital services clients;

³⁹ Ibid.

⁴⁰ Karlzén, Henrik. 2020. 'Usefulness of Cyber Attribution Indicators'. ECCWS 2020 20th European Conference on Cyber Warfare and Security. 168–176.

⁴¹ Davis, John S. et al. 2017. *Stateless Attribution: Toward International Accountability in Cyberspace*. Rand Corporation

- ◇ being held responsible for damage caused by the cyber-attacks (such as loss, damage, or theft of data stored in their systems); and
- ◇ revealing secret information about their systems and its vulnerabilities.

As a result, the number of cyber-attacks that take place is generally much higher than the number of attacks revealed to the public, and it is difficult to obtain accurate figures. The following section will examine in more detail the factors that states and national policymakers should consider when deciding whether to publicly attribute a cyber-attack.

2.4 Public attribution of cyber-attacks by states

In cases where the cyber-attack investigation results in the successful identification of a given offender, this does not imply that the state will publicly attribute the attack. As there is no international requirement for cyber-attack attribution, the decision to publicly attribute an attack is ultimately political. When making such a decision, policymakers can take into account a complex matrix of political objectives, including the following: to show accountability to a domestic constituency; to name and shame the accused; to ensure effective deterrence; to observe the possible reaction of the accused state; to hold a state legally responsible and justify possible measures in response; or to support efforts to establish limits and norms.⁴²

Two questions shape a state's decision to publicly attribute a cyber-attack: 1) what is the goal of public attribution? and 2) do the factors surrounding the attack and its attribution enable or constrain the state to publicly attribute? The following table outlines the goals and factors for consideration developed by Egloff and Smeets in 2021, which aim to guide states' decisions to publicly attribute a cyberattack.

Table 2: Framework for the public attribution of cyber-attacks⁴³

Goals
<p>By publicly attributing a cyber-attack, states pursue the following main objectives:</p> <ul style="list-style-type: none"> ● Norm-setting clarifies and enforces appropriate standards of behaviour for states and other actors in cyberspace. By publicly attributing cyber-attacks, states demarcate what they consider unacceptable behaviour in cyberspace, which demonstrates state practice and may lead to the development of customary international law.

⁴² Yang, Fan. 2022. 'The Problem with Ill-Substantiated Public Cyber Attribution: A Legal Perspective', in Ariel E. Levite, Lu Chuanying, George Perkovich and Fan Yang, eds., *Managing U.S.-China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace and Shanghai Institutes for International Studies, pp. 6-7

⁴³ See Egloff, Florian J. and Smeets, Max. 2021. 'Publicly attributing cyber attacks: a framework'. *Journal of Strategic Studies*

- **Coercion** is used to deter adversaries. Public attribution leads adversaries to alter their behaviour by compelling them to either refrain from certain acts, due to the threat of possible repercussions, or to behave or cease to behave in a certain way. The very act of public coercion can change the cost-benefit calculus of the adversary through, for example, delegitimization and shame.
- **Counter-threats** cause friction for adversaries (for example by forcing them to spend time and resources on capability-development and potentially follow gruelling counter-intelligence leads). Cyber-attack attribution and the disclosure of technical information about attacks can force adversaries to amend their strategy, tools, and infrastructure.
- **Prevention and defence** efforts are enhanced by spreading information about potential threats. Network administrators lack the necessary time and resources to address their vulnerabilities. Attributing a cyber-attack to, for example, a nation-state actor generally compels them to respond faster, which in turn enhances the state's cybersecurity.
- **Community building** allows states to share information and act together to address public perceptions of threats. It may also serve as a starting point for developing other types of response, beyond attribution.
- **Legitimacy and reputation building** enhances the domestic and international legitimacy or credibility of actors involved in the attribution process. While attribution capabilities generally cannot be observed by outside actors, a high-profile attribution case can serve to legitimize and strengthen the reputation of the attributing actor, which may in turn carry both financial and political implications (such as increased funding for state or non-state actors).

Factors

The following factors shape a state's decision to publicly attribute a cyber-attack:

Intelligence

- **Degree of attribution certainty:** The state should consider not only the individual who carried out the intrusion but also who is actually responsible for the cyber-attack. When a government has limited evidence to allow them to link an operation or campaign to a state, there is less incentive for public attribution.
- **Potential intelligence gains and losses:** Public attribution may provide insights into the sources and methods used by the government and obstruct efforts to collect intelligence.
- **TTPs used by the intruder:** Selectively revealing TTPs may strengthen the government's cybersecurity by forcing the adversary to abandon the least visible TTPs.
- **Ability to control relevant attribution information:** If states are aware that other actors may conduct cyber-attack investigations and publicize their findings, this may influence how and when they decide to publicly attribute the attack. If a government has little confidence in their ability to control the flow of information about the intrusion, a more proactive public information strategy is needed.

Incident severity

- **Legitimacy and motivation of the responsible actor:** Some adversaries cannot be shamed by public attribution and doing so may instead serve to draw attention to them and their activities (for example, non-state armed actors). In such cases, public attribution may be counterproductive to the state's objectives. A public attribution can only damage an actor's reputation if it contradicts their identity and is likely to be perceived as negative.
- **Impact of the operation:** The scale of a cyber-attack affects the government's decision to publicly attribute the attack. Incidents with limited impact have little geopolitical relevance, and states may prefer not to attribute them. They may also take into account whether the cyber-attack is considered unlawful under international law. Permissible conduct (that is, peacetime cyber espionage) would not trigger any consequences under international law.

Geopolitical situation

- **Context (relationship between the attributing government and the intruder):** Peacetime cyber espionage is common even among allied states. Governments are less likely to attribute cyber incidents conducted by their allies. In case of attribution to states other than close allies, other considerations may come into play, such as the impact on domestic politics, the potential for strategic partnerships, and so on.
- **Timing (operational and political considerations):** Operationally, it is strategically astute to publicize an attribution only once the state has derived the maximum intelligence value out of observing the adversary. Politically, policymakers should consider whether there are any time-sensitive political agendas that attribution can support or be detrimental to.

Process and follow-on actions

- **Potential for follow-on policy or military responses:** A public attribution is a prerequisite for certain responses – both legally and politically (for example, the ability to condemn the state at the international level). Policymakers may also consider whether creating an environment where public attribution becomes a regularity is desirable in light of their own activities.
- **Type of actor and audience:** Public attribution should consider not only the responsible state but also the wider audience, since it may have both negative and positive consequences for international stability.
- **International cooperation:** Coordinated multi-state public attributions can facilitate norm-setting as well as coercion, especially for smaller and middle powers. International coordination can also, however, delay the process of public attribution.

Once a state decides to publicly attribute an attack, they also need to determine how much evidence to disclose to support their findings. Under international law, it is not an obligation for states to provide evidence of the basis upon which it attributes a cyber-attack to another state.⁴⁴

⁴⁴ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge

This constitutes one of the key dilemmas of public attribution. On one hand, a state's ability to persuasively communicate a finding to an intended audience depends, among other things, on its ability to provide strong evidence, its track record of accuracy and precision, and a transparent methodology that includes an independent review process.⁴⁵ On the other hand, the disclosure of such information also reveals sensitive sources of information and its methodology, and therefore allows adversaries to adapt their techniques, tactics, and strategies. For this purpose, Grotto developed a framework that distinguishes between analytical and strategic attribution.⁴⁶ While analytical attribution relies mainly on technical artifacts and all-source intelligence, strategic attribution refers to the process that follows the analytical attribution.

There are three types of strategic attribution:

- private (when an analytic attribution is not disclosed to third parties);
- selective (when an analytic attribution is disclosed to a select third party); and
- public (when an analytic attribution is made public).

Each of these options carries political and economic consequences for the state in deciding whether to publicly attribute a cyber-attack. These must be considered on a case-by-case basis.

2.5 Case study on Ukraine

The 2022 war in Ukraine is sometimes referred to as the first cyberwar. While this characterization is commonly disputed, the cyber dimension of this conflict is unprecedented and shows that future conflicts are likely to have a significant cyber component.

Ukraine has been subject to various cyber-attacks since 2014, but the number of incidents increased in the months preceding the beginning of the war. As of 6 February 2023, CyberPeace Institute, which monitors major cyber-attacks and cyber operations related to the conflict, counted 964 such events from over 75 different actors.⁴⁷ This included attacks against Ukraine (257 cyber-attacks) and Russia (178 cyber-attacks), as well as those that affected the rest of the world (529 cyber-attacks). According to the CyberPeace Institute, the origin of a significant number of these attacks is unknown, and most of the known ones are due to self-attribution. Figure 1⁴⁸ depicts the problematic nature of attributing cyber-attacks by showing that while some cyber-attacks have been technically attributed (65), a smaller number were politically attributed (15), and only two cyber-attacks have been legally attributed.

University Press, ch. 4, sec. 1, para. 13.

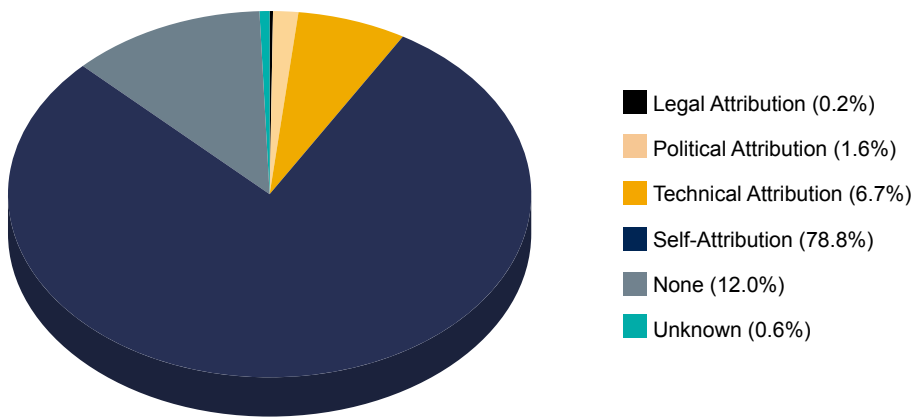
⁴⁵ Davis, John S. et al. 2017. *Stateless Attribution: Toward International Accountability in Cyberspace*. Rand Corporation

⁴⁶ Grotto, Andrew. 2020. 'Deconstructing Cyber Attribution: A Proposed Framework and Lexicon'. *IEEE Security and Privacy*, Vol 18, Iss. 1.

⁴⁷ See CyberPeace Institute. 'Cyber Threats'. Accessed 17 February 2023.

⁴⁸ This figure is based on data collected by the CyberPeace Institute. See CyberPeace Institute. 'Cyber Threats'. Accessed 17 February 2023.

Figure 1: Attribution of cyber-attacks during Russia-Ukraine war

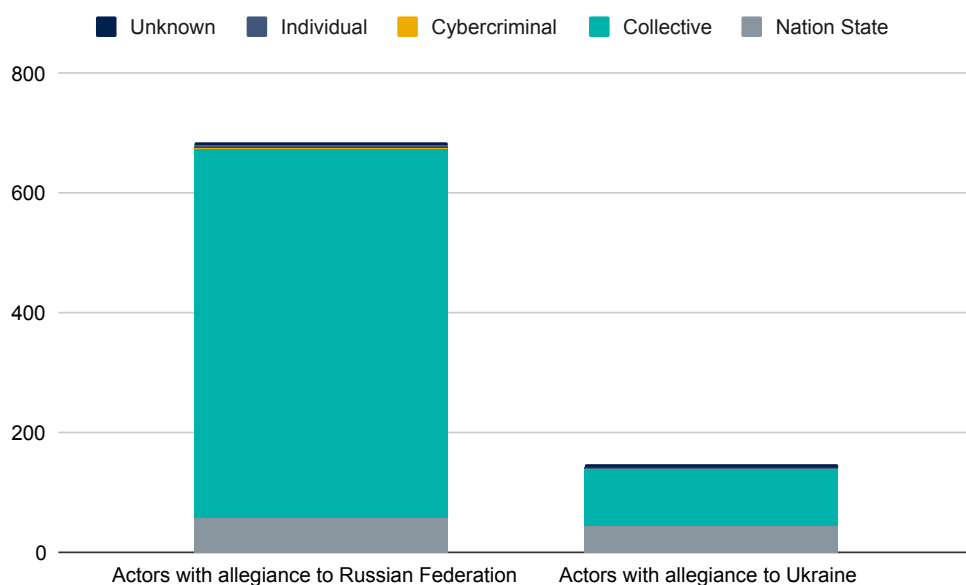


The perpetrators of these attacks can be grouped into three categories: nation state, collective, and cybercriminal. What is notable about this conflict is that a significant proportion of engaged actors are collectives rather than nation-state actors (see Figure 2).⁴⁹ In both cases, the involvement of cybercriminals is marginal, which can be explained by the fact that this is an international armed conflict and these actors typically pursue profit-making objectives. Main actors with allegiance to Ukraine include Anonymous, the IT Army of Ukraine, Haydamaki, NB65, GhostSec, RIA, Anonymous-Depaix Porteur, and Cyber Partisans (a Belarussian cyber collective). This categorization considers the IT Army of Ukraine as a collective rather than a state actor. Main actors with allegiance to Russia include cyber groups KillNet, NoName057(16), and National CyberArmy, as well as state-affiliated groups Sandworm, DEV-0586, UNC1151, Fancy Bear, and others. With respect to the different types of attribution, collectives have a higher tendency to self-attribute cyber-attacks, which is not the case for state actors. The primary attributing agency in Ukraine is the Computer Emergency Response Team of Ukraine (CERT-UA), while Russia has not publicly attributed any cyber-attacks against it.

It is important to note that the aforementioned distinction between nation states and collectives is only illustrative and should always be assessed on a case-by-case basis in light of international norms for attribution. As Russia and Ukraine are in an armed conflict, political attribution indicators are likely to play a much more significant role than during peacetime, and several actors that would normally not be considered as nation-state actors would now be labelled as such. This can be misleading, however, as the international standards of attribution are not precluded by war. For example, in the absence of effective controls, cyber-attacks carried out by non-state actors that support Russia, with Russian support, would not be attributable to Russia.

⁴⁹ This figure is based on data collected by the CyberPeace Institute. See CyberPeace Institute. 'Cyber Threats'. Accessed 17 February 2023.

Figure 2: Types of actors engages in Ukraine war, by number of attacks



The most notable case of a cyber-attack attribution in the Russia-Ukraine war – the only one considered as a legal attribution – is the cyber-attack on the satellite KA-SAT network owned by Viasat Inc, which took place on 24 February 2022. The attack affected tens of thousands of people in Ukraine and Europe, as well as the remote monitoring and control of approximately 5,800 Enercon wind turbines. This attack was caused by a new strain of malware called ‘AcidRain’, which is designed to remotely erase vulnerable modems and routers. The first technical attribution was conducted and publicly disclosed by SentinelLabs at the end of March 2022, when they discovered that AcidRain shared developmental similarities with a 2018 VPNFilter campaign previously attributed to the Russian government – the Sandworm group.⁵⁰ Several months later, the state publicly attributed this cyber-attack to the Russian government, more specifically the Russian foreign military intelligence agency. On 10 May 2022, the European Union (EU) condemned Russia’s malicious cyber activity, which targeted the satellite KA-SAT network owned by Viasat. In a press release, the high representative stated that the attack facilitated Russia’s military aggression; caused indiscriminate communication outages and disruptions across several public authorities, businesses, and users in Ukraine; and affected several EU member states.⁵¹ On the same day, the United States released a press statement also condemning Russia’s destructive cyber activities.⁵² Overall, at least 18 countries have released public statements that attribute this cyber-attack to the Russian government. Several statements declared that the cyber-attack was incompatible with international norms. The EU, for example, stated that ‘[t]his unacceptable cyberattack is yet another example of Russia’s continued pattern of irresponsible behaviour in cyberspace, which also formed an integral part of its illegal and unjustified invasion

⁵⁰ See Guerrero-Saade, Juan Andres. 2022. ‘AcidRain: A Modem Wiper Rains Down on Europe’. SentinelLabs.

⁵¹ Council of the European Union. 2022. ‘Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union’. Press release.

⁵² Blinken, Antony J. 2022. ‘Attribution of Russia’s Malicious Cyber Activity Against Ukraine’. Press statement.

of Ukraine. Such behaviour is contrary to the expectations set by all UN Member States, including the Russian Federation, of responsible State behaviour and the intentions of States in cyberspace.⁵³ Nevertheless, despite the extensive public attribution, there was no specific international response to the attack.

3. Responses to cyber-attacks

The central question for policymakers is how can states respond to cyber-attacks. The following section explores the factors affecting the scope and appropriateness of national responses to cyber-attacks, with a particular focus on their relation to attribution. In general, the number of considerations that contribute to a state's decision to respond to a cyber-attack is non-exhaustive, and may include the following: political and economic relations, technical capacities, degree of attribution certainty, applicable international instruments and international agreements concluded by the state, public opinion, and internal politics. This section considers several key considerations for decision-makers with respect to attribution and international norms.

3.1 Has the cyber-attack been attributed to a state?

A state bears international responsibility for a cyber-related act if it is attributable to the state and constitutes a breach of an international legal obligation.⁵⁴ This includes not only cases where a cyber operation is conducted by a state, but also instances where a state makes its cyber infrastructure available to non-state groups or other states, fails to take necessary measures to terminate cyber operations in its territory, or provides hardware or software to conduct such operations.⁵⁵ In cases where a cyber-attack cannot be attributed to a given state, this does not mean that the state bears no responsibility. A state can be held responsible for its role in a cyber-attack if its conduct violates a primary norm of international law. For example, if a state provides a non-state group with malware that is subsequently used for a cyber-attack, the state may still be held responsible, although the attack cannot be attributed to it, because it violated norm of prohibited intervention by state (Tallinn Manual 2.0, Rule 66).⁵⁶ Attribution in this case would concern the provision of malware to a non-state group, rather than the cyber-attack itself.

As the attribution of an internationally wrongful act is one of the fundamental principles of legality and the rule of law, attributions must be based on convincing evidence to trigger responses under

⁵³ Council of the European Union. 2022. 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union'. Press release.

⁵⁴ See ILC. 2001. Responsibility of States for Internationally Wrongful Acts, art. 2; Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, rule 14.

⁵⁵ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. 84-85.

⁵⁶ Ibid., rule 17, para. 9.

international law (such as counter-measures and self-defence). If a state plans to make a counter-measure, they must first identify the wrongdoer at the requisite level of legal certainty before imposing a coercive measure to enforce legal rights; to do otherwise would go against the principles of legality, which require, as a matter of fairness, that punishment is imposed only on the perpetrator and not the innocent.⁵⁷ In the absence of attribution, the scope of lawful responses is limited to those permitted under international law at all times. Any attribution claim can, of course, be disputed but, in the absence of any evidentiary standards under international law or an international investigatory or adjudicatory body on this matter, such contestation does not preclude counter-measures. If a misattribution occurred, however, a counter-measure used by a state can be retroactively considered as an unlawful response, meaning that the responding state itself conducted a wrongful act.⁵⁸

3.2 Was the attribution public?

Whether an attribution was made public does not limit the scope of responses that a state can take. There is no international obligation to make the attribution of a cyber-attack public, nor is there an obligation to provide the evidence upon which the cyber attribution is made when responding in accordance with the law of state responsibility.⁵⁹ Nevertheless, if a state decides to respond with counter-measures or another action that would normally be considered wrongful (such as the use of force), the responding state has to invoke state responsibility by attributing the wrongful act in order to preclude its wrongfulness.⁶⁰ To do so, the injured state must give notice of its claim to the allegedly responsible state.⁶¹ This notice can take a variety of forms – for example, an unofficial and confidential reminder of the need to fulfil the obligation, a formal protest, or a consultation. Failure to do so may have legal consequences, including the eventual loss of the right to invoke responsibility by waiver or acquiescence.⁶²

3.3 What is the scale and nature of the cyber-attack?

The presence of an internationally wrongful act is a prerequisite for the invocation of state responsibility. Acts that are not regulated under international law, such a peacetime cyber espionage,⁶³ would thus not warrant counter-measures. The nature and scale of the cyber-attack

⁵⁷ O'Connell, Mary Ellen. 2020. 'Attribution and Other Conditions of Lawful Countermeasures to Cyber Misconduct'. *Notre Dame Journal of International & Comparative Law*, Vol. 10, Iss. 1.

⁵⁸ International law does not currently provide clear norms on this matter. For more information, see Yang, Fan. 2022. 'The Problem with Ill-Substantiated Public Cyber Attribution: A Legal Perspective', in Ariel E. Levite, Lu Chuanying, George Perkovich and Fan Yang, eds., *Managing U.S.-China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace and Shanghai Institutes for International Studies, p. 12.

⁵⁹ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, ch. 4, sec. 1, para. 13.

⁶⁰ *Ibid.*, rule 20.

⁶¹ See ILC. 2001. Responsibility of States for Internationally Wrongful Acts, arts. 43, 52.

⁶² See ILC. 2001. Responsibility of States for Internationally Wrongful Acts, art. 43, para. 2 of commentary.

⁶³ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, rule 32.

would determine the wrongful act or omission at hand, as well as the applicable legal regime that may warrant specific responses. For example, large-scale indiscriminate attacks on civilian critical cyber infrastructure may constitute war crimes that would fall under the jurisdiction of the International Criminal Court (ICC) (see case study below).⁶⁴ Furthermore, the scale and nature of a cyber-attack determines the permissible scale of response. For example, counter-measures must be commensurate with the injury suffered – taking into account the gravity of the internationally wrongful act and the rights in question.⁶⁵

These considerations ultimately shape states' decisions on how to respond adequately to a cyber-attack. The table below outlines the main types of responses that states can take in light of the severity of the cyber-attack and other geopolitical and strategic considerations.

Table 3: Main types of responses to cyber-attacks

Category	Response	Description of Response	Attribution Requirement	International Legal Regime
Retorsion and diplomatic responses	Acquiescence and strengthening cybersecurity	Internal lawful defensive measures	No	n/a
	Diplomatic protests	Public or confidential diplomatic statement from state or international organization; expulsion of diplomats (predominantly reputational damage)		
	Legal measures	Indictment of individuals or organizations responsible for a cyber-attack at the national level, or claims against states at the international level	Yes	Usually national criminal law
	Retorsion	Unfriendly acts that are permissible under international law (such as cyber espionage), including political and economic sanctions if they do not breach states' international obligations. Political sanctions include blacklisting persons and organizations involved in cyber-attacks	No (but may be required in some cases)	n/a

⁶⁴ Ambos, Kai. 2022. 'Cyber-Attacks as International Crimes under the Rome Statute of the International Criminal Court?'. ICC Forum 2022.

⁶⁵ See ILC. 2001. Responsibility of States for Internationally Wrongful Acts, art. 51.

		and limiting their travel and ability to make international financial transactions. Economic sanctions may prohibit economic transactions with the responsible country.		
	Cyber counter-measures	Counter-cyber-attacks against the responsible state proportional to the injury incurred, intended to stop the wrongful act. Political and economic sanctions are considered within this category if the act would, under normal circumstances, be considered as a breach of a state's international obligation.	Yes	Public international law (on state responsibility)
	Other non-cyber counter-measures	All other non-forcible counter-measures against the responsible state proportional to the injury incurred, intended to stop the wrongful act, which would, under normal circumstances, be unlawful.		
Use of force	Use of force	Grave forms of intervention that may involve the use of armed force; requires authorization from the UN Security Council	Yes	UN Charter
	Armed attack	Only permissible if conducted in self-defence under the UN Charter		

Some sources refer to cyber retaliation as a response to cyber-attacks.⁶⁶ While this may occur in practice, it is not permissible under international law, since all counter-measures must aim to ensure the cessation of the wrongful act, as well as subsequent assurances of non-repetition and reparation.⁶⁷ The table above shows that any form of response that triggers a legal regime requires an attribution of the wrongful act. This includes, in particular, all responses that would, under normal circumstances, be in violation of international law. The most frequently used responses are those under the category of retorsion and diplomatic responses. While the use of force has never been employed, nor has self-defence been invoked, in response to a cyber-attack, these responses remain permissible if a cyber operation rises to the level of an armed attack.⁶⁸ It is worth noting that the greater the gravity of a state's response to a cyber-attack, the greater the likelihood that the situation will escalate. To prevent such escalation, the UN Charter provides that 'all Members shall settle their international disputes by peaceful means in such a

⁶⁶ See, for example, van der Meer, Sico. 2018. 'State-level responses to massive cyber-attacks: a policy toolbox'. Clingendael Policy Brief.

⁶⁷ See ILC. 2001. Responsibility of States for Internationally Wrongful Acts, arts. 48(2), 49.

⁶⁸ Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, rule 71.

manner that international peace and security and justice are not endangered'.⁶⁹ Article 33 states that '[t]he parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice'.⁷⁰ It follows that states must exhaust all possible avenues to resolve a dispute before resorting to non-peaceful responses.

To illustrate this point, three examples of responses to cyber-attacks will be outlined: Albania's severance of diplomatic relations with Iran in response to a cyber-attack; the EU cyber sanctions regime; and consideration by the ICC of a cyber operation carried out by the Sandworm group.

3.4 Diplomatic protests

On 15 July 2022, Albania suffered a cyber-attack that prevented access to governmental websites and services. The attack was launched by Iranian state cyber actors identified as 'Home-Land Justice', who on July 18 claimed credit for the cyber-attack and later posted videos of the attack on their website.

The investigation into the attack was conducted in parallel by several actors. The preliminary results, together with the technical analysis, were published by the cybersecurity firm Mandiant, which assessed 'with moderate confidence' that one or multiple threat actors supporting Iranian goals were involved.⁷¹ Further findings of the investigation were announced following the Albanian government's public attribution of the attack on 7 September. The US government declared that, together with private sector partners, it supported the investigation into the cyber-attack.⁷² The United Kingdom announced that the National Cyber Security Centre (NCSC) had assessed that Iranian state-linked cyber actors were almost certainly responsible for the series of cyber-attacks against the Albanian government and condemned this conduct.⁷³ In late September, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity Advisory providing technical details of the investigation. The investigation showed that Iranian state cyber actors acquired initial access to the victim's network approximately 14 months before launching the destructive cyber-attack, which included a ransomware-style file encryptor and disk wiping malware.⁷⁴ The actors maintained continuous network access for approximately a year, periodically accessing and exfiltrating email content.

⁶⁹ UN (United Nations). 1945. [Charter of the United Nations](#). 24 October, art. 2(3).

⁷⁰ *Ibid.*, art. 33.

⁷¹ Jenkins, Luke, Emiel Haeghebaert, Alice Revelli, and Ben Read. 2022. '[Likely Iranian Threat Actor Conducts Politically Motivated Disruptive Activity Against Albanian Government Organizations](#)'. Mandiant. 4 August.

⁷² Watson, Adrienne. 2022. '[Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania](#)'. The White House. 7 September.

⁷³ Foreign, Commonwealth & Development Office and The Rt Hon James Cleverly MP. 2022. '[UK condemns Iran for reckless cyber attack against Albania](#)'. Press release. 7 September.

⁷⁴ Cybersecurity & Infrastructure Security Agency. 2022. '[Iranian State Actors Conduct Cyber Operations Against the Government of Albania](#)'. Cybersecurity Advisory. 23 September.

Along with publicly attributing the cyber-attack to the Iranian government on 7 September, Albania severed diplomatic relations with Iran and expelled its diplomats with 24 hours' notice. In his announcement, Prime Minister Edi Rama said that this extreme response was 'fully proportionate to the gravity and risk of the cyberattack that threatened to paralyse public services, erase digital systems and hack into state record, steal government intranet electronic communication and stir chaos and insecurity in the country'.⁷⁵ On the same day the Spokesperson of the US National Security Council said that the United States strongly condemned Iran's cyber-attack and would 'take further action to hold Iran accountable for its actions that threaten the security of its ally and set a troubling precedence for cyberspace'.⁷⁶ The United States promised to take measures to support its NATO ally. One day later, the North Atlantic Council issued a statement that acknowledged the declarations of Albania and other allies attributing the responsibility for the cyber-attack to the government of Iran.⁷⁷ The Albanian government's response was unprecedented and constitutes the first instance of a country severing diplomatic relations due to a cyber-attack.

3.5 Retorsion

In 2017, the Council of the European Union adopted a decision on restrictive measures against cyber-attacks threatening the Union or its member states, which effectively enabled it to use sanctions against aggressors in cyberspace.⁷⁸ In 2020, the EU imposed its first cyber-related sanctions against six individuals and three entities involved in significant cyber-attacks or attempted cyber-attacks against the EU or its member states. The sanctions include travel bans and the freezing of assets. In addition, EU persons and entities are forbidden from making funds available to those listed.⁷⁹ The cyber sanctions regime was extended to 18 May 2025 and individual listings are reviewed every 12 months.⁸⁰ The sanctions target, among others, two Russian state agencies: the Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of Russian Federation (GU/GRU) and the 85th Centre for Special Services (GTsSS) of the GRU. The sanctions against GTsST were adopted due to the agency's role in conducting two cyber-attacks in 2017 referred to as 'NotPetya' or 'EternalPetya', and attacks targeting the Ukrainian power grid in winter 2015 and 2016, which later spread into Europe and worldwide, rendering data inaccessible and resulting in significant economic loss. In addition, GTsST played an active role in the cyber activities undertaken by Sandworm.⁸¹ GTsSS

⁷⁵ Reuters. 2022. 'Albania cuts Iran ties over cyberattack, U.S. vows further action'. 7 September.

⁷⁶ Watson, Adrienne. 2022. 'Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania'. The White House. 7 September.

⁷⁷ NATO. 2022. 'Statement by the North Atlantic Council concerning the malicious cyber activities against Albania'. Press Release 118. 8 September.

⁷⁸ EU Council (Council of the European Union). 2019. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. *Official Journal of the European Union*. ST/7299/2019/INT.

⁷⁹ The Diplomatic Service of the European Union. 2020. 'EU imposes first ever cyber sanctions to protect itself from cyber-attacks'.

⁸⁰ EU Council. 2022. 'Cyber-attacks : Council extends sanctions regime until 18 May 2025'. Press release.

⁸¹ EU Council. 2020. Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning

was targeted as it was considered responsible for cyber-attacks carried out in April and May 2015 against the German Federal Parliament, as well as for attempted cyber-attacks aimed at hacking into the Wi-Fi network of the Organization for the Prohibition of Chemical Weapons (OPCW) in April 2018.⁸² In addition to the two entities, several GRU officers were also added to the sanctions list – including two human intelligence officers and two cyber operators involved in the attempted cyber-attack on the OPCW, as well as one military intelligence officer and the Head of the GRU for their role in the cyber-attack on the German Federal Parliament.

3.6 Legal measures

The last case concerns a cyber-attack that targeted electric utilities in western Ukraine in December 2015 and in Kyiv in 2016, leading to blackouts that affected hundreds of thousands of civilians. This attack has been attributed to a group of hackers called Sandworm who are associated with the GRU. This case was picked up by the Human Rights Center at the University of California, Berkeley, which sent a formal request in March 2022 to the Office of the Prosecutor for the ICC in the Hague. In its request, the Center urged the ICC ‘to consider war crime prosecutions of Russian hackers for their cyber-attacks in Ukraine’, together with more traditional war crime claims related to the Russia-Ukraine conflict.⁸³ The non-governmental organization also recommended that the prosecutor ‘expand the scope of his investigation to include the cyber domain in addition to traditional domains of warfare – land, air, maritime, and space – given the Russian Federation’s history of hostile cyber activities in Ukraine’.⁸⁴ The ICC Prosecutor’s Office is currently considering the recommendation, which would constitute the first case of cyber war crimes adjudicated at the ICC. At the domestic level, Sandworm hackers already face criminal charges – the US State Department issued a bounty of up to 10 million USD for information that could lead to their capture. In addition to providing justice for the victims of the cyber-attacks, however, prosecution by an international court could serve as a broader deterrent against attacks on civilian infrastructure as it would enable such acts to be considered as war crimes and adjudicated by all states that employ universal jurisdiction. While the court’s final decision is unclear, Ukrainian officials have been gathering evidence of cyber-attacks linked to military strikes and sharing this information with the ICC in an effort to support potential prosecutions of Russia’s actions.⁸⁵

[restrictive measures against cyber-attacks threatening the Union or its Member States](#). *Official Journal of the European Union*. Document 32020R1125. ST/9568/2020/INIT.

⁸² EU Council. 2020. [Council Implementing Regulation \(EU\) 2020/1536 of 22 October 2020 of implementing Regulation \(EU\) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States](#). *Official Journal of the European Union*. Document 32020R1536.

⁸³ Greenberg, Andy. 2022. [‘The Case for War Crimes Charges Against Russia’s Sandworm Hackers’](#). *Wired*.

⁸⁴ *Ibid.*

⁸⁵ Van Sant, Shannon. 2023. [‘Kyiv argues Russian cyberattacks could be war crimes’](#). *Politico*.

4. Role of parliaments in cyber-attack attribution and subsequent responses

When it comes to the attribution of, and responses to, cyber-attacks, the role of parliaments is limited. Cyber-attack investigations are generally conducted by designated government bodies (such as the NCSC in the United Kingdom; the CISA, FBI, and Cyber National Mission Force and National Security Agency in the United States; and the Australian Cyber Security Centre in Australia) – sometimes in cooperation with private cybersecurity companies or in coordination with international partners. Similarly, the decision to publicly attribute a cyber-attack and respond to it lies in the hands of the government. The role of parliament in this regard is twofold: 1) to ensure there is an adequate domestic legal framework to facilitate these processes, and 2) to oversee these processes to guarantee they are conducted in line with domestic and international law. To this end, parliamentarians should ensure the following:

Development of domestic legislation:

- ◇ **Delineation of domestic jurisdiction and critical infrastructure:** International law provides little to no guidance on which areas of cyberspace fall under domestic jurisdiction and which constitute critical infrastructure. In light of this, parliaments can develop legislation that clarifies this distinction. This allows for the criminalization of cyber-attacks in areas that fall under a state's jurisdiction, and for more stringent and severe responses to attacks on critical infrastructure.
- ◇ **Criminalization of cyber-attacks:** Parliaments should ensure there is clear legislation on cyber-attacks that not only defines what constitutes cybercrime under a state's jurisdiction, but also stipulates how the existing criminal code and other laws apply to cyber-attacks. The legislation should specify the level of legal certainty required for the attribution of the cyber-attack and the applicability of the criminal code.
- ◇ **Development of a legal framework for cyber-attack investigations:** Parliaments should ensure that domestic legislation delegates authority to the appropriate state agencies to investigate cyber-attacks and issue authoritative reports of their investigation to relevant government bodies. Such legislation can specify the potential to cooperate with private companies and international partners on this matter and outline applicable requirements for such cooperation (for example, in the case of private companies, this can include vetting procedures or the applicability of the law on state secrets). Furthermore, such legislation can include a requirement for the appropriate state agencies to report on the findings of cyber-attack investigation to the parliament, which can facilitate the parliament's ability to oversee the ongoing process.
- ◇ **Development of a legal framework on international responses to cyber-attacks:** While few states have such a legal framework, this can define permissible or even obligatory responses for government for certain types of cyber-attack. The legal framework must conform to the state's obligations under international law, including ensuring the

progressive stages and severity of response correspond to the severity of the cyber-attack. The legislation should further specify the level of legal certainty in the cyber-attack attribution required to trigger a state response. Furthermore, such legislation can include a requirement for the appropriate government bodies to report on, and provide justification for, their responses, which can facilitate the parliament's ability to oversee the ongoing response.

- ◇ **Oversight:** Oversight of cyber-attack attribution and subsequent response: Parliaments should ensure that cyber-attack investigations reach the requisite level of legal certainty and that the subsequent response conforms to the state's domestic law and international obligations. To this end, parliaments can require state agencies to issue reports and conduct hearings with relevant representatives. Beyond compliance with domestic and international law, parliamentarians can inquire about whether the processes were conducted in cooperation with private companies and international partners to assess the reliability of the cyber-attack attribution and the effectiveness of the response.

5. Recommendations

The following recommendations outline ways to address – at both the national and international level – the existing challenges of cyber-attack attribution:

- **Development of national evidentiary standards for cyber-attack attribution:** At the national level, policymakers should specify the evidentiary standards to be applied by agencies responsible for cyber-attack investigations. If the cyber-attack investigation is outsourced or conducted in cooperation with private companies, authorities should specify the standards to be applied by the service providers in their investigation.
- **Development of a national cyber-attack attribution methodology:** At the national level, policymakers should specify the applicable methodology for cyber-attack investigations, both for the responsible state agencies as well as for private companies that cooperate with state authorities in this area.
- **Development of national policies on the disclosure of evidence for cyber-attack attribution:** While disclosing evidence for the attribution of a cyber-attack may carry certain risks and there is no international obligation to do so, in the absence of any supporting evidence, the attribution may put into question the legitimacy of the state's position and the legitimacy of any subsequent response. Policymakers should aim to develop policies on the disclosure of evidence for cyber-attack attributions to the public and to international partners. These policies should consider what evidence can be communicated and what should remain confidential (for example, intelligence gathered from classified information).
- **Multi-stakeholder coordination of attribution investigations and public attributions:** National actors should aim to coordinate the findings of their cyber-attack investigations and public attributions with those of international partners and, if applicable, non-state actors (private companies and non-governmental organizations). Such coordination significantly

increases the authoritativeness of state findings and condemnation of irresponsible behaviour in cyberspace.

- **Response following public attribution:** If a public attribution is not followed by a national response, it is not an effective deterrent against adversaries and fosters an environment of impunity. National authorities should consider potential responses prior to publicly attributing a cyber-attack. If possible, the steps that the national authorities are going to take to respond to the responsible perpetrator should be outlined clearly at the same time as the public attribution.
- **International norm-setting, consensus-building, and harmonization:** National authorities should take steps at the international level to foster norm-setting, consensus-building, and the harmonization of cyber-attack attribution norms and standards – particularly regarding the evidentiary standards and methodology for cyber-attack attribution. This can take the following forms:
 - **Bilateral or multilateral agreements and coordination:** Allied states are encouraged to harmonize the evidentiary standards and methodology they apply in cyber-attack investigations. This will enable the verification and corroboration of attribution findings and increase the authoritativeness of investigation findings.
 - **International coalition on cyber attribution:** The creation of international forums and platforms where like-minded states can discuss their attribution policies and define common norms in this area will contribute to norm-setting, consensus-building, and the international harmonization of attribution standards. Such forums can help foster inter-state dialogue and the exchange of good practices in cyber-attack attribution.
 - **Establishment of an international organization for cyber-attack attribution:** The creation of a permanent international entity for cyber-attack attribution has been proposed numerous times by various actors.⁸⁶ While no such organization exists to this day, its establishment would help to foster international norm-setting on cyber-attack attribution, to develop effective methodologies to this end, and to review public attribution claims. Such organizations could further support states' capacities and efforts to investigate cyber-attacks, as well as issue authoritative public cyber-attack attributions.

⁸⁶ Microsoft. n.d. '[An attribution organization to strengthen trust online](#)'. Policy Paper; Healey, Jason, John C. Mallery, Klara Tothova Jordan, and Nathaniel Youd. 2014. [Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security](#). Atlantic Council. 5 November; Davis, John S. et al. 2017. [Stateless Attribution: Toward International Accountability in Cyberspace](#). Rand Corporation; Droz, Serge and Daniel Stauffacher. 2018. '[Trust and Attribution in Cyberspace: A Proposal for an Independent Network of Organizations Engaging in Attribution Peer-review](#)'. ICT4Peace Foundation. Cyber Security Policy Process Brief.

CHAPTER 4

Cybersecurity and its challenges: an introduction for members of parliament

by Teodora Fuior

*'In the world of cybersecurity,
if you are standing still you are going backwards'.*
Dan Tehan, Australian politician

Table of contents

	Introduction.....	73
1.	Exploring what makes cybersecurity different from traditional security.....	76
2.	Defining the cybersecurity realm.....	79
3.	Writing comprehensive cybersecurity legislation.....	83
4.	Harmonizing national laws with international norms.....	87
5.	Identifying good practice in cybersecurity oversight.....	92

Introduction

Parliaments shape and prepare the future of our societies by debating and endorsing policies, enacting laws, and approving budgets, to enable the delivery of public services and to prioritize government actions. But parliaments are also judges of the past, as they monitor, assess, and control how strategies, laws, and budgets have been implemented. Indeed, parliamentary oversight is a retrospective analysis of the legality, effectiveness, and appropriateness of government action. It seeks to uncover potential wrongdoing, inefficiencies, or failures in governance, and prescribes remedies to improve accountability and decision making.

Cybersecurity is among the many areas parliaments affect through policy and for which they have oversight responsibilities, and the 2007 digital siege of Estonia placed cybersecurity high on the agenda of policymakers across the globe.¹ Recognized as the world's first significant cyber event, it foreshadowed the power, multi-dimensionality, and omnipresence of cyber threats and their potential to destabilize nations and cause widespread political and economic turmoil. More recent cyberattacks on government websites and public services across Europe have also demonstrated how important it is that countries have a functioning cybersecurity system, to protect national security as well as the integrity of democratic processes and the rights and lives of citizens. Thus, parliaments across the globe must take on the new responsibility of engaging meaningfully in cybersecurity.

As digitalization accelerates, more and more services are delivered online, increasing speed and efficiency but also producing volumes of data that are being collected and used by government and industry systems. The coronavirus pandemic has also changed the traditional office environment, moving ever more corporate data into 'the cloud'. Our individual and collective vulnerability to personal data breaches, the theft of sensitive information, critical infrastructure attacks, and other forms of cybercrime is only growing. Securing cyberspace is therefore a concern of government and state agencies, private companies, and individuals alike.

Legislators are expected to play a key role by ensuring that national cybersecurity systems are comprehensively regulated, well-resourced, and effective. Yet, the complex and rapidly evolving nature of cybersecurity brings significant challenges both as far as lawmaking and oversight. Successfully addressing these challenges requires the appropriate combination of technical expertise, legislative agility, and international cooperation, alongside a thorough understanding of various cyber phenomena and their place in the evolving cyber threat landscape. This chapter will explore some of the differences between cybersecurity and traditional security and the challenges cyber threats raise for lawmaking and oversight, and will highlight good practices developed in some national parliaments – which may inspire parliamentary action elsewhere.

1 Heli Tiirmaa-Klaar, 'The Evolution of the UN Group of Governmental Experts on Cyber Issues: From a Marginal Group to a Major International Security Norm-Setting Body', Cyberstability Paper Series, Global Commission on the Stability of Cyberspace and The Hague Centre for Strategic Studies, 2021. Available as a PDF at: <https://hcsc.nl/wp-content/uploads/2021/12/Klaar.pdf>

Box 1. Cyberattacks and hybrid warfare

Recent years have seen a proliferation of cyberattacks on governmental and parliamentary websites.² These attacks send a clear message about the vulnerability of democratic institutions and may obstruct essential governmental functions, voting processes, and decision-making mechanisms, eroding public trust and fomenting social divisions. Breaches of government systems may also result in direct harm to citizens by impacting essential public services such as health care, emergency response, or public utilities.

In the context of hybrid warfare, cyberattacks on parliament and government websites are not just isolated incidents of digital vandalism, but strategic manoeuvres designed to destabilize, confuse, and demoralize targeted states. The increasing frequency of these attacks highlights the evolving nature of global conflicts in the digital age.

Costa Rica suffered a series of ransomware attacks to its public sector in April and May 2022, marking the first time a cybersecurity incident led to a national emergency declaration, and representing the first time a ransomware group explicitly targeted a national government and called for it to be overthrown.³ Initiated by the Russia-based criminal organization Conti (known to use ransomware since 2020), the attack began at the Ministry of Finance and quickly spread to some 30 other central and local government authorities, and to the health system. The country was unable to pay the salaries of government employees, or collect taxes, payments, and customs duties. Tens of thousands of state employees were affected by disrupted payroll systems, inciting public unrest. On top of this, the attackers posted more than 600 GB of government data online, including taxpayers' information. The private sector lost some USD 38 million daily, and imports and exports stalled.⁴

Montenegro was struck by a massive cyberattack in August 2022, which the Agency for National Security attributed to 'coordinated Russian services'. The attack crippled online government information platforms and put Montenegro's essential infrastructure, including banking, transportation services, and utilities at high risk. Several services had to be taken offline or

² Cyberattacks appear to be a prevalent tool in what many have described as Russia's 'hybrid warfare against the West'. This merges traditional military strategies with non-traditional tactics like cyber warfare, disinformation campaigns, and political influence operations. When a country's leadership is under siege in the digital realm, it can demoralize the population and make them more amenable to alternative narratives or external influences. For example, see: Mason Clark, 'Russian Hybrid Warfare', Military Learning and the Future of War Series, Institute for the Study of War, 2020. Available as a PDF at: <https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf>

³ Jonathan Reed, 'Costa Rica state of emergency declared after ransomware attacks', Security Intelligence, 16 November 2022. Available at: <https://securityintelligence.com/news/costa-rica-state-emergency-ransomware/>

⁴ Christine Murry & Mehul Srivastava, 'How Conti ransomware group crippled Costa Rica — then fell apart', Financial Times, 9 July 2022. Available at: <https://www.ft.com/content/9895f997-5941-445c-9572-9cef66d130f5>

disabled to preserve data and operations.⁵ NATO allies provided support in monitoring and combatting the attacks and a US FBI team assisted the local investigation.⁶

Bosnia and Herzegovina (BiH) was targeted by an attack that crippled state parliamentary websites and servers for several weeks in September 2022. Though this attack was confirmed by the State Investigation and Protection Agency, there has been no official comment on eventual data leaks that may have resulted or whether the incident was connected to previous attacks in Albania and Montenegro.⁷ The attack took place at a time of growing tensions over approaching general elections, which left the country in a state of uncertainty and citizens particularly vulnerable to misinformation.⁸

Norway experienced a significant cyberattack on its parliament in 2020, when the email accounts of several members and employees were breached. The attack was attributed to Russia.⁹ The **European Parliament** was targeted by a sophisticated cyberattack in November 2022 that brought its website down just hours after MEPs passed a resolution declaring Russia a 'state sponsor of terrorism'. A pro-Kremlin group claimed responsibility.¹⁰ **Poland**¹¹ and **Lithuania**¹² have also been hit by cyberattacks on their parliaments while members were in the midst of voting on declarations for economic measures against Russia. Also, **Switzerland** experienced an 'exceptionally high' intensity DDoS attack in June 2023, directed against government websites including that of parliament and the federal administration, while the Swiss parliament was preparing for a video address by Ukrainian President Volodymyr Zelensky.¹³

5 Associated Press, 'Montenegro Wrestles Massive Attack. Russia Blamed', 22 September 2022. Available at: <https://www.securityweek.com/montenegro-wrestles-massive-cyberattack-russia-blamed>

6 Ines Kagubare, 'Cyber officials prioritizing securing critical sectors, foreign partnerships amid rising threats', The Hill, 27 October 2022. Available at: [Cyber officials prioritizing securing critical sectors, foreign partnerships amid rising threats | The Hill](https://www.thehill.com/cybersecurity/cyber-attacks/364444-cyber-officials-prioritizing-securing-critical-sectors-foreign-partnerships-amid-rising-threats/)

7 Azem Kurtici, 'Bosnia Remains Silent on Hacker Attack on Parliament', BIRN, 28 September 2022. Available at: [Bosnia Remains Silent on Hacker Attack on Parliament | Balkan Insight](https://www.birneurope.eu/en/bosnia-remains-silent-on-hacker-attack-on-parliament/)

8 Mat Mastracci, 'Bosnia's Contested Election Sparks Heated Rhetoric Online', BIRN, 17 October 2022. Available at: [Bosnia's Contested Election Sparks Heated Rhetoric Online | Balkan Insight](https://www.birneurope.eu/en/bosnia-s-contested-election-sparks-heated-rhetoric-online/)

9 BBC, 'Norway Blames Russia for Cyberattack on Parliament', 13 October 2020. Available at: <https://www.bbc.com/news/world-europe-54518106>

10 Euronews, 'EU Parliament website hacked after MEPs passed critical Russian resolution', 23 November 2022. Available at: https://www.euronews.com/my-europe/2022/11/23/eu-parliament-website-down-after-passing-resolution-calling-russia-a-state-sponsor-of-terror

11 AFP, 'Slovak, Polish Parliaments Hit by Cyberattacks', 28 October 2022. Available at: <https://www.securityweek.com/slovak-polish-parliaments-hit-cyberattacks/>

12 AFP, 'Lithuania Says Hit by Cyberattack, Russia 'Probably' to Blame', 27 June 2022. Available at: <https://www.securityweek.com/lithuania-says-hit-cyberattack-russia-probably-blame/>

13 Reuters, 'Pro-Russian Hackers Step-up Attacks against Swiss Targets', 14 June 2023. Available at: <https://www.swissinfo.ch/eng/politics/pro-russian-hackers-step-up-attacks-against-swiss-targets/48588976>

1. Exploring what makes cybersecurity different from traditional security

The nature of cyberspace poses unique challenges when it comes to developing legal and policy frameworks. It is relatively novel, complex, and dynamic, and encompasses a wide range of actors and aspects, across many disciplines and industries. Moreover, cyber phenomena – whether cyber warfare, cybercrime, artificial intelligence or digitalization – are constantly evolving. Crafting effective regulatory tools while striking a balance between security, privacy, and innovation is a difficult task, as inherent challenges arise from the characteristics of cybersecurity itself. Some of these are briefly outlined below.

Cyber threats perpetually adapt and evolve, and at a much faster pace than traditional security threats, making them harder to anticipate and mitigate. As new attack methods emerge, driven by rapid advancements in technology, the legal landscape surrounding cyber activities and the prosecution of cybercrime must be agile enough to adapt as well. To that end, parliaments must engage in ongoing monitoring of cyber developments, must access high level experts in the field to understand cyber phenomena, and must have the political will and capacity to respond swiftly to complex developments.

Cyber threats and cybercrime are not confined by national borders, unlike most traditional security threats. Cybercrime can involve aggressors and victims in different countries, and cyberattacks can be launched from virtually any location. The borderless nature of cyberspace confuses the legal questions of jurisdiction and attribution, complicating (or even precluding) the imposition of sanctions in response to some cybercrimes. Establishing comprehensive and coherent legislative frameworks is thus a challenge. This means that international cooperation and coordination among national cybersecurity counterparts is essential to addressing global threats. However, private companies operating internationally may not be fully accountable to national oversight bodies, potentially making the task of parliamentary scrutiny more difficult.

Cyberattacks are cost-effective as a means of warfare because they require a smaller financial investment than conventional warfare. A well-coordinated cyberattack can yield significant disruptions and instability at a fraction of the cost of kinetic military operations, and can incur considerable financial costs on a target.¹⁴

The lines are blurred between state-sponsored attacks and non-state cybercriminal activities, which makes it more challenging to attribute attacks and respond to them. Both state-sponsored cyber attackers and non-state actors working with criminal organizations and hacktivists

¹⁴ According to the European Commission, the annual cost of cybercrime to the global economy is estimated to have reached €5.5 trillion by the end of 2020, doubling the figure from 2015. Information available at: <https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/>

can pose equally significant threats. Yet, even when indications point to the responsibility of a particular state, definitive attribution can be elusive. In fact, as a strategic tool of governments, part of what cyberattacks offer is deniability, providing aggressor states a means of exerting influence or causing disruption without engaging in overt acts of war, reducing the risk of direct retaliation. This calls for a multifaceted approach to cybersecurity that incorporates diplomatic and law enforcement elements.

Public-private collaboration is crucial to cybersecurity, in contrast to other areas of national security, where the state has primary responsibility. Because cybersecurity involves the participation of technology companies, critical infrastructure operators, and other private entities, effective cybersecurity can only be achieved by collaborating, sharing information, and coordinating response efforts between the public and private sectors. However, when both public and private entities are involved, responsibilities may be divided or shared in ways that are not always clear, and this can make it more challenging to deliver comprehensive, effective oversight. While public sector entities are responsible and must answer to legislative bodies like parliament, private entities such as technology firms or private infrastructure operators are primarily accountable to their shareholders or private boards. Hence, there is a discrepancy in how accountability is enforced across sectors; and when both the public and private sectors collaborate on cybersecurity but only public entities are directly accountable to parliament, there can be some ambiguity as to how accountability is enforceable across the whole cybersecurity system. This can result in regulatory gaps and oversight deficits, ultimately undermining the effectiveness of cybersecurity measures.

Cybersecurity is a highly technical field, in which new vulnerabilities, attack vectors, and hacking techniques emerge frequently. Staying ahead of cyber threats requires continuous learning about a vast and complex ecosystem of interconnected networks, devices, software, protocols, and standards, used across diverse sectors and industries. Thus, understanding how to secure this intricate web of interconnected systems and ensure their resilience poses significant and specific challenges when compared to more traditional physical security domains.

Many technologies have dual-use capabilities and may be used for both legitimate and malicious activities. In other words, the same technologies that enable economic growth, innovation, and social benefit also introduce potential vulnerabilities to cyberattack. This complicates the task of designing effective cybersecurity measures, as they must avoid hindering technological advancements while also protecting privacy and individual rights.

Balancing security and privacy in cybersecurity systems is particularly challenging, as effective cybersecurity measures often involve the collection, sharing, and analysis of personal data. Finding a regulatory approach that can strike the right balance between ensuring robust security measures and protecting individual privacy rights requires careful consideration and in-

formed decision making. For example, the European Union's General Data Protection Regulation (GDPR) is a regulatory framework designed to protect user privacy while still allowing the use of data for security purposes, by imposing strict rules on data processing and sharing, to ensure that privacy is not compromised in the name of security. Companies regulated by the GDPR must have legal grounds to process personal data and must protect it accordingly.

Box 2. Cybersecurity and the collective defence of NATO

Recognizing that cybersecurity now sits alongside traditional military challenges, NATO has acknowledged that cyber threats can disrupt and damage societies just as significantly as conventional military attacks. This positions cybersecurity not just as an IT issue but as a strategic concern that is central to national and collective defence. In 2014, at the NATO Summit in Wales, cyber defence was first declared an integral part of collective defence, as member states conceded that a cyberattack could threaten national and Euro-Atlantic prosperity, security, and stability, and could subsequently lead to the invocation of Article 5 of the North Atlantic Treaty.¹⁵ This was a pivotal moment and marked a new understanding of the potential severity and consequences of cyberattacks in the context of collective defence.¹⁶

Two years later, at the Warsaw Summit held in 2016, NATO formally recognized cyberspace as a domain of operations alongside land, air, and sea, and defined cyber defence as among NATO's core tasks of deterrence and defence.¹⁷ Since then, the 2016 NATO Cyber Defence Pledge,¹⁸ the launch of the Defence Innovation Accelerator of the North Atlantic (DIANA),¹⁹ the 2021 Comprehensive Cyber Defence Policy,²⁰ and the 2022 NATO Strategic Concept²¹ have all illustrated a strengthening commitment to national cyber defences on the part of NATO member states, which share similar views on the gravity and urgency of cyber threats.

¹⁵ The Wales Summit Declaration, paras 72 and 73. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

¹⁶ NATO has not yet defined the threshold that could trigger Article 5. The view of many experts is that a cyberattack must result in a major loss of life, equivalent to traditional military action, in order to trigger an Article 5 response. Identifying who is responsible for cyberattacks also makes retaliation difficult. NATO Secretary General Jens Stoltenberg spoke about this in a press conference, available online at: <https://www.c-span.org/video/?c5003322/nato-chief-cyberattacks-trigger-article-5>

¹⁷ The Wales Summit Declaration, paras 70 and 71. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber

¹⁸ The Pledge states in its first para: 'we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea'. NATO Press Release, 8 July 2016. The text of the Pledge is available at: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

¹⁹ The Defence Innovation Accelerator for the North Atlantic (DIANA) is an organisation established by NATO to find and accelerate dual-use innovation capacity across the Alliance. It provides companies with the resources, networks and guidance to develop deep technologies to solve critical defence and security challenges. See DIANA's online page at: <https://www.diana.nato.int/>

²⁰ https://www.nato.int/cps/en/natohq/topics_78170.htm#governance

²¹ In paragraph 24, the Concept reads, 'We will expedite our digital transformation, adapt the NATO Command Structure for the information age and enhance our cyber defences, networks and infrastructure'. See: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO works to **enhance the cyber defence capabilities** of its member states by sharing best practices, intelligence, and technology. It also hosts cyber defence exercises at the **NATO Cooperative Cyber Defence Centre of Excellence** in Tallinn, Estonia, a multinational and interdisciplinary cyber defence hub, think tank, and training facility that organizes the annual Locked Shields exercise. This is the largest and most complex live-fire cyber defence exercise in the world and involves teams from NATO member states, which practice protecting national IT systems and critical infrastructure against cyberattacks.

The role of NATO in cybersecurity is geared towards **prevention, resilience, and support**, offering a platform for political consultation, mutual assistance, and collective action in the event of significant cyber incidents, including by providing rapid response teams. At the 2023 NATO Summit in Vilnius, for instance, the Virtual Cyber Incident Support Capability (VCISC) was launched to support national mitigation efforts in response to significant malicious cyber activities. Involvement of this sort by NATO in cybersecurity underscores its adaptation to new challenges and the importance of international cooperation in the digital age.

2. Defining the cybersecurity realm

It is difficult to define cybersecurity, for two main reasons. First, because technological advancements occur so quickly; and second, because it encompasses interconnected concepts that collectively shape and are shaped by our shared understanding of the digital landscape. This means that what cybersecurity is, and how it functions, are both ever evolving.

Therefore, practically speaking, the nature and needs of cybersecurity inevitably outpace the speed at which policymakers can frame and enact relevant regulations. New vulnerabilities can emerge overnight, making yesterday's security measures potentially obsolete today. And new paradigms – from the Internet of Things (IoT), to artificial intelligence (AI), to quantum computing – introduce novel dimensions to the cybersecurity landscape. Consequently, the norm in cybersecurity is a state of constant flux, in dialogue with and in response to emerging technologies and challenges.

Often, cybersecurity is used as an umbrella term to describe various digital mechanisms used to protect critical infrastructure, counter disinformation, and ensure personal data protection. Yet, formulating effective and actionable policies and laws demands a foundational understanding of both the broad scope and finer intricacies of what constitutes the cybersecurity domain. This means delineating where cybersecurity begins and ends.

Cybersecurity is, in the simplest terms, the protection of digital assets from theft, damage, or unauthorized access, with the goal of ensuring the confidentiality, integrity, and availability of

computer systems, networks, and data. Cyber threats may emanate from hackers, state actors, and cybercriminals, or from inside organizations and enterprises, and can range from viruses and malware to sophisticated cyber espionage and cyber warfare attacks. Cybersecurity thus encompasses measures like firewalls, intrusion detection systems, malware protection, encryption, and more.

Critical Infrastructure Protection (CIP) refers to the protection of assets that are essential to the functioning of a society and its economy, such as power plants, transportation systems, water supplies, financial services, telecommunications networks, emergency services, and more. A cybersecurity breach targeting critical infrastructure could have catastrophic consequences, leading to physical damage, economic disruption, or even loss of life. Hence, cybersecurity is crucial to safeguarding these vital systems. Importantly, though, while CIP includes cybersecurity, it also encompasses physical security measures. For example, protecting a power grid involves both defence of its computer systems and measures to ensure that physical assets like transformers and power lines are secure from threats such as terrorism, natural disaster, or theft.

Protecting personal data safeguards the privacy rights of individuals by ensuring that their personal data is collected, stored, and processed securely and responsibly. Breaches in cybersecurity can lead to the unauthorized access, theft, or release of sensitive personal data, whereas robust cybersecurity practices can ensure the protection of this data, which is increasingly stored and processed online. Similar to CIP, however, the protection of personal data extends beyond cybersecurity to non-cyber measures aimed at securing all digital assets. This may include physical data storage protection or procedural safeguards.

Disinformation is false or misleading material created with the intent to deceive, sow discord, or manipulate public opinion. In disinformation attacks, this material is deliberately spread, often through social media platforms and other online channels, so that deceptive narratives rapidly enter the mainstream. The tools and tactics of cyberattacks can be used to disseminate disinformation, such as through hacking and leaking, or by using bots to amplify false messages. Cyberattacks can also be deployed to steal information that is then distorted and shared as disinformation. Thus, knowledge of how information travels in cyberspace and how it can be manipulated is key to developing a comprehensive cybersecurity strategy, and to formulating cybersecurity measures that help detect and counter disinformation. That said, disinformation exists outside the digital realm as well, and it is important to understand that it can be instrumentalized without a cybersecurity breach.

The growing issue of disinformation and ‘fake news’²² intersects directly with the core responsibilities of parliamentarians, to protect democratic processes, ensure national security, and uphold public trust. It is therefore natural that parliamentarians would show significant interest in disinformation as it relates to the broader theme of cybersecurity. Still, despite some overlap, it is crucial to maintain a distinction between these two phenomena. Cybersecurity measures such as stronger firewalls or encrypted communication may not address the challenge of disinformation; and conversely, fact-checking or media literacy campaigns aimed at combating disinformation may not enhance the security of digital systems.

Box 3. Cybersecurity and disinformation in the European Union (EU)

In digital environments, security implies not only protection against cyberattacks but also the assurance that information ecosystems are not polluted by disinformation. To that end, **the EU treats cybersecurity and disinformation as interconnected but distinct challenges**, recognizing them both as significant threats to the integrity of the digital single market, the security of EU member states, and democratic processes. There is significant interplay between cybersecurity and disinformation, especially given the role of cyber tools in propagating disinformation. When cyberattacks are used to obtain and leak information that is manipulated as disinformation, or cyber tools like bots are deployed to amplify disinformation, this can severely undermine public trust in digital security measures and institutions, making societies even more vulnerable to cyber threats.

Recognizing its widespread and harmful influence on democratic processes and social cohesion, the EU has worked to actively tackle disinformation, especially since 2015. By introducing regulatory measures, encouraging self-regulation, supporting research, and empowering citizens with knowledge, the EU seeks to build a holistic defence against disinformation. This includes engagement with social media companies and online platforms to ensure they detect, analyse, and expose disinformation campaigns, limit their spread, and counteract false narratives by providing facts and critical analysis.

Among the measures introduced since 2015, the following should be highlighted:

- In 2018, the EU developed an Action Plan against disinformation²³ and began collaborating with online platforms, advertisers, and the media to ensure the integrity of information

²² Fake news is a colloquial term for disinformation. Experts favour the term ‘disinformation’, however, arguing that ‘fake news’ is narrower and ‘has been appropriated and used misleadingly by powerful actors to dismiss coverage that is simply found disagreeable’. See European Commission, ‘A Multidimensional Approach to Disinformation - Report of the Independent High level Group on fake news and online disinformation’, 2018, p. 10–11. Available at: <https://www.ecsite.eu/sites/default/files/amulti-dimensionalapproachtodisinformation-reportoftheindependenthighlevelgrouponfakenewsandonlinedisinformation.pdf>

²³ European Union, ‘Action Plan against Disinformation’, 2018, available at: https://www.eeas.europa.eu/node/54866_en

and to address the spread of fake news online through the **Code of Practice on Disinformation**.²⁴

- In 2015, the European External Action Service (EEAS) established a **Strategic Communications Division** to lead its work on disinformation, analyse the information environment, and develop targeted approaches to communicating with audiences in geographic priority regions, mostly in the EU's neighbourhood.²⁵
- In 2018, the European Commission formed a High-Level Expert Group to more precisely clarify and diagnosis the problem of disinformation, which it labelled **Foreign Information Manipulation and Interference (FIMI)**.²⁶ This brings the focus to external actors, particularly state actors, engaged in information warfare or influence operations to affect European decisions, public opinion, or electoral and political processes. Such activity is manipulative, and is conducted in a way that is intentional and coordinated.²⁷
- Three Strategic Communications Task Forces were created to help respond to FIMI activity in the Eastern Partnership, the Southern Neighbourhood, and the Western Balkans.
- In 2015, **EUvsDisinfo**, the flagship project of the East StratCom Task Force, was launched to better forecast, address, and respond to disinformation campaigns of the Russian Federation that affect the EU, its members, and countries in its neighbourhood.²⁸ Using data analysis and media monitoring services in 15 languages, EUvsDisinfo identifies, compiles, and exposes disinformation originating in pro-Kremlin media. Each case (and a disproof) is collected in the EUvsDisinfo database, the only searchable, open-source repository of its kind, which currently includes over 15,000 entries.

The goals and challenges of cybersecurity listed above – CIP, disinformation, and personal data protection – are operationalized and countered through a wide array of actions, mechanisms, and practices that constitute **the cybersecurity domain**. The concepts summarized below represent only some facets of this domain, and while each stands alone, they are also intertwined, with developments in one area often impacting others. This is part of why holistic approaches and cross-discipline collaboration are such an imperative in cybersecurity.

- ◇ **Incident Response:** The approach and processes used by an organization to detect, respond to, and recover from a cybersecurity incident.
- ◇ **Network Security:** Protection of computer network infrastructure against unauthorized intrusion, data exfiltration, and denial-of-service attacks.

²⁴ The 2022 EU updated Code of Practice on Disinformation is available at: <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>

²⁵ See the Countering Disinformation page on official website of the European Union, updated on 12 October 2021, at: https://www.eeas.europa.eu/countering-disinformation/tackling-disinformation-information-work-eeas-strategic-communication_en

²⁶ For more information see the dedicated page on the official website of the EU, updated on 27 Mai 2024, at: https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en

²⁷ Ibidem.

²⁸ See the official page of EUvsDisinfo at: <https://euvsdisinfo.eu/about/>

- ◇ Endpoint Security: Protection of endpoints or endpoint devices like computers, smart-phones, and tablets against potential cyberattack.
- ◇ Cloud Security: Safeguarding cloud-based data, applications, and infrastructure from cyber threats.
- ◇ IoT (Internet of Things) Security: Protection of network-connected devices and systems, ranging from smart thermostats in residential homes to industrial machinery.
- ◇ Digital Identity and Access Management: Ensuring that certain digital resources can be accessed only by authorized individuals, and managing digital identities.
- ◇ Threat Intelligence: Gathering and analysing information about potential threats, to predict or detect future or ongoing cyberattacks.
- ◇ Application Security: Safeguarding software applications against various types of attacks by identifying and fixing vulnerabilities.
- ◇ Information Assurance: Ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of information and services.
- ◇ Supply Chain Security: Protecting supply chain processes, hardware, and software against cyber threats.
- ◇ Cryptography: Using codes to encrypt data, rendering it unreadable unless it is in the possession of someone who has the key to decrypt it.
- ◇ Phishing and Social Engineering: Methods used by attackers to deceive individuals into divulging sensitive information or performing specific actions that compromise security.
- ◇ Digital Forensics: The collection and analysis of electronic data, usually ex post facto, to gather evidence and understand the scope and impact of a cyber incident.
- ◇ Cyber Warfare and Cyber Espionage: State-sponsored cyber activities aimed at gathering intelligence on, causing harm to, or gaining a strategic advantage over other nations.
- ◇ Malware Analysis: Investigating the functionality, origin, and potential impact of malicious software.
- ◇ Vulnerability Management: The process of identifying, assessing, treating, and reporting security vulnerabilities in systems.
- ◇ Zero Trust Architecture: A security concept that advises organizations should not trust any entity, outside or inside their perimeter, by default.

Parliamentary debates on policy and law must start by delineating where the challenges of cybersecurity end and where the issues of information integrity, media literacy, and disinformation begin. These phenomena are all salient in the digital age, but require different tools, strategies, and expertise to address effectively, and can be best managed by different actors.

3. Writing comprehensive cybersecurity legislation

It is essential that laws are crafted to adequately address all aspects and actors in the cybersecurity domain, establish clear standards, outline specific responsibilities, and prescribe penalties.

Such legislation sets expectations for cybersecurity and helps foster a society-wide culture of cybersecurity awareness. But the complexity of cybersecurity phenomena means that legislation regulating the field is often fragmented and spread across multiple domains, including technology, national security and defence, law enforcement, intelligence, data protection, and private industry. This makes it difficult to assess how various legal provisions interact, and complicates the job of legislators to clearly define different areas of regulation, understand their interconnectedness, and anticipate how changes in one area might impact others. Yet, a holistic and integrated approach is considered a prerequisite to creating robust, effective, and adaptable cybersecurity frameworks.

This includes **laws regulating the functioning of state security agencies**, which often contain provisions relevant to cybersecurity, commonly centred on the protection of critical infrastructure, sensitive government data, and digital assets. In some cases, there is no clear separation between cybersecurity and broader national defence and security issues, as cybersecurity is one element of the larger construct of national defence. Regulations pertaining to cybersecurity may also be incorporated into existing defence and security laws. This can create ambiguities in the implementation of cybersecurity measures, for instance if a law provides for the defence of critical infrastructure without explicitly stating whether this includes digital assets, leaving room for interpretation. Further, the legal mandates of security and defence agencies may overlap in the area of cybersecurity, making it difficult to delineate their specific responsibilities.

Laws regulating non-governmental entities and their cybersecurity activities are also important and are often sector specific. For example, antitrust laws may relate to cybersecurity by focusing on the competitive aspects of technology markets, consumer protection laws may focus on data privacy and identity theft prevention, and infrastructure protection laws may govern how utilities and other critical infrastructure entities secure their networks against cyber threats. The actions of and interactions between private actors have a considerable impact on the development of cybersecurity norms, and thus on the overall cybersecurity ecosystem. These actors have custody of vast amounts of sensitive data and control over extensive networks and systems, the security of which is integral to national security. Their actions, or lack thereof, can significantly influence a country's cybersecurity posture, including its resilience against cyberattacks and its overall cybersecurity culture. For these reasons, in many countries, collaborative approaches to cybersecurity have been adopted, with policies and regulations shaped through consultations with industry experts, many from the private sector.

Practices and guidelines established by private actors can have far-reaching effects, even if they are not legally binding. Corporate bylaws can set internal cybersecurity standards that exceed public regulations, for instance, and can thereby push the entire industry to adopt these higher standards in order to remain competitive. In some cases, this can even set a global precedent, transcending national boundaries and providing a blueprint for international cybersecurity norms.

Industry leaders thus have quite a bit of power to establish de facto standards, which smaller companies may adopt voluntarily or through market pressure. For example, if a major tech company requires multi-factor authentication, smaller companies may follow suit to maintain consumer trust. Groups of companies within a specific industry can also establish collective cybersecurity standards, such as the Payment Card Industry Data Security Standard (PCI DSS), an information security standard for organizations that handle branded credit cards from the major card schemes, created by major credit card companies.²⁹ When private organizations act as certification bodies to assess and certify the cybersecurity measures of other organizations, they set norms as well, while increasing transparency.

Working together, private companies and public agencies can create guidelines that, though not legally enforceable, provide a roadmap for best practices in cybersecurity. Companies may then opt to follow these, at least to avoid future litigation or regulatory scrutiny. At the same time, corporate interest groups and lobbying organizations can actively shape legislation and standards by advocating for the interests of businesses within the cybersecurity domain.

Box 4. Estonia's e-Revolution

Estonia has integrated digital technologies into public services, governance, and daily life to such a degree that it is now among the world's most advanced digital societies. This transformation began shortly after the country declared independence, with government-backed investments allowing all schools to connect to the internet by the late 1990s and facilitating the introduction of computer programming curricula to students as young as seven.³⁰ Estonia has established a digital government in which most state functions are accessible online, and it became the first country in the world to introduce online voting for parliamentary elections, in 2005.

Still, the country's dependence on the internet made it one of the first to come under attack in the era of hybrid warfare.³¹ In 2007, when the 'Bronze Soldier' monument (which most Estonians saw as a symbol of Russian oppression) was removed from the centre of Tallinn, protest erupted in Russian media and among Russian speakers. Two nights of riots and looting were followed by a massive cyberattack that stretched over three weeks. Government and parliamentary portals, media outlets, banks, and small businesses were all taken down by a combination of malware attacks and DDoS.³²

²⁹ See more on their website, available at: https://www.pcisecuritystandards.org/about_us/

³⁰ Tim Mansel, 'How Estonia became E-stonia', BBC news, 16 May 2013. Available at: [How Estonia became E-stonia - BBC News](#)

³¹ Hybrid warfare blends conventional warfare, irregular warfare, and cyber warfare with other tools of malign influence, including disinformation, diplomacy, and foreign electoral intervention. The aim is to disrupt, disable, or defeat an opponent without necessarily resorting to open hostilities or full-blown war. Disinformation campaigns can be part of broader information warfare or influence operations conducted by state or non-state actors.

³² Distributed denial-of-service (DDoS) attacks are malicious attempts to disrupt the normal traffic of a targeted server, service, or network

Most of the malicious network traffic was of Russian-language origin, and though the Russian government denied any involvement, the attacks were accompanied by hostile political rhetoric on the part of Russian officials towards Estonia. Moreover, they were followed by Russia's implementation of hostile economic measures and a refusal to cooperate with the Estonian investigation into the attacks.³³ The crisis exposed Estonia's cyber vulnerabilities and demonstrated the potential of cyberattacks to cause significant damage to a country. In response, Estonia initiated major reforms to bolster its cyber defenses and cyber resilience. These included:

the development of a comprehensive national cybersecurity strategy, including measures to protect critical infrastructure and ensure the security of citizens' personal data security;

- ◇ the creation of a Cyber Defence Unit in the Ministry of Defence, responsible for handling attacks on major utility or vital service providers, and comprising an anonymous team of IT professionals who volunteer their expertise and are trained by the Ministry after security vetting;
- ◇ the adoption of legislation to better tackle cybercrimes, making activities like distributed denial-of-service (DDoS) attacks clearly criminalized and punishable;
- ◇ strong advocacy for international cooperation in cyber defence and the establishment of partnerships with other countries, as well as involvement in various international fora, to discuss norms and best practices in cyberspace (in 2008, Estonia became home to NATO's CCDCOE, which conducts research and training on cyber defence);
- ◇ collaboration between the private sector and the government to ensure cybersecurity, resulting in the development of cooperation frameworks to facilitate the sharing of best practices, expertise, and resources; and
- ◇ increased initiatives to raise cybersecurity awareness among the public and to train professionals in this field, including through regular cyber defence exercises.³⁴

By swiftly implementing these measures, Estonia fortified its cyber defences and positioned itself as a leader in cybersecurity, ranking third in the 2021 Global Cybersecurity Index (GCI), following only the United States, and UK and Saudi Arabia (tied for second).³⁵ It is the National Defence

by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks utilize multiple compromised computer systems as sources of attack, making a DDoS attack like an unexpected traffic jam clogging up a highway, preventing regular traffic from arriving at its destination. DDoS attacks are a primary concern in cybersecurity today.

³³ The so-called Bronze Soldier attacks are the first suspected state-backed cyberattacks on another nation. For more on this see NATO Strategic Centre of Excellence Riga, 'Hybrid Threats: 2007 cyber-attacks on Estonia', 6 June 2019. Available at: [StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia \(stratcomcoe.org\)](https://stratcomcoe.org/)

³⁴ Jakub Warzecha, 'Lessons from Estonia: How to Become Cyber-proof', 3 SEAS Europe, 18 June 2019. Available at: <https://3seaseurope.com/cybersecurity-estonia-cyberproof/#:~:text=International%20Cooperation%3A%20Estonia%20has%20established,in%20the%20field%20of%20cybersecurity>

³⁵ Global Cybersecurity Index 2020, ITU. Available at: <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E>. It is worth noting that there are several such lists, made by different expert groups and using different ranking criteria. While the countries appearing among the top 10 in each list vary, the United States almost always sits in the top spot. For example, see 'National Cyberpower Index 2022', available at: <https://www.secureworld.io/industry-news/top-10-most-powerful-countries-in-cyberspace>

Committee of the Estonian Parliament that is responsible for reviewing legislation and exercising oversight in cybersecurity.

4. Harmonizing national laws with international norms

Because cyberspace lacks physical boundaries, actions in this domain often have transnational implications, making international cooperation essential. Parliamentarians must therefore consider how national laws align with international norms, principles, and guidelines, which have evolved rapidly.³⁶ These norms provide a blueprint for national actors to follow and can help ensure the harmonization of national and international laws.

While there is no single, comprehensive treaty defining and regulating cybersecurity, it is widely accepted that existing international law, including International Humanitarian Law (IHL) and Human Rights (HR) law, applies in cyberspace. Additionally, various international legal frameworks address specific aspects of cybersecurity and establish parameters for robust cybersecurity at the national level. Some of these, which may be valuable and even inspirational to national legislators, are discussed below.

The UN framework for responsible state behaviour in cyberspace is an initiative aimed at promoting peace, security, and stability in the digital realm.³⁷ The framework contains **11 Norms of Responsible State Behaviour**, which guide states in what they should and should not do vis-à-vis cybersecurity.³⁸ Developed by the United Nations Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace,³⁹ and later endorsed by all UN Member States, these non-binding norms outline expected standards of state conduct such as avoiding harmful activities, protecting critical infrastructure, and cooperating to address cyber incidents, among others. The 11 Norms serve as one pillar of the UN framework for responsible state behaviour in cyberspace, along with three others: binding international law, confidence building measures, and capacity building.

The UN framework:

- emphasizes that existing international law, including the UN Charter, International Humanitarian Law (IHL), and Human Rights (HR) law, applies to state behaviour in cyberspace, and provides a legal basis for state actions and interactions in the digital domain by integrating cyberspace into the broader framework of international legal norms;

³⁶ For a comprehensive review of different types of norms that regulate state behaviour in cyberspace, see: Anna-Maria Osula and Henry Rõigas, eds., 'International Cyber Norms: Legal, Policy & Industry Perspectives', NATO CCD COE Publications, Tallinn 2016, available online at: https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf

³⁷ UNIDIR, Background to UN Discussions on Responsible State Behaviour, available at: <https://nationalcybersurvey.cyberpolicyportal.org/background-to-un-discussions-on-responsible-state-behaviour/>

³⁸ The UN Norms are available online at: <https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf>

³⁹ United Nations Groups of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security was gathered under the auspices of the UN Disarmament Committee in 2004-2005. For more on the GGE see: <https://disarmament.unoda.org/group-of-governmental-experts/>

- encourages states to implement confidence-building measures, particularly to strengthen transparency, predictability, and stability – such as information sharing, the establishment of communication channels, and the development of mutual understanding when it comes to cybersecurity practices and policies – as a means of reducing the risk of misunderstandings and conflicts in cyberspace; and
- advocates for enhancing the cybersecurity capabilities of states, especially those with less developed cyber infrastructures, including through technical training, the sharing of best practices, and the provision of resources to build robust cybersecurity defences and response mechanisms.

The framework constitutes an internationally recognized set of standards and expectations for state conduct in the digital domain, and promotes consistency and predictability in cyberspace when adopted and implemented by states. By ensuring that principles governing inter-state relations in the physical world continue to hold relevance in the digital world, it contributes to a collective understanding that fosters consensus around cyber issues.

The Tallinn Manual is not a legal instrument per se, but it provides a comprehensive academic analysis of how existing international law can be applied to cybercrimes, particularly to operations that qualify legally as a ‘use of force’ or ‘armed attack’ or which take place in the context of an armed conflict.⁴⁰ The Manual, developed by a group of international law experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, announced NATO’s commitment to the vital role of promoting a rules-based international order in cyberspace. Some important norms it sets relate to the applicability of international law to cyberspace and the extension of the collective defence principle (Article 5) to cyberattacks (for more on NATO and cybersecurity see Box 2).

Regional organizations have also worked to define the rules and boundaries that regulate the behaviour of states in cyberspace, with the goal of further harmonizing norms and standards in this area. In Europe, both the Council of Europe and the EU have developed a number of legal mechanisms in this field that have already served as useful models for governments elsewhere. For example, the EU’s GDPR has become something of a gold standard for data privacy protection laws in other countries.

The Budapest Convention (the Council of Europe Convention on Cybercrime), adopted in 2004, was the first international treaty on cybercrime.⁴¹ It requires member states to enact legislation

⁴⁰ Version 1.0 of the Tallinn Manual was published in 2013. It deals primarily with questions like when a cyber operation can be classified as an act of war and how international humanitarian law regulates cyber warfare. Version 2.0, published in 2017, expanded the scope of the original, also discussing less severe cyber operations that occur outside the context of armed conflict. It delves into topics such as state sovereignty, state responsibility, human rights, and international telecommunications law in the context of cyber activities. For more, see: <https://ccdcoc.org/research/tallinn-manual/>

⁴¹ The Convention has been in force since 2004. It is available at: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>. For more on state’s benefits in joining the convention see the COE Factsheet, April 2023, available at: <https://rm.coe.int/cyber-buda-benefits-19april2023-en/1680aafa3d>

that criminalizes certain cyber activities (from illegal access and systems interference to computer-related fraud and child pornography), and provides guideline on improving investigative techniques and fostering international cooperation in cybercrime investigations. Any country may use the text of the Convention as a model or tool, and the treaty is open for accession even by non-member states. The role of the EU in setting a normative framework for cybersecurity has also been pivotal. It has established standards and policies to guide member states, but has had a broader influence on global cybersecurity practices as other countries have sought to replicate its comprehensive approach to cybersecurity. This approach is aimed at creating a secure digital environment, fostering trust and confidence in digital services, and ensuring the protection of data and infrastructure across the single market, and has set a benchmark for cybersecurity and data protection worldwide.

The **Directive on Security of Network and Information Systems (NIS Directive)** was the first piece of EU-wide legislation on cybersecurity. Adopted in 2016 and requiring member states to ensure the implementation of adequate security measures, the Directive also made it mandatory for serious cyber incidents to be reported by operators of essential services in critical sectors such as energy, transport, banking, and healthcare, as well as digital providers like cloud computing services. In response to the evolving and increasingly sophisticated cyber threat landscape, the EU updated and strengthened this framework in 2022, adopting the NIS2 Directive six years after the NIS Directive first entered into force.

The updated **NIS2 Directive** addressed shortcomings of the original by:

- ◇ **Expanding the scope:** The NIS2 Directive covers more sectors and types of entities, including all entities of a certain size and/or belonging to certain sectors, including energy, transport, banking, healthcare, digital infrastructure, public administration, space, waste management, chemicals, and food, among others.
- ◇ **Establishing stricter security requirements:** NIS2 sets out stricter security measures and requirements for entities, emphasizing risk management and the need to address cybersecurity risks proactively.
- ◇ **Incorporating more stringent mandatory reporting requirements:** NIS2 reduces the timeframe for reporting and requires that entities are even more transparent about significant cyber incidents.
- ◇ **Increasing fines for non-compliance:** NIS2 includes provisions through which significant fines can be imposed to ensure compliance, bringing it into alignment with the enforcement mechanism seen in the GDPR, with the aim to incentivize entities to prioritize cybersecurity and protect the EU's digital economy.
- ◇ **Enhancing enforcement and supervision:** NIS2 introduces more robust and harmonized enforcement and supervisory measures across member states, to ensure that national authorities have the necessary powers to effectively oversee the cybersecurity practices of entities within their jurisdiction.

- ◇ **Improving information sharing:** NIS2 encourages more information sharing about cyber risks and incidents between companies and with relevant authorities, to foster a culture of security and resilience.⁴²

The NIS2 Directive is a testament to the commitment of the EU to strengthening its cybersecurity framework to keep pace with the changing cyber threat landscape. It recognizes and underscores the need for a collective effort to protect the digital single market and the privacy and data of individuals within the EU.

The 2018 **General Data Protection Regulation (GDPR)** complements the Directive by enforcing strict security measures that protect personal data against cyber threats. And the **EU Cybersecurity Act**, adopted in 2019, has established a European cybersecurity certification framework for information and communications technology (ICT) products, services, and processes, while strengthening the role of the **EU Agency for Cybersecurity (ENISA)** in preventing and responding to cyber threats and attacks.⁴³ ENISA now has a permanent mandate and is charged with managing the EU's certification framework.

The recently adopted **Cyber Resilience Act (CRA)**, which passed the European Parliament in March 2024, is the first ever EU-wide legislation to introduce mandatory cybersecurity requirements for manufacturers and developers of products with digital elements, covering both hardware and software and extending throughout the product lifecycle.⁴⁴ The CRA will harmonize the EU regulatory landscape, replacing overlapping requirements that stem from different pieces of legislation and creating greater legal certainty for operators and users across the Union. Importantly, the Act will also complement and facilitate compliance with the NIS2 Directive.

Box 5. Obligations of states, deriving from the NIS2 Directive

The NIS2 Directive imposes some obligations on countries aimed at improving their cybersecurity capabilities. These include:

The development of a national cybersecurity strategy: Member states must develop and implement a national strategy on the security of network and information systems, which

⁴² The text of the Directive, as well as Guidelines for its application, are available at: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

⁴³ European Commission, News Article, 'The Cybersecurity Act strengthens Europe's cybersecurity' 19 March 2019. Available at: <https://digital-strategy.ec.europa.eu/en/news/cybersecurity-act-strengthens-europes-cybersecurity> (NB: ENISA was established in 2004 and is dedicated to achieving a high common level of cybersecurity across Europe. It is mandated to encourage operational cooperation with member states that request assistance in handling cyber security incidents and cross-border cyberattacks, and functions as the secretariat of the national Computer Security Incidents Response Teams (CSIRTs) Network. See: <https://www.enisa.europa.eu/about-enisa>).

⁴⁴ Businesses will soon have to comply with only one single set of cybersecurity rules across the EU. Text available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html

should outline the objectives and measures to ensure a high level of cybersecurity.

The designation of national competent authorities and CSIRTs: Countries are required to designate one or more national competent authorities responsible for monitoring the application of the Directive, and must also establish Computer Security Incident Response Teams (CSIRTs) to handle incidents and defend against cyber risks at the national level.

The adoption of risk management and incident reporting measures: Essential service operators and digital service providers are required to adopt appropriate and proportionate technical and organizational measures to manage risks to their network and information systems, and must also report any significant incidents to the relevant national authority.

Cooperation among member states: A mandated Cooperation Group composed of representatives from member states, the European Commission, and ENISA is meant to facilitate strategic cooperation and the exchange of information and best practices.

Cross-border collaboration: Member states must work together to manage and respond to cybersecurity incidents that have cross-border impacts, by sharing information and coordinating their responses to ensure a unified approach to the handling of cyber threats.

Supervision and enforcement: National authorities must supervise implementation of the Directive and are empowered to enforce compliance, including by imposing penalties for non-compliance.

The Directive also stipulates some **sector-specific obligations** in sectors such as energy, transport, banking, financial market infrastructures, health, water supply, and digital infrastructure. Identified as critical, operators in these sectors have specific obligations to ensure the security and continuity of their services.

Other regional initiatives that should be mentioned include: the OSCE's Confidence-Building Measures (CBMs), focused on reducing the conflict risks associated with the use of ICT;⁴⁵ the Agreement among Governments of Shanghai Cooperation Organization Member States on Cooperation in the Field of Ensuring International Information Security, which frames the spread of content via the internet as a potential security threat and proposes means to regulate it;⁴⁶ and the ASEAN Cybersecurity Cooperation Strategy, the latest version of which (2021–2025) calls for the establishment of a regional CERT.⁴⁷

⁴⁵ CCDCOE, 'OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection', available at: <https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/>

⁴⁶ CCDCOE, Shanghai Cooperation Organisation, available at: <https://ccdcoe.org/organisations/sco/>

⁴⁷ The ASEAN Cybersecurity Strategy is available at: <https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation->

These global and regional instruments lay a normative foundation for state behaviour in cybersecurity, and various **bilateral agreements** add to this normative framework. These agreements address everything from cooperation in cybercrime investigations, to information sharing, to capacity- and confidence-building measures. For example, the U.S. and China agreed in 2015 that neither nation would ‘conduct or knowingly support cyber-enabled theft of intellectual property’ for economic advantages.⁴⁸

5. Identifying good practice in cybersecurity oversight

Developing and periodically updating comprehensive cybersecurity legislation is only the starting point of parliamentary engagement with cybersecurity. The role of parliaments in cybersecurity is multifaceted, extending beyond legislation to **budgetary and oversight functions** that ensure laws and policies are effectively implemented, and are observed. This requires regular updates and reports from government agencies, the enforcement of cybersecurity regulations, and, where necessary, the will to take corrective actions against entities that fail to comply with cybersecurity standards. How parliaments can effectively oversee cybersecurity is explored below, using some examples of best practice.

Investing in cybersecurity expertise within parliament

Parliamentary oversight of cybersecurity poses unique challenges due to its technical complexity and evolving nature. The technicality of the field can be a particular barrier to people who are not experts themselves, and the speed of change in ICT environments can be intimidating to industry outsiders. Indeed, most parliamentarians do not possess specialized technical knowledge of cybersecurity and digital systems and are tasked with legislating and overseeing matters they do not fully understand.

However, this should not be an obstacle to effective engagement, especially because some strategies for improving cybersecurity are not technical at all. For instance, parliamentarians may concentrate on legal and governance aspects of cybersecurity that do not necessarily require in-depth technical knowledge, reviewing whether competent authorities and national computer emergency response teams (nCERTs) have been established as proposed, critical information infrastructure (CII) has been recognized, incident report systems established, and information-sharing mechanisms in place. These are questions that can be answered without technical expertise or knowledge. That said, parliamentarians bring a diverse range of expertise to the

[Paper-2021-2025_final-23-0122.pdf](#)

⁴⁸ The White House, Office of the Press Secretary, ‘Remarks by President Obama and President Xi of the People’s Republic of China in Joint Press Conference’, 25 September 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>

table, and often invest substantial time and effort to expand their knowledge base, attending briefings, participating in workshops, and consulting with external experts. They can draw upon previous experience with legal, ethical, economic, geopolitical, and social issues to deepen their understanding of the cyber landscape and its many complexities and intersections, and may see the potential for interdisciplinary approaches that can help bridge technical knowledge gaps. Expertise tends to be concentrated in the working bodies of a parliament, particularly the standing committees, which accumulate considerable knowledge in their area of competency. This is a product not only of their continued focus on an area but also the support of expert staff who provide research, analysis, and advice. The dynamic combination of structured committee support and individual member initiative can create an environment in which both robust scrutiny and informed decision-making are central to the legislative process.

It is unusual for parliaments to have a single dedicated standing committee for cybersecurity. Thus, cybersecurity is typically addressed through committees that oversee related areas, including defence and security, intelligence, technology, industry, digital affairs (i.e., the security of critical infrastructure and business sectors), human rights, and judiciary or constitutional affairs (e.g., on questions related to the protection of personal data and the legal framework for cybercrime). This mirrors the way in which responsibility for cybersecurity is fragmented at the government level, across multiple agencies or departments. While having more than one committee engaged in some aspect of cybersecurity allows for its integration into broader discussions of national importance, this fragmentation can pose a challenge in understanding the overall regulatory landscape and can lead between relevant committees is an ongoing imperative.

The interdisciplinary nature of cybersecurity demands expertise that spans law, technology, international relations, military strategy, and more. If parliaments face resource constraints, including budgetary limitations and a shortage of specialized staff, their ability to effectively tackle cybersecurity challenges can be hindered. However, Box 6 (below) details several strategies for developing expertise within parliaments, to mitigate these constraints. to potential gaps and inconsistencies in oversight.

Box 6. Cybersecurity expertise within parliaments can be developed by...

1. **Establishing a dedicated committee on cybersecurity:** Although these are uncommon, a dedicated parliamentary committee on cybersecurity could bring more focus to the issue, while facilitating expert consultation and enabling swifter legislative responses to emerging threats. Even absent this, different committees that cover various aspects of cybersecurity

should regularly exchange information and hold joint meetings. Moreover, cybersecurity experts should be employed within the parliamentary structure, or expert staff should be seconded temporarily from government agencies, to advise committees on how to monitor, assess, and supervise the functioning of cybersecurity systems.

2. **Ongoing training for members and staff:** To improve the effectiveness of cybersecurity oversight, it is crucial that specialized training is provided to committee members and staff.
3. This should focus on both the technical aspects of cybersecurity and its broader implications and should be updated frequently to reflect the changing cyber landscape. Parliamentary research services should also be strengthened and should be enabled to provide in-depth analyses on cybersecurity matters.
4. **Keeping up to date and collaborating internationally:** It is essential that parliaments stay informed on the latest evolutions and innovations in cybersecurity and maintain active collaborations with international bodies and forums. This helps parliaments align their strategies with global standards and effectively manage the international aspects of cyber threats. Participation in international forums, workshops, and conferences can also provide a broader view of global cybersecurity trends and best practices.
5. **Engaging in multistakeholder exchange:** Given the centrality of public-private partnerships to effective cybersecurity, it is important that parliamentarians both participate in and foster dialogue on cybersecurity, and involve diverse experts and stakeholders. This can provide parliaments with additional expertise and perspectives that are necessary to carry out comprehensive oversight. By establishing partnerships and by holding regular consultations and public hearings with national cybersecurity agencies, industry representatives, academic institutions, and research organizations, parliamentary members and staff can gain a more complete view of the field.
6. **Simulating scenarios:** Conducting mock cyberattack exercises can offer parliamentarians a hands-on appreciation of cyber threats, their potential impacts, and the response mechanisms required to defend against them.

Mapping a cybersecurity system: A condition for integrated approaches to oversight

Cybersecurity should be understood as a system characterized by complexity and multi-disciplinarity, in which roles and responsibilities are distributed among various stakeholders and sectors. Primarily, these include:

- Government departments or ministries, particularly in the areas of defence, law enforcement, communications, or technology, as these are usually responsible for setting and enforcing laws and standards, actively countering the threat from hostile actors, facili-

tating intelligence sharing, and providing technical guidance. The role played by these different government bodies in cybersecurity depends largely on the emphasis of a given country, either on the 'softer' social and economic aspects of cybersecurity (in which case, the ministries of interior or finance are likely to play a key role), or on military capabilities and cyber defence (which elevates the ministries of defence and/or intelligence in cybersecurity).

- Intelligence services, which have a mandate for countering threats from terrorism, espionage, large cybercrime networks, and foreign state actors, making them indispensable to any cybersecurity system.
- Specialized cybersecurity agencies (see Box 7, below), which have been created in most countries with the goal of protecting national networks, systems, and data from cyberthreats. The functions and scope of these agencies vary rather widely but include the provision of cybersecurity guidance and technical advice to government agencies, businesses, and individuals, as well as incident response, the monitoring and reporting of cyber incidents, threat assessment and early warning services, the promotion of cybersecurity awareness and good practice, and engagement in critical infrastructure protection (CIP).
- Regulatory bodies and specialized authorities responsible for the implementation of cybersecurity requirements in specific sectors, such as data protection authorities (e.g., an information commissioner), financial and telecommunications regulators, and consumer protection agencies, each of which plays a critical role in ensuring the security and integrity of information systems across various industries and jurisdictions.
- Private industry, which typically includes critical national infrastructure companies. These companies, which may be operators in critical sectors (energy, water, transport, health, telecommunications), or digital service providers (cloud services, online search engines, online marketplaces, etc.) all have cybersecurity responsibilities. They must manage their cyber risks in a way that protects data and digital assets while maintaining services.
- Academia, which contributes significantly to research and innovation, providing education and training to develop the cybersecurity workforce, raise public awareness, and inform policy decisions.

The large number of entities involved not only in ensuring cybersecurity, but also in providing direction and oversight, can hinder effective governance. Navigating the diverse mandates of these entities and mapping all the public and private actors with roles and responsibilities in cybersecurity can be a challenge for parliamentarians. This is why collaboration and information exchange across the parliamentary committees that oversee cybersecurity is so vital.

Furthermore, traditional allies of parliament in the realm of security sector oversight, such as a national audit office or ombuds institution, may have little influence over the private sector, which plays such an important role in cybersecurity. A number of other regulators and specialized

bodies may therefore be more relevant in cybersecurity oversight, and may bring unique perspectives and capabilities to the work of regulating the complex digital ecosystem. Due to this complexity, and the limited time and resources of parliament, oversight should be focused on the specialized competent authority for cybersecurity in any country, and on its key mechanisms for securing national digital systems.

Box 7. Examples of specialized cybersecurity agencies

Some specialized agencies for cybersecurity take a comprehensive approach, providing CIP, cybersecurity guidance, and incident response services. These include:

- the UK's **National Cyber Security Centre (NCSC)**, under the umbrella of the Government Communications Headquarters (GCHQ)
- the French National Cybersecurity Agency (ANSSI)
- The **National Cyber Security Centre (NCSC)** of The Netherlands, in the Ministry of Justice and Security
- The **Swedish Civil Contingencies Agency (MSB)**

Alternatively, some of these agencies are more focused on end-users, providing cybersecurity guidance, technical support, and training, and promoting best practices and awareness. These include:

- Germany's **Federal Office for Information Security (BSI)**, in the Ministry of Interior, Building and Community
- The Spanish **National Institute for Cybersecurity (INCIBE)**, in the Ministry of Economy Affairs and Digital Transformation
- The **Centre for Cybersecurity Belgium (CCB)**

National cybersecurity systems generally emphasize either centralization or coordination. In centralized systems, one entity sits atop a hierarchy, and there are clearly defined responsibilities and means of coordination. These systems can be rigid and may struggle to adapt to rapidly emerging threats and needs, however. In systems that prioritize coordination, multiple ministries and agencies share responsibilities, each operating independently. This approach allows for more flexibility in responding to cyber threats, but can present challenges including potential inconsistencies in implementing strategies, as the functioning of the system relies heavily on effective collaboration and government guidance.

Box 8. Switzerland's coordinated approach to cybersecurity

The coordinated approach to cybersecurity taken by Switzerland rests on a comprehensive National Cybersecurity Strategy, which integrates efforts across the federal government, cantonal authorities, the private sector, and international partners.⁴⁹

⁴⁹ Adopted in 2023, this is the third Swiss cybersecurity strategy, prepared with the involvement of over one hundred experts from the cantonal level, the business community, universities, civil society, and the federal government. It sets out the objectives and measures with which the

The responsibility for cybersecurity is distributed across various sectors and agencies in a holistic way to leverage the strengths of different stakeholders, enabling each of them to better respond to threats and provide mutual assistance. Because cybersecurity is not only a technical or IT issue, but is central to any overarching risk management strategy – whether that of a government body or a private corporation – it is considered an inherent lateral function spanning all departments and levels and affecting every aspect of all operations.

By rooting cybersecurity in this risk management approach, Switzerland has emphasized the need to identify, assess, and manage cyber risks systematically and continuously. To that end:

- The government plays a subsidiary and complementary role, and is tasked with identifying cybersecurity expertise, knowledge, support capabilities, and regulatory possibilities in support of critical infrastructure providers, the economy, and society.
- The National Cyber Security Centre (NCSC) is the central point of contact for matters of cybersecurity, providing support, coordination, and expertise to federal entities, cantons, businesses, and the public.
- Within the NCSC, the Reporting and Analysis Centre for Information Assurance (MEL-ANI) is key in handling and coordinating responses to cyber incidents and threats at the national level, providing critical information on threats to both private and public entities and assisting in the operational handling of cyber incidents.
- The Swiss military has also integrated cyber defence as a key component of its capabilities, in recognition of the fact that cyber threats represent a significant national security challenge.

Switzerland places a significant emphasis on cybersecurity education and research as well, supporting academic research, innovation in the private sector, and the development of cutting-edge cybersecurity solutions. Initiatives like the Cyber-Defence Campus, for example, serve as a link between government, industry, and academia in research, development, and training, and thereby foster innovation.

The Swiss Parliament is working to address legal gaps stemming from digitalization, and is continuously assessing, updating, and realigning the country's cybersecurity regulatory framework to meet evolving external conditions and internal priorities. The Security Policy Committee actively oversees the cyber domain and introduces legislative initiatives to enhance cybersecurity.⁵⁰ And in the plenary, questions and interpellations on cybersecurity topics are common.⁵¹

federal government and the cantons, together with the business community and universities, intend to counter cyber threats.

See: <https://www.ncsc.admin.ch/ncsc/fr/home/strategie/cyberstrategie-ncs.html>

⁵⁰ For example, see the initiative to create an independent digital infrastructure: <https://www.parlament.ch/press-releases/Pages/mm-sik-n-2022-02-15.aspx?lang=1036>

⁵¹ See the search results on the website of the Swiss Parliament at: <https://www.parlament.ch/fr/suche#k=cyber>

Making full use of oversight tools

Effectively scrutinizing cybersecurity requires not only knowledge, but focus and vigilance. Indeed, it is essential that parliamentarians approach cybersecurity with the conviction that this domain must be governed and overseen democratically, just like any other significant area of government activity. Their work can and should lead to the development of more robust and efficient cybersecurity systems, to better safeguard national security and the interests of citizens and businesses. But the strength of this work relies on the strategic and ongoing use of oversight tools; and thus, it is important for committees to understand and plan oversight as a process, and not as a series of independent, isolated activities. This means acknowledging that different oversight tools are better suited to different stages of the oversight process, and that tailoring tools to specific phases will enhance the effectiveness of oversight and allow for more targeted and relevant action. These tools include:

- 1. Monitoring and evaluation.** Cybersecurity policies and practices are monitored and evaluated mainly through analysis of the regular activity reports that are submitted to parliaments by government agencies, audits and reviews, consultative or expert hearings, and field visits. These offer members a multifaceted understanding of the sector, while offering assessments of the implementation of policy and law.
- 2. Parliamentary investigations.** Parliamentary committees often hold hearings to scrutinize the actions and effectiveness of the government agencies responsible for cybersecurity, and to look more closely at the compliance and cooperation of private sector entities. These hearings, which can serve as a platform for discussions of cyber incidents, technological developments, and challenges in implementing cybersecurity measures, allow MPs to analyse these matters in depth, ask for clarifications and details, and gather valuable insights into cyber threats and vulnerabilities. This can help them to assess the compliance of relevant entities, and to evaluate the country's cybersecurity infrastructure and incident response capabilities as well as the adequacy of government responses to cyber threats. By inviting experts, industry leaders, and stakeholders to provide their input and feedback on the effectiveness of policy and on emerging threats, the expertise of a parliament is developed along with its capacity for independent oversight. Another very valuable means by which parliamentarians can dig deeper into an issue like cybersecurity is through the Questions and Interpellations method, wherein individual MPs make direct requests to the government for responses on specific questions, independent from the mandate and agenda of the committees on which they serve.
- 3. Legislative amendments and adaptive systems.** Based on insights gained from monitoring and evaluation, hearings, and investigations, parliaments formulate legal remedies, debate amendments, and develop recommendations for government and the private sector, and also update cybersecurity laws to address any gaps, weaknesses, or emerging challenges. This

iterative process ensures that legislation keeps pace with the rapidly evolving nature of the cyber landscape and related technological advancements.

Box 9. Parliamentary inquiries into matters of cybersecurity

In the UK Parliament, the Joint Committee on the National Security Strategy conducted a year-long inquiry into **ransomware**, identified by UK authorities as the most significant cyber threat to the nation.⁵² The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time, to appoint specialist advisers, and to make reports to both parliamentary chambers; and throughout 2023, the Committee took written and oral evidence on ransomware from state officials, experts, and representatives of the private sector. The resulting report, *A hostage to fortune: ransomware and UK national security*, published on 13 December 2023, highlights how critical national infrastructure in the UK remains vulnerable despite the efforts of both government and the National Cyber Security Centre (NCSC).⁵³

The report presents 27 conclusions, and offers recommendations designed to boost cyber resilience and make ransomware a pressing political priority to which substantial resources are devoted. These include recommendations to:

- Conduct regular national exercises to prepare for major national ransomware attacks, with participation from the private sector.
- Take a more direct approach at the NCSC to protect electoral integrity and support political parties and high-risk individuals before, during, and after elections.
- Transfer the responsibility for tackling ransomware from the Home Office to the Cabinet Office, under the direct oversight of the Deputy Prime Minister.
- Fund the NCSC and National Crime Agency (NCA) to provide support to all public sector victims of ransomware, to the point of full recovery.
- Work with the insurance sector to establish a re-insurance scheme for major cyberattacks.
- Establish a central reporting mechanism for ransomware attacks, to ensure a full understanding of the nature and scale of the threat, and how best to tackle it.
- Ensure external scrutiny of government progress in implementing the National Cyber Strategy, including through National Audit Office performance audits.

The Government Response was presented in March 2024, and outlined the steps taken to improve cyber resilience in response to each conclusion and recommendation of the Committee.

⁵² Ransomware, which is a type of cyber extortion, can cause severe disruption to core public services and serious economic losses. Mass data loss from an attack can be irreversible, even when the ransom is paid. In 2021, the UK's *Integrated Review of Security, Defence, Development and Foreign Policy* identified ransomware as one of the most 'pernicious forms of cybercrime' and the National Cyber Strategy described it as 'the most significant cyber threat facing the UK'. See: <https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf>

⁵³ The evidence submitted to the Committee, the report, and the government's response are available at:

In the **Australian Parliament**, in October 2023, the **Joint Committee on Law Enforcement** opened an investigation into the capacity of law enforcement to respond to cybercrime. In a matter of months, the Committee received over 40 submissions of evidence from a variety of law enforcement agencies, government agencies, and private entities.⁵⁴ This inquiry, still ongoing at the time of writing, aims to assess:

the existing capabilities of law enforcement in detecting, investigating, and prosecuting cyber-crime;

- the coordination mechanisms used by law enforcement in investigating cybercrime and sharing information related to emerging threats;
- the degree of coordination among law enforcement, civil society, and private sector organizations in responding to cybercrime and its risks;
- the scale and scope of cybercrime carried out in/from Australia and against Australians;
- opportunities and challenges that exist in the legislative framework when it comes to supporting law enforcement to investigate and act upon cybercrime; and
- the best prevention and education approaches and strategies to reduce the number of cybercrime victims.

Promoting accountable public-private partnerships

Collaboration between government and the private sector is vital to robust cybersecurity. The information and communications technology (ICT) infrastructure that makes the internet possible is neither owned nor operated by states, but by thousands of private companies, which also hold expertise, capacities for innovation, and technical infrastructures unequalled by government entities. Hence, state cybersecurity goods and services often rely on private companies.

The importance of the private sector to cybersecurity and the dominance of private digital infrastructure is recognized by many parliaments worldwide, which therefore actively foster public-private partnerships and create incentives for such cooperation. These incentives may include:

- Providing a legal framework that encourages or requires information sharing and collaboration.
- Offering legal protections for companies that participate in information sharing, addressing concerns over privacy, confidentiality, and potential legal repercussions.
- Creating shared platforms and centres where government and private sector representatives can collaborate, share threat intelligence, and work on joint initiatives.
- Providing resources and expertise to help the private sector improve cybersecurity practices.

<https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/198995/a-hostage-to-fortune-ransomware-and-uk-national-security/>

⁵⁴ Details of the inquiry are available here: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/LECybercrime47

Box 10. Parliamentary support for public-private partnerships in cybersecurity

In 2015, the **U.S. Congress** passed the **Cybersecurity Information Sharing Act** to facilitate and encourage the sharing of cyber threat information between the government and the private sector.⁵⁵ The law provides legal liability protections for companies that share threat data with the government, a key concern that had previously hindered information exchange. It also aims to help both parties better understand and respond to cyber threats by enhancing the overall cyber resilience of critical infrastructure.

In the **UK**, the parliament has supported the **Cyber Security Information Sharing Partnership (CiSP)**, a joint industry-government initiative designed to share cyber threat and vulnerability information in a secure and confidential manner.⁵⁶ A ranking parliamentarian also co-chairs the **National Cyber Advisory Board**, a forum for inclusive and engaged national dialogue on cyber issues that includes leaders from academia, industry, and the non-profit sector, focused on increasing the national skills base in cybersecurity, identifying and mitigating cyber vulnerabilities, and protecting digital supply chains.⁵⁷

The **Australian Parliament** supports partnerships of the Australian Cyber Security Centre (ACSC) with the private sector, through initiatives that include **Joint Cyber Security Centres**.⁵⁸ These centres are located across the country and serve as hubs for government and industry to collaborate on cybersecurity issues, share threat intelligence, and work together on enhancing Australia's cyber resilience.

In the **EU**, the **NIS(2) Directive** requires members to encourage public-private cooperation in the field of cybersecurity, and has led to the establishment of Information Sharing and Analysis Centers (ISACs) in various sectors. ISACs provide a framework for threat intelligence and best practice sharing, within industries such as finance, healthcare, and energy.

The **National Diet of Japan** has supported the establishment of a **Cybersecurity Strategic Headquarters** to promote comprehensive measures meant to ensure cybersecurity across the country.⁵⁹ This includes initiatives to promote information sharing, joint exercises, and collaborative research and development projects aimed at protecting critical infrastructure and improving incident response capabilities.

⁵⁵ The bill is available at: <https://www.congress.gov/bill/113th-congress/senate-bill/2588>

⁵⁶ The platform is available here: <https://www.ncsc.gov.uk/cisp/home>

⁵⁷ Information on the Cyber Advisory Board is available at: <https://www.gov.uk/government/groups/the-national-cyber-advisory-board>

⁵⁸ Information on the program is available at: <https://www.cyber.gov.au/partnershipprogram>

⁵⁹ Pratinashree Basu, ORF, 27 March 2024. Available at: <https://www.orfonline.org/expert-speak/from-reactive-to-proactive-japan-s-advances-in-cybersecurity-and-cyber-defence-strategies>

Beyond encouraging public-private partnerships, parliaments must ensure robust accountability mechanisms in the context of public-private cooperation, to ensure the responsible use of power and resources. Securing cyber space without compromising public interests or privacy requires the establishment of clear legal frameworks and oversight processes to monitor activities and their effectiveness, to assess adherence to cybersecurity standards, and to ensure transparency in decision-making and public spending. Yet, oversight has traditionally functioned as a political relationship between the legislative and executive branches, and has not been focused on private companies, which are not accustomed to the level of scrutiny and transparency mandated of public institutions. This, combined with the significant economic size and leverage of some private companies, complicates accountability.

Parliaments must navigate these challenges by creating stringent regulatory frameworks and developing oversight practices that compel private companies to adhere to standards of transparency, performance, and ethical conduct, while also balancing the political complexities inherent in legislative-executive interactions. Parliamentary hearings and inquiries often call upon private companies to testify on cybersecurity issues, especially in cases where significant breaches have occurred, or where companies play a critical role in the digital infrastructure. These hearings can help parliamentarians understand a cyber incident, assess a company's response, evaluate the impact on consumers and national security, and shape future legislation. Representatives of large technology companies like Google, Amazon, and Microsoft are also frequently called upon to testify in parliamentary inquiries around the world, not necessarily about breaches but about their companies' cybersecurity practices, data protection measures, and the role they play in protecting users from cyber threats.

Box 11. Parliamentary hearings on incidents involving private services providers

Facebook and Cambridge Analytica (U.S. and UK): After the 2018 revelation that the data of millions of Facebook users had been improperly shared with Cambridge Analytica, a political consulting firm, executives from Facebook, including CEO Mark Zuckerberg, were called to testify in front of the U.S. Congress and the UK Parliament. These hearings focused on issues of data privacy, the protection of user information, and the potential for misuse of data in political campaigns.

Equifax Data Breach (U.S.): In 2017, Equifax, one of three major consumer credit reporting agencies in the U.S., experienced a massive data breach affecting approximately 143 million Americans. The breach included sensitive information such as Social Security numbers and birth dates. Following the breach, Equifax executives were called to testify before several committees in the U.S. Congress to explain how it had occurred, how the company had responded, and what measures were being taken to prevent future incidents.

Sony Pictures Entertainment Hack (U.S.): After a 2014 cyberattack on Sony Pictures Entertainment that resulted in the leak of vast amounts of data, including personal information about employees and their families, email exchanges, and unreleased movie files, executives from Sony were called to testify before the U.S. Congress. The hearings examined the nature of the cyberattack, its implications for cybersecurity in the entertainment industry, and its broader national security implications.

TalkTalk Telecom Group (UK): In 2015, the UK broadband provider TalkTalk suffered a significant cyberattack that compromised the data of more than 150,000 customers, including sensitive financial information. The incident led to a parliamentary inquiry by the Culture, Media, and Sport Committee, which examined the circumstances of the breach, the effectiveness of regulatory responses, and implications for cybersecurity practices within the telecom industry.

Allocating resources and ensuring financial accountability

Allocating budgetary resources for the development of cybersecurity capacities is probably the most significant means by which parliaments influence cybersecurity. These allocations are usually debated and voted upon annually, during the adoption of a national budget. Investments in institutional capacities, research, technology, personnel, and training related to cybersecurity are increasing worldwide and the cybersecurity economy is growing rapidly, surpassing overall global economic expansion and outpacing the tech sector. In fact, in 2022, the cybersecurity economy expanded twice as fast as the world economy; and in 2023, four times as fast.⁶⁰

Encouraging education and public awareness

Cybersecurity simply must be on the parliamentary agenda. As a highly visible state institution, the members of which are frequently in the media spotlight, parliaments can easily shape public priorities and lift issues to the attention of citizens. To highlight the importance of cybersecurity and ensure it receives the attention it deserves, parliamentarians must raise cybersecurity issues in legislative debates, policy discussions, and their interactions with the media.⁶¹ Indeed, it is the power of parliament to shape the public agenda that allows it to influence policy and increases its leverage in exercising oversight. As parliaments have no executive power, they often rely on public pressure and awareness as a means of compelling the executive to respond to their concerns and recommendations.

⁶⁰ World Economic Forum, Global Cybersecurity Outlook 2024, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

⁶¹ ENISA has collected good practices on raising awareness on cybersecurity. See: <https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity>

Through **good public communication on cybersecurity**, parliaments can also foster a culture of cybersecurity awareness and enhance the resilience of society against cyber threats. This should entail:

- Active engagement with the media, through press releases, interviews, and social media, to keep cybersecurity issues in the public eye, raise awareness about cybersecurity risks and the importance of cyber hygiene, and encourage individuals and organizations to be more vigilant in protecting themselves.
- Public debates, hearings, and consultations on cybersecurity issues, to allow for the discussion of diverse opinions and solutions that can lead to more effective and inclusive cybersecurity policies.
- Efforts to foster dialogue among various stakeholders, to strengthen cooperation and coordination in addressing cyber threats.
- Transparency regarding parliamentary findings, assessments, and recommendations drawn from government hearings and expert exchanges on cybersecurity, to build public trust in the democratic institutions and processes aimed at increasing accountability.⁶²
- Educational campaigns and initiatives, requested and supported by parliament and implemented by government, academia, and civil society, to promote cybersecurity awareness, safe online practices, and cyber literacy for citizens of all ages.
- Specialized training for government officials involved in cybersecurity policymaking and implementation, funded by parliament.

Parliamentary debate and approval of a **National Cybersecurity Strategy** is one of the most effective ways to bring cybersecurity issues to the forefront of public consciousness. This process can elevate the importance of cybersecurity in the national agenda, facilitate public understanding of the country's cybersecurity posture, and invite citizen engagement. Parliaments should ensure that any cybersecurity strategy addresses the most pressing threats and aligns with the nation's broader security and economic goals. A comprehensive cybersecurity strategy typically includes an assessment of current cyber threats, an outline of national cybersecurity objectives, and specific measures to protect critical infrastructure, safeguard government and private sector information, and enhance incident response capabilities. Typically, the importance of public awareness, workforce development, international collaboration, and legal frameworks to combat cybercrime are also emphasized.

Encouraging international cooperation and information sharing

Cyber threats know no borders. This means that the effectiveness of cybersecurity measures depends on global cooperation and a unified approach to international cyber threats. Parliaments

⁶² For example, see the Australian Parliament page on cybersecurity, with brief summaries and links to committees cybersecurity initiatives: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook46p/Cybersecurity

can therefore contribute meaningfully to strengthening cybersecurity on a global level through a commitment to international collaboration and information sharing. Such cooperation may be facilitated by the ratification of international treaties and participation in global cybersecurity forums and initiatives, and merely by encouraging national authorities to engage in an exchange of information and best practices with other countries. One way or another, parliaments must advocate for and participate in international efforts to harmonize cybersecurity standards, share threat intelligence, and support global cybercrime law enforcement.

Box 12. Everyone must start cooperating

The NotPetya cyberattack, launched in June 2017, underscored the critical need for international cooperation in cybersecurity. Created by Russia's military spy agency, the GRU, and originally targeted at Ukraine, the attack quickly escalated into a global crisis that affected systems in over 60 countries including the United States, Great Britain, and Germany. Designed to look like a traditional ransomware programme, the malware at the centre of the attack took the form of a 'wiper' designed for mass destruction rather than financial gain. This was a shift towards the use of cyber tools for political warfare, and led to widespread data loss and significant operational disruptions across various sectors, including government, finance, energy, utilities, and healthcare. The financial damages have been estimated at over USD 10 billion.⁶³

This incident marked a significant turning point and prompted the realization that effectively responding to and preventing cyber threats would require robust global partnerships and a unified approach. In its aftermath, new levels of international collaboration emerged, such as increased information sharing between countries and between the public and private sectors, strengthened cybersecurity protocols, and a rise in international cyber defence exercises.

The role of the international community in defining and enforcing cybersecurity norms cannot be overstated. Simply put, collective action can lead to enhanced cyber resilience. As international frameworks not only set standards but also facilitate crucial cross-border cooperation in the fight against cybercrime, parliaments should advocate that their countries actively participate in these frameworks and should adapt domestic laws to align with global best practices.

Through engagement in international forums, parliaments can contribute to the ongoing discourse on cyber norms, ensuring they reflect a wide range of interests and values. The cybersecurity landscape is constantly evolving, presenting both challenges and opportunities to legislators and society alike. However, by adopting a proactive, collaborative, and global perspective, parliaments can make important contributions to digital safety and cyber resilience. This not only protects national security but also supports economic stability and the democratic values upon which our societies are built.

⁶³ Julia Bellabarba, 'NotPetya: Understanding the Destructiveness of Cyberattacks', Security Outlines, 21 January 2024. Available at: <https://www.securityoutlines.cz/notpetya-understanding-the-destructiveness-of-cyberattacks/>

CHAPTER 5

Safeguarding digital democracy: the evolving role of non-public actors in Albania

by Megi Reçi and Sara Kelmendi

Table of contents

	Introduction.....	108
1.	State of affairs: The role of CSOs and non-public actors in cybersecurity oversight in Albania.....	109
1.1	Inclusion in cybersecurity policymaking.....	109
1.2	Challenges for CSOs and non-public actors in Albania's cybersecurity oversight.....	112
2.	Examining accountability in cyber attacks & data leaks: a case study.....	114
2.1	Significant citizens' personal data leaks in Albania.....	114
2.1.1	Accountability for citizens' personal data leaks.....	115
2.2	Cyberattacks against the Albanian government.....	116
2.2.1	Accountability for cyberattacks against the Albanian government.....	116
2.2.2	Did government reporting on the crisis meet transparency standards?.....	117
2.3	Testing the post-cyberattack transparency of public authorities.....	120
2.4	Perception of government's approach during and after the incidents.....	122
2.5	Media coverage of the incidents in Albania.....	124
3.	Areas for future engagement: insights from the Western Balkans...	127
3.1	Replicable advocacy practices.....	127
3.2	Opportunities for non-public actors to enhance their contribution to cybersecurity oversight in Albania.....	129
	Conclusions.....	132

Introduction

Engagement with civil society is key to a culture of participation that enhances the democratic nature of decision making about security. The expertise and independence of civil society acts as a counterbalance and complements government policy by providing decision-makers with a wider range of perspectives, information, and ideas.¹ One of the mechanisms that enables civil society inclusion in decision making is public consultations, which are essential to ensuring the transparency, accountability, credibility, and legitimacy of decision-making processes. In Albania, however, studies show that public consultations remain largely formal exercises that offer few opportunities for meaningful engagement and impact.²

This leaves a gap between the theoretical benefits of civil society engagement and its actual impact in Albania and invites an in-depth analysis of how civil society organizations (CSOs) and other non-public actors are contributing to greater cybersecurity oversight in the country. Hence, this chapter explores civil society efforts to protect digital rights and promote a more inclusive digital governance framework in Albania, despite limited capacities and a lack of opportunities to meaningfully participate in policymaking. Through a case study analysis of Albania's response to cyberattacks and data breaches, the chapter identifies critical gaps in institutional accountability and transparency; and on this basis, advocates for a refined digital governance approach that prioritizes transparency, inclusivity, and accountability. Additionally, successful practices within the Western Balkans and Albania are highlighted, as a guide to potential areas for future engagement and openings through which non-public actors may be able to significantly enhance their contributions to Albanian digital governance and cybersecurity.

This chapter draws from qualitative interviews and extensive desk research conducted from October 2023 to January 2024.³ Thirteen interviewees, including representatives from CSOs, journalists, factcheckers, researchers, whistleblowers, and experts in human rights and cybersecurity, offered important insights into the challenges and opportunities of the Albanian digital landscape. Their interviews were transcribed and analysed using MAXQDA software, to identify patterns and themes. Six Freedom of Information (FOI) requests were also submitted to public institutions as a means of testing and validating their transparency and accountability following cyberattacks and data leaks.

¹ DCAF – Geneva Centre for Security Sector Governance, 'Civil Society', SSR Backgrounder Series, 2019.

² Megi Reçi and Besjana Kuçi, *A Decade of Consultation Law in Albania: Call for Reform* (Tirana: Institute for Democracy and Mediation, 2023).

³ It is important to note that this paper does not encompass events occurring or information available after January 2024.

1. State of affairs: The role of CSOs and non-public actors in cybersecurity oversight in Albania

1.1 Inclusion in cybersecurity policymaking

Public consultations are one of the key mechanisms that enable civil society engagement. They are essential for transparency, accountability, credibility and legitimacy of decision-making. However, studies have shown that in Albania, public consultations remain widely formal exercises, with limited opportunities for engagement and impact⁴.

Between 2021 and 2023, the Albanian government made significant changes to policy and law in the areas of cybersecurity and digitalization, including by revising or drafting the Digital Agenda 2022–2026, the Law on Protection of Personal Data, the Law on Cybersecurity, and the Law on E-governance. As of January 2024, these laws had all been adopted or were in the process of being adopted. Despite their importance, there remains a lack of transparency in the consultation processes of these documents. The efforts toward impact assessment and risk analysis are also insufficient, indicating a limited policy reflection on recent cyber incidents and data leaks.⁵

These laws were published on the country's Electronic Registration for Notification and Public Consultations, yet only the Law on E-governance was accompanied by a comprehensive report on the public consultation process.⁶ And even then, this report fails to clearly convey which stakeholders were consulted, vaguely and inaccurately referring to civil society as 'civil societies' and labelling other participants as 'various economic operators'. The report also reveals the inadequacy of providing access to the draft law only a week in advance, raising concerns about whether the time allowed for review was ample for thoughtful and thorough consideration, as it generated just five comments during public consultation, all from telecommunication companies. Similarly, according to the consultation report on the Digital Agenda provided by NAIS via Freedom of Information (FOI) request⁷, the institution had received zero comments, and the participants were referred to (again) as "civil societies".

Moreover, although the Ministry of Justice and the Information and Data Protection (IDP) Commissioner did conduct relevant consultations for the Law on Protection of Personal Data⁸, a

⁴ Institute for Democracy and Mediation (2023) A decade of public consultation law: Call for reform <https://idmalbania.org/research-report-a-decade-of-public-consultation-law-in-albania-call-for-reform/>

⁵ Friedrich-Ebert-Stiftung, *Cybersecurity in Southeast Europe: Past, Present, and Future, Political Trends and Dynamics Briefing*, vol. 2 (Sarajevo: FES Dialogue Southeast Europe, 2023).

⁶ See the entry for the Law on E-governance, on the Electronic Registration for Public Notices and Consultations (Rigjistri Elektronik për Njoftimet dhe Konsultimet Publike), at: <https://konsultimipublik.gov.al/Konsultime/Detaje/413>. See the entries for the Law on Cybersecurity here: <https://konsultimipublik.gov.al/Konsultime/Detaje/626>; and for the Law on Protection of Personal Data here: <https://konsultimipublik.gov.al/Konsultime/Detaje/472>.

⁷ Similarly, a consultation report on the Digital Agenda provided by the National Agency for Information Society (NAIS) to the authors showed that the Agency received zero comments on the Law on E-governance. Information provided by NAIS in response to a FOI request made on 7 December 2023.

⁸ See a summary of these consultation activities (in the local language) on the website of the IDP Commissioner, at: <https://www.idp.al/2022/07/12/konsultimi-publik-i-projektligjit-per-mbrojtjen-e-te-dhenave-personale/>

consultation report was not published by January 2024. Other important documents associated with the Law were published, however, which made the absence of a key document – the regulatory impact assessment (RIA) report – more notable, as it is used to evaluate and analyse the potential impacts and consequences of proposed regulations or legislation before they are implemented. While a report accompanying the draft law refers to the RIA in its text, the RIA itself has not been made public.⁹

The authors viewed the consultation report for the Law on Cybersecurity only by making a FOI request to the National Authority on Electronic Certification and Cybersecurity (NAECCS)¹⁰, as it, too, was not published by January 2024. Furthermore, the report revealed that consultations had engaged mostly governmental actors from agencies, ministries, and the national bank, along with the IDP Commissioner, and that the only non-state actors were representatives of the Association of Banks and the Embassy of the United States. A related report on the results of consultations for the National Strategy on Cybersecurity was neither published nor made available in response to a FOI request.

This was not the only request to government agencies that went unfulfilled over the course of this research. The authors also received no response to inquiries made to the National Agency for Information Society (NAIS) and the NAECCS for information on their institutional databases of stakeholders, which are typically maintained and disclosed by all public authorities to transparently identify target stakeholders for public consultation efforts. Similarly, both institutions failed to provide examples of how they cooperate with civil society, and how they include non-state actors in decision-making processes or technical working groups.

Yet, these are essential questions, as inclusion is crucial to policymaking and good governance. In fact, an array of experts in cybersecurity policymaking and digitalization have noted this and have emphasized the absence of inclusive dialogue.

The experience of one cybersecurity expert interviewed for this research, who was invited to engage with the government on cybersecurity as part of an ad-hoc expert group for crisis management, is instructive in this regard. Despite an initially positive reception of the initiative, concerns soon arose in relation to restricted data access and the confidentiality of topics under discussion within the group. According to this expert, when the proposals they put forward for important enhancements – such as penetration test authorization, the transparent documentation of institutional tests, and oversight of non-state information and communication technology (ICT) actors – were also dismissed, they decided to end their participation.¹¹

⁹ Information provided by the IDP Commissioner in response to a FOI request, on 1 December 2023.

¹⁰ Information provided by the NAECC in response to a FOI request, on 30 November 2023.

¹¹ G.P., IT expert and whistleblower, interview by authors, 11 October 2023.

Another interviewee, a civil society representative, noted that cybersecurity professionals should develop good communication skills to engage constructively in inclusive policymaking, but also highlighted the need for dialogue that draws on the value of diverse expertise. In their view, public consultations are enriched by a blend of technical knowledge and ‘soft skills’ and should include social scientists and human rights experts alongside cybersecurity experts. They pointed out that, despite some successful child cyber safety efforts in Albania, the exclusion of expertise outside specific sectors means that issues like gender rights, and other societal concerns, are neglected.¹² This reflects previous research in the country that has underscored an existing disparity between cybersecurity and human rights, and has highlighted the need for cybersecurity governance to adopt a human rights-oriented approach - aimed at addressing and mitigating human rights risks posed by digitalization.¹³

This reflects previous research in the country that has underscored an existing disparity between cybersecurity and human rights, and has highlighted the need for cybersecurity governance to adopt a human rights-oriented approach - aimed at addressing and mitigating human rights risks posed by digitalization.

Commenting on what some perceive as a lack of engagement on the part of civil society organizations to cybersecurity policymaking, one expert attributed this to a mistrust of the government, capacity limitations within civil society in this relatively new field. This interviewee emphasized the need for specialized knowledge but noted that *even sizable organizations may lack the in-house expertise to effectively engage in an area like cybersecurity, which features an ever-evolving landscape*.¹⁴

Another interviewee, a representative from a fact-checking organization, explained that new technologies such as e-services and so-called artificial intelligence (AI) products are often introduced without adequate discussion or a clear understanding of the potential risks.¹⁵ Drawing on past experiences, they contended that the embrace of these technologies absent any real consideration of the risks is likely to bring negative consequences. This underscores the importance of non-governmental actors who can contribute in meaningful ways to digital governance and policy development by shedding light on the social implications and perils associated with new technologies. By advocating for inclusive decision-making, civil society can play a key part in strengthening cybersecurity policy, facilitating an informed debate, rather than unquestioned acceptance of emerging technologies.¹⁶

¹² A.H., civil society expert on children’s online safety, interview by authors, 23 October 2023.

¹³ Megi Reçi and Sara Kelmendi, ‘Albania: Bridging the Gap Between Cyber Policy Fragmentation and Human Rights’ in *Cybersecurity and Human Rights in the Western Balkans: Mapping Governance and Actors*, edited by Franziska Klopfer and Laylo Merali (Geneva: DCAF, 2022).

¹⁴ B.B., civil society and media researcher, interview by authors, 27 October 2023.

¹⁵ P.P., journalist, interview by authors, 10 November 2023. Also see: Fjori Sinoruka, ‘Albanian Plan to Use AI to Align Laws With EU Questioned’, *Balkan Insight*, 20 December 2023, <https://balkaninsight.com/2023/12/20/albanian-plan-to-use-ai-to-align-laws-with-eu-questioned/>.

¹⁶ P.P., journalist, interview by authors, 10 November 2023.

Collectively, interviewed civic actors shed light on the challenges—exclusion, technical bias, and the necessity for specialized expertise—in cybersecurity and digitalization policies.

They emphasized the need for a more holistic approach, involving open dialogue and efforts to spread awareness about cybersecurity more broadly. Achieving informed decision-making requires that past setbacks are acknowledged, emerging human rights concerns are addressed, and transparent consultations are held with civil society, diverse interest groups, and affected communities. This kind of *stakeholder engagement is essential to rebuilding trust, encouraging participation, and mitigating potential risks to security and human rights*.

1.2 Challenges for CSOs and non-public actors in Albania's cybersecurity oversight

According to an expert interviewed for this research, *the primary obstacle faced by CSOs that seek to fill a digital governance role in Albania is a significant lack of expertise in cybersecurity*.¹⁷ This severely limits the ability of these organizations to make meaningful contributions to policy formulation and monitoring. They can and do leverage soft skills to engage key demographics and scrutinize policies but are hindered in any further engagement by deficiencies in human and financial resources and essential technical skills.¹⁸

To bridge this gap, CSOs often hire external experts to manage the technical dimensions of their projects. However, this approach tends to lead to a fragmentation of efforts rather than to a greater cohesion and can dilute the original objectives or mission of an organization. For, when external experts are not fully on board with the vision and values of a contracting CSO, their work can potentially lead to altered project outcomes. Despite this risk, the choice of civil society to seek external expertise is understandable, given the degree to which *in-depth technical knowledge is a prerequisite for a CSO to effectively monitor government actions, push for significant changes, or participate on equal footing in important discussions of digital governance*.¹⁹ In other words, the absence of such knowledge reduces the impact of civil society on digital policymaking and undermines the very system of checks and balances on which democracy rests.

In addition to these structural challenges, this research sought to determine whether CSOs and non-public actors face any specific threats or repercussions extending from their work in digital governance. While a majority of interviewees reported no direct repercussions associated with this work, some said that colleagues in both the public and private sectors had confronted these

¹⁷ A.H., civil society expert on children's online safety, interview by authors, 23 October 2023; P.P., journalist, interview by authors, 10 November 2023.

¹⁸ B.B., civil society and media researcher, interview by authors, 27 October 2023; A.H., civil society expert on children's online safety, interview by authors, 23 October 2023.

¹⁹ P.P., journalist, interview by authors, 10 November 2023; B.B., civil society and media researcher, interview by authors, 27 October 2023.

threats. This highlights the need for a more supportive legal environment for independent experts and those engaged in important investigative and reporting work in this area. Such an environment will have to be cultivated through reforms to the existing legal framework, to better protect individuals who uncover and share critical information from legal repercussions. For example, the Vulnerability Disclosure Policy of the US ensures that security researchers acting in good faith and adhering to the guidelines of a relevant agency are authorized by the agency and protected against legal action for their research.²⁰ The policy requires researchers to pause their investigation upon finding a vulnerability or encountering sensitive data, immediately notify the agency, and avoid disclosing the information; in turn, the agency guarantees its collaboration to resolve issues and its defence of the researcher's authorization if third-party legal challenges arise.

In Albania, such a policy would encourage experts to cooperate more closely with state institutions and would help mitigate the fears of repercussion that lead to self-censorship. These fears can hardly be dismissed, even if, as one expert put it, they are *'often... more imaginary than real.'* This interviewee shared that *'after over a decade of appearances in the media, nearly 90% of which have been critical, I have yet to be blackmailed or threatened,'* but admitted that *'some colleagues have faced blackmail and threats and have reported them to law enforcement agencies.'*²¹ Similarly, journalists interviewed for this research said that they themselves had not faced any threats for reporting on cybersecurity issues, but that some of their colleagues had. However, one interviewee who is a journalist described being contacted by a private bank for citing the bank's own public statement disclosing that it had experienced a cyberattack. In the statement, the bank had reassured its customers that, despite the incident, no data had been compromised and its systems had been fully restored to normal operation. Yet, curiously, upon finding that this statement had been cited in an online post, the bank urged the media to suppress any coverage of the incident it detailed, though it had already been acknowledged publicly.²²

One interviewee claimed that some individuals have even experienced economic repercussions for standing against institutional mismanagement and calling for greater transparency in cybersecurity at the state level. For instance, the business of an IT expert suffered as they perceived their clients were pressured to sever ties, in what appeared to be a form of retaliation for having taken public stances and having issued critical declarations against the government's mismanagement of data leaks and cyberattacks.²³ This expert suggested that media outlets in Albania do not report on such reprisals, as these outlets are highly dependent on public funding. Their editorial policies are therefore shaped by the need to secure contracts with public institutions, which gives these institutions financial and political leverage to shape press coverage in the country.

²⁰ See: Cybersecurity and Infrastructure Security Agency, 'Vulnerability Disclosure Policy Template', <https://www.cisa.gov/vulnerability-disclosure-policy-template> (accessed 5 April 2024).

²¹ B.S., cybersecurity expert, interview by authors, 12 October 2023.

²² F.S., journalist, interview by authors, 17 October 2023.

²³ G.P., IT expert and whistleblower, interview by authors, 11 October 2023.

In the case of this IT expert, such leverage may have been wielded to revoke an invitation extended by a private TV channel to discuss cyberattacks on air. The expert was dis-invited at the last minute on the premise that the show had been cancelled, but it was in fact broadcast, featuring only representatives from state institutions excluding independent voices. Yet, the challenges for this expert extended beyond professional repercussions and into the realm of personal safety and security after they filed a whistleblower lawsuit, prompting threats to their life and against their family members. At one point, GPS trackers were even installed on their car, according to their statements. In an interview, they said that these threats have profoundly affected their personal life, to such a degree that they have considered leaving the country.²⁴

While the experience of this expert may not be the norm, the prevailing perception among cybersecurity professionals in Albania is that individuals who act as whistleblowers or seek government accountability are likely to face some kind of retribution. On its own, this presumption serves as a key obstacle to better digital governance in the country, as it leads to systemic self-censorship. This only adds to the array of challenges facing CSOs and non-public actors in their efforts to safeguard digital democracy.

2. Examining accountability in cyber attacks & data leaks: a case study

2.1 Significant citizens' personal data leaks in Albania

Over the past three years, Albanian citizens have been the victims of several significant breaches of personal data. In 2021 alone, leaks exposed databases containing:

- *The personal and sensitive data of the voting population of Tirana (910,061 citizens)*
- *The salaries of individuals in both the public and private sectors (637,138 employees)*
- *License plate information (591,964 individuals and companies)*

These exposures divulged personal and sensitive data, including personal identification numbers, employment information, addresses, phone numbers, assumed political preferences, license plate numbers, salaries, and more. Notably, the leak of voter data contained particularly sensitive details in some cases, as it turned out that a 'patron' had been assigned to each voter by the ruling Socialist Party, to monitor their voting preferences and potentially exploit vulnerabilities that might influence their voting behaviour. To facilitate this, the information collected on some voters was so broad and sensitive as to encompass health data, family dynamics, religious views, and ethnicity identity.²⁵

²⁴ G.P., IT expert and whistleblower, interview by authors, 11 October 2023.

²⁵ Reçi and Kelmendi, 'Albania: Bridging the Gap Between Cyber Policy Fragmentation and Human Rights'.

The release of this information constituted a grave breach, facilitating the construction of detailed profiles for affected citizens.²⁶ And yet, no government institution has recommended or initiated the issuance of new personal identification numbers to Albanian citizens. The experts interviewed for this research were unanimous that this should have been paramount, given the security risks associated with a leak of these data, which include the potential for identity theft. This enables criminals to commit financial fraud by making formal requests to financial institutions or conducting unauthorized bank transactions as the victim and can lead to other serious breaches of personal security and privacy.

2.1.1 Accountability for citizens' personal data leaks

For two of the data breaches that took place in 2021 (of salary data and license plate information), some responsibility was attributed individually, resulting in charges of passive corruption and misuse of power against specific employees. In addition, fines were imposed by the IDP Commissioner on the General Directorate of Taxes and the General Directorate of Road Transport Service.

However, in response to the voter database leak, there has yet to be any institutional or political accountability. Investigations conducted by the IDP Commissioner involving the Socialist Party, the NAIS, and the civil registry did not yield definitive answers, thus failing to deliver accountability, even if the IDP Commissioner left open the possibility that the leak may have been conceived and exploited by the ruling Socialist Party for electoral purposes. And, though criminal investigations into the leak commenced in 2021, the Prosecution has yet to identify any suspects.²⁷

Findings of the IDP Commissioner, indicate that institutions have pointed fingers at each other, without taking responsibility or ownership of the situation.²⁸ According to the experts interviewed, this lack of accountability and tendency towards blame-shifting could partly be attributed to the disjointed institutional framework for cybersecurity governance in Albania. This is something the authors have also noted previously,²⁹ and which the government itself acknowledged in its rationale for proposed legal amendments to the Law on Cybersecurity.³⁰ Moreover, as some interviewees observed, these structural problems with digital governance may also be exacerbated by the absence of a dedicated minister who acts as a central, responsible authority.³¹

²⁶ Orkidea Xhaferaj, Blerjana Bino, and Erjon Curraj, 'Working Paper: Mapping personal data violations in Albania: A short retrospective on massive breaches in the country', SCiDEV, December 2022. Available as a pdf at: <https://scidevcenter.org/wp-content/uploads/2024/03/Data-breach-1.pdf>.

²⁷ Information provided by the Prosecutor's Office in Tirana in response to a FOI request, on 24 November 2023.

²⁸ Xhaferaj, Bino, and Curraj, 'Working Paper: Mapping personal data violations in Albania'.

²⁹ Reçi and Kelmendi, 'Albania: Bridging the Gap Between Cyber Policy Fragmentation and Human Rights'.

³⁰ See the entry for the Law on Cybersecurity, on the Electronic Registration for Public Notices and Consultations, at: <https://konsultimipublik.gov.al/Konsultime/Detaje/626>.

³¹ B.B., civil society and media researcher, interview by authors, 27 October 2023; A.H., civil society expert on children's online safety, interview by authors, 23 October 2023.

2.2 Cyberattacks against the Albanian government

In July 2022, Albania experienced severe cyberattacks that resulted in the temporary shutdown of government websites and disruptions to public e-services, as well as extensive data leaks affecting citizens, public officials, and various institutions. The attacks targeted the NAIS, the State Police, and other public entities. The hacking group responsible soon began publishing files from government ministries, police directorates, the municipality of Tirana, the Traveler Information Management System (TIMS), the Albanian Parliament, and the mailboxes of the Prime Minister and President, citizens' phone numbers, data of employees from the Albanian State Intelligence Service, and other state officials.³² But the situation escalated even further when the personal data of Albanian citizens was sold on the dark web³³; again, leaving these citizens vulnerable to crimes including identity theft and fraud.

2.2.1 Accountability for cyberattacks against the Albanian government

Criminal investigations into the cyberattacks against NAIS systems have been opened by the Prosecution Office in Tirana, relating to the offences of 'interference with computer data', 'interference with computer systems', and 'misuse of equipment'. But these investigations are currently suspended as the Prosecution awaits information from mutual legal assistance requests submitted to other states.³⁴

Although technical reports have attributed the attack to Iranian state actors, there remains a lack of national authorities' definitive attribution of responsibility. On an individual level, five former public administration employees were accused of the criminal offence of "abuse of duty"³⁵, whilst on a political level, diplomatic ties between Albania and Iran were severed following these events.

According to experts interviewed for this research, this absence of institutional and political accountability for cyberattacks in Albania significantly limits the ability of the country's cybersecurity structures to reflect constructively on security failures and respond adaptively. As an international scholar with an expertise in digital security put it, *'When you pay public money to build state systems, you expect that there will be enough security, and monitoring, so that even when incidents occur, they are identified and caught quickly. In the case of Albania, these internal systems clearly have flaws', as exposed by both the data leaks and cyberattacks; flaws this expert ascribed to 'either... corruption, or incompetence'.*

³² See: Nensi Bogdani, 'Digital Transition Creates New Challenges in Albania's Online Environment', in *Digital Rights in a Time of Crisis: Authoritarianism, Political Tension and Weak Legislation Boost Violations – Digital Rights Violations Annual Report 2022-2023* (Balkan Investigative Reporting Network, 2023). Available as a pdf at: <https://birn.eu.com/wp-content/uploads/2023/12/01-BIRN-Digital-Rights-Violations-Annual-Report-2022-2023.pdf>.

³³ Ibid.

³⁴ Information provided by Prosecutor's Office in Tirana in response to a FOI request, on 24 November 2023.

³⁵ Ibid.

2.2.2 Did government reporting on the crisis meet transparency standards?

In the face of a crisis, international best practices recommend that governments conduct after-incident reviews and analysis. For the cyberattacks directed against Albania, publicly available analysis of this kind consists of a technical report by the Microsoft Detection and Response Team and the US FBI's Cyber Action Team, which aided the Albanian government in the aftermath of the attack.³⁶ It is this report that assigns attribution for the attack to Iranian actors, who are said to have infiltrated Albanian networks 14 months before executing the operation. In the opinion of a cybersecurity expert interviewed by the authors, this is 'not sufficient to ensure accountability', though, '*since it is not a[Albanian] government report, but a report by a private company, which is [above all] driven by economic interest.*'³⁷

The only relevant document offered by the Albanian government has been a three-page document issued by the NAIS itself, which reiterated the technical findings of the Microsoft report and acknowledged the sophistication of the attack, while emphasizing that only 10 percent of affected systems had been erased and that they were fully restored within a week due to backup policies and disaster recovery measures.³⁸ Problematically, some questionable additions to the document, such as a comparison between the gross domestic product (GDP) of Albania and the budget of the Iranian Revolutionary Guard – which appears to have been included in order to illustrate the scale of the problem and the government's relative helplessness in fighting attacks from certain sources – led to a perception of the document being more political than technical in nature.³⁹ Still, these reports addressed only the cyberattacks against the NAIS; meaning, there are no after-incident reports on the attacks directed against the Albanian State Police and other entities, nor on more recent attacks that occurred in 2023.⁴⁰

That said, according to the Prosecution Office in Tirana, the attacks against the NAIS and the State Police shared the same typology and arose from the same source, and are therefore being investigated as a single case.⁴¹ It is notable, however, that attempts by journalists to learn more

³⁶ See: Microsoft Threat Intelligence, 'Microsoft investigates Iranian attacks against the Albanian government', *Microsoft Security* (blog), 8 September 2022, <https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/>; US Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, 'Iranian State Actors Conduct Cyber Operations Against the Government of Albania', Joint Cybersecurity Advisory, AA22-264A, 21 September 2022.

³⁷ B.S., cybersecurity expert, interview by authors, 12 October 2023.

³⁸ NAIS, 'Sulmi kibernetik i 15 korrikut 2022 në Shqipëri: Një analizë e detajuar, sipas gjithë etapave që nga 15-16 korriku 2022' [The Cyberattack of July 15 2022 in Albania: A detailed analysis of all stages from 15-16 July 2022] (n.d.). Available as a pdf at: <https://akshi.gov.al/wp-content/uploads/2022/09/Raporti-i-plot%C3%AB-i-sulmit-kibernetik-t%C3%AB-15-korrikut-2022.pdf>.

³⁹ See: 'Sulmi kibernetik: neglizhencë e specialistëve apo institucioneve publike?', *Faktoje*, 1 December 2022, <https://faktoje.al/sulmi-kibernetik-neglizhence-e-specialisteve-apo-institucioneve-publike/>.

⁴⁰ F.S., journalist, interview by authors, 17 October 2023; B.S., cybersecurity expert, interview by authors, 12 October 2023.

⁴¹ Prosecutor's Office of Tirana, 'Njoftim i Prokurorisë Tiranë në lidhje me hetimet e ndërmarra ndaj sulmit në sistemet kompjuterike të institucioneve të Republikës së Shqipërisë' [Announcement of the Tirana Prosecutor's Office regarding the investigations undertaken into the attack on the computer systems of the institutions of the Republic of Albania], 20 September 2022, https://www.pp.gov.al/Tirane/Media/Njoftim_i_Prokurorisë_Tirane_ne_lidhje_me_hetimet_e_ndermarra_ndaj_sulmit_ne_sistemet_kompjuterike_te_institucioneve_te_Republikes_

about the implications of the attack on systems of the State Police have been met by inconsistent messaging and closed doors when soliciting information. For instance, one journalist who was interviewed for this research, and who works for a prominent regional outlet, has reported on the cyberattack on the TIMS system, but has found that different government institutions offer different assessments of the matter, or none at all: *‘The interior minister declared that TIMS data has not been compromised. The Prosecution of Tirana confirmed to journalists that a related case was referred to them. The Agency for Oversight of the State Police neither confirmed nor denied it.’*⁴² This runs contrary to best practices that call for a clear and coordinated communication strategy by governments in the wake of cybersecurity incidents (or other high-impact events), to address the public at large, as well as affected individuals and stakeholders.

Considering this confusion, and seeking transparency about the July 2022 cyberattacks, a journalist from a fact-checking organization in Albania engaged in a four-month email correspondence with the NAIS, from November 2022 through February 2023. The exchange revolved around various FOI requests that had gone unaddressed by the agency, eventually leading the journalist to file a complaint with the IDP Commissioner – who finalized the case through ‘mediation’ without compelling the NAIS to provide the information that had been requested.

Interviews with three journalists⁴³ and two cybersecurity experts who have worked to investigate and understand the attack, as well as a review of the FOIs submitted by the fact-checking organization mentioned above and related correspondence, clarified that key questions about the attack remain unanswered, including:

- *Which vulnerability facilitated the attack?*
- *Precisely which systems and data were affected?*
- *What damages/losses were incurred?*
- *Have all compromised data been recovered, or have some been lost permanently?*
- *What sequence of responses and measures were taken in the aftermath of the incident?*
- *What are the repercussions of the attack on systems of the State Police?*

This is information that Albanian citizens not only have an interest in, but a right to know, considering that they were among the data subjects affected - adding to the many reasons why effective communication during and after a crisis is essential. Furthermore, a commitment to communicating in a way that is forthright and transparent can mitigate the negative impacts of a crisis, and support lesson learning.⁴⁴ This requires the relevant authorities to provide regular updates on

[se_Shqiperise.html](#).

⁴² F.S., journalist, interview by authors, 17 October 2023.

⁴³ P.P., journalist, interview by authors, 10 November 2023; K.L., investigative journalist, interview by authors, 17 October 2023; F.S., journalist, interview by authors, 17 October 2023.

⁴⁴ Sanja Savić and Jovan Krivokapić, *Booklet on Crisis Communication* (Geneva: DCAF, 2022).

a crisis, describe the steps taken to resolve it, and educate anyone affected about how to protect themselves. Yet, when the authors inquired with the NAECCS as to whether a public communication plan had been developed by the government to coordinate messaging related to cyberattacks, such a plan was said to be in the process of being finalized, with approval expected soon, over 16 months *after* the incident in question.⁴⁵ Good practices recommend that crisis management and communication plans are instead developed in advance, so that they can guide decision making and citizens during high-impact events and help ensure that leaders are prepared to communicate effectively in the midst of crisis.

Notably, the institutional responses received by interviewees who pursued information about the cyberattack tended to reference the law, deny the specific responsibilities of the institution, or invoke ‘confidentiality’ to block requests, and did not provide even partial disclosures of information. This may represent a contravention of Albania’s Law on the Right to Information, which states that, “any time national security restrictions pertain only to part of a requested document, public authorities are mandated to clearly indicate which parts have been rejected while disclosing the rest of the information... to the applicant”.⁴⁶

Between 2021 and 2022, NAIS faced nine formal complaints for alleged violations of freedom of information, primarily from journalists.⁴⁷ However, because this agency combines reports on its FOI requests with other types of requests it receives (such as for technical assistance), it is impossible to determine the ratio of FOI requests to complaints and draw any conclusions on that basis. On the other hand, during the same period, NAECCS only received a single freedom of information request, resulting in no complaints. Experts interviewed for this research argued that this apparent relative disinterest reflects the perception that NAECCS is a technical body with limited competences. They therefore saw efforts to empower the institution as a positive step.

2.3 Testing the post-cyberattack transparency of public authorities

In November 2023, nearly a year-and-a-half after the July 2022 cyberattack, the Institute for Democracy and Mediation (IDM), submitted its own FOI requests to relevant authorities, as a testing and validation exercise. Much like the journalists mentioned above, the organization received no response to requests related to the most important questions, about assessments of damages and risks. The State Police and General Prosecution did not respond at all, for instance.⁴⁸ The NAIS responded very selectively, providing information related to the country’s Digital Agenda 2022-2026 and the Law on E-governance, while ignoring altogether, or refusing disclosure on

⁴⁵ Information provided by the NAECC in response to a FOI request, on 30 November 2023.

⁴⁶ Law on the Right to Information, No. 119/2014.

⁴⁷ Information from the Register of Complaints for 2021 and 2022, available on the website of the IDP Commissioner at: <https://idp.al/statistika-2/>.

⁴⁸ IDM submitted the FOI to the State Police on 16/11/2023; and the FOI to the General Prosecution on 20/11/2023.

legal grounds, ten other requests about cyberattacks, damage assessments, and preventive measures.⁴⁹ And the response of the NAECCS, while somewhat more forthcoming in other ways, noted that a damage assessment report submitted to authorities could not be provided due to its ‘confidential’ classification. They also informed being in the process of designing a methodology for national-level risk assessment while having implemented measures, such as operating the National Cyber Security Operational Centre 24/7, increasing the workforce, approving technical measures for information infrastructures, conducting training sessions, reviewing the cybersecurity law to ensure alignment with the EU 2022/2555 Directive of the European Parliament and of the Council (NIS2 Directive), developing of a national procedure for managing cyber crises, currently awaiting approval, assessing the security level of defence and security infrastructures, and reviewing the National Cyber Security Strategy.⁵⁰

The IDM also submitted FOI requests to the IDP Commissioner, which was relatively responsive but did not provide information about any recommendation or initiative to change the personal identification numbers of citizens, and did not furnish the Regulatory Impact Assessment for the new Law on Protection of Personal Data. The latter was suggested to be a document belonging to the Ministry of Justice which initiated the legislative amendment and led its consultation.⁵¹ The Prosecution Office in Tirana was the only public authority that responded comprehensively to a FOI request from the IDM, sharing information on the status of investigations within its jurisdiction, as well as details on the enforcement of a prosecutorial directive for non-disclosure of data related to the cyberattack. Nevertheless, in response to a request for statistical data on criminal offenses linked to or facilitated by the leak of personal and state data, as recorded by the Prosecution, the IDM was informed that, *‘Due to the electronic reporting system providing disaggregation based on names of individuals rather than the nature of the report (criminal offense), we have identified only two reported cases.’*⁵² This speaks to the importance of structuring the data collection systems in public entities in such a way that they are appropriately disaggregated, lest they impede access to information.⁵³

The responsiveness of Albanian public institutions to FOI requests of the IDM is summarized in Table 1, below, and illustrates the clear disparity in how they responded – reflecting the timely and comprehensive response of the Prosecutor’s Office in Tirana, the timely but partial response

⁴⁹ Information provided by the NIAS in response to a FOI request, on 7 December 2023.

⁵⁰ Information provided by the NAECCS in response to a FOI request, on 30 November 2023. The response of the NAECCS also highlighted that the institution was in the process of designing a methodology for national-level risk assessment, and listed measures that had already been implemented – such as expanding operations at the National Cyber Security Operational Center to a 24/7 timeline and increasing its workforce, approving technical measures for information infrastructures, conducting training sessions, reviewing the cybersecurity law to ensure alignment with the EU’s NIS2 Directive (on measures for a high common level of cybersecurity across the union), undertaking development of a national procedure for the management of cyber crises, assessing the security level of defense and security infrastructures, and reviewing the National Cyber Security Strategy.

⁵¹ Information provided by the IDP Commissioner in response to a FOI request, on 1 December 2023.

⁵² Information provided by the Prosecutor’s Office in Tirana in response to a FOI request, on 24 November 2023.

⁵³ Institute for Democracy and Mediation, *Civil Society Report on the Implementation of Chapter II (Prevention) & Chapter V (Asset Recovery) the United Nations Convention Against Corruption in Albania* (IDM and the UNCAC Coalition, 2023).

of the NAECCS and IDP Commissioner, the limited and untimely response of the NAIS, and the non-response of the State Police and General Prosecution. While the testing exercise validates several observed trends and provides a snapshot of the situation, it should be noted that the asymmetry in the nature and scope of questions posed to different institutions limits the comparative analysis – as FOI requests were tailored to each entity's roles, operational scope, and the information IDM had access to at the time of submission.

It is essential to recognize that while cyberattacks raise concerns related to security and state secrecy, adherence to international best practices necessitates a delicate equilibrium between transparency and security considerations to uphold public trust.

Table 1. Responsiveness of public authorities to FOI requests submitted by IDM

	Response received	Partial response	Complete response	Respected legal deadline
NAIS	x	x		
NAECCS	x	x		x
State Police				
IDP Commissioner	x	x		x
General Prosecution				
Prosecution Office Tirana	x		x	x

2.4 Perception of government's approach during and after the incidents

The response of the government to data breaches and cyberattacks in Albania has affected public trust in the capacity and reliability of the country's information systems. For example, a 2022 national survey measuring trust in governance found that 90.3 percent of respondents considered it critical to safeguard personal data, but that a substantial number lacked confidence in the handling of this data by public entities (59.8 percent) and by the private sector (58.8 percent).⁵⁴ One cybersecurity expert contextualized these findings in rather stark terms, remarking in an interview that, '*Unfortunately, [Albanian] citizens are more inclined to believe the hackers, who or-*

⁵⁴ Irma Semini, Besjana Kuçi, and Marsela Dauti, *Opinion Poll 2022: Trust in Governance*, 10th ed. (Tirana: Institute for Democracy and Mediation, 2023).

*chestrated what could be seen as a terrorist attack on our country, than to have faith in our state institutions.*⁵⁵

Regrettably, the handling of these cybersecurity breaches has also become a political battleground with both the government and the opposition capitalizing on the issue for political gain; prioritizing politics over citizen privacy and neglecting to address the real impact of these incidents on people's lives. The resulting political discord has sidelined any constructive discussion on preventive and protective measures, leaving the public confused by conflicting narratives and scarcely any more aware or educated on data protection than they were before.⁵⁶

Institutional accountability has taken a backseat to political discourse, allowing cybersecurity weaknesses to be minimized rather than resolved, and elevating political propaganda over substantive technical discussion. For instance, the interior minister swiftly assured the public that Police systems remained unbreeched; government officials accused journalists of slander and spreading panic; and the PM publicly disclosed his personal ID number to emphasize its harmlessness - all preceding thorough technical analysis. On another occasion, the PM asserted that the leak of salaries served as a lesson on the necessity to combat tax evasion. This prevailing approach carried the risk of desensitizing individuals through claims of '*having nothing to hide*'⁵⁷. By making these premature statements, political figures thus normalized the abnormal and created confusion⁵⁸, and contradicted the initial narrative of the government that the country was in 'a war', which prompted the unprecedented decision to cut diplomatic ties with Iran.⁵⁹

From the lenses of local journalists and fact-checkers, the approach the government took regarding the cyberattacks was political instead of technical, and aimed at reputational damage control, rather than taking responsibility and informing the public.⁶⁰

Interviewees pointed to a video released by Microsoft as an example.⁶¹ Featuring Albanian public officials from the NAIS, the promotional video showcases how Microsoft has supported the small nation in safeguarding its citizens and crucial infrastructure against cyber threats. The Albanian Prime Minister is portrayed as a hero for severing diplomatic relations with Iran following the 2022 cyberattack, and despite the significance of the data breaches the attack entailed, the attackers are said to have gained nothing in the end. This does not comport with publicly available information about the scope of the leaks.

⁵⁵ B.S., cybersecurity expert, interview by authors, 12 October 2023.

⁵⁶ B.S., cybersecurity expert, interview by authors, 12 October 2023.

⁵⁷ P.P., journalist, interview by authors, 10 November 2023.

⁵⁸ P.P., journalist, interview by authors, 10 November 2023.

⁵⁹ Fjori Sinoruka, "This is a War": Albania Struggles to Keep Lid on Hacked Data,' Balkan Insight, 28 September 2022, <https://balkaninsight.com/2022/09/28/this-is-a-war-albania-struggles-to-keep-lid-on-hacked-data/>.

⁶⁰ P.P., journalist, interview by authors, 10 November 2023.

⁶¹ Microsoft Security, 'How Microsoft Incident Response helped Albania respond to Iranian cyberattack,' YouTube video, 11:34, 1 August 2023, <https://www.youtube.com/watch?v=7YuSUYJUEZ0>.

One cybersecurity expert explained that governments often choose not to disclose the details of such incidents due to a sense of embarrassment associated with being hacked.⁶² But another interviewee, from civil society, noted that the NAIS had adopted an opaque approach, and according to the same interviewee, institutional transparency was the weakest element of the government's response chain.⁶³

Moreover, communication on data security remained ineffective. The failure to simplify technical policies for broader understanding disengaged the public and fostered an environment ripe for manipulation and non-transparency.⁶⁴

The deliberate exclusion of the public from discussions worsened the situation, highlighting institutions' responsibility to simplify technical policies for wider comprehension. This is especially concerning given that evaluations reveal a low level of basic digital skills among Albanian citizens, with only 23.8% possessing such skills, placing the country at the bottom of the rankings in Europe.⁶⁵ One interviewee emphasized that these concerns align with the initial findings of a recent national assessment of e-readiness in Albania, which measures the country's capacity and preparedness to engage in the digital realm⁶⁶. In this regard, several interviewees underscored the vital role played by civil society actors and experts in creating awareness about these issues.⁶⁷

Indeed, the recent data leaks and cyberattacks in Albania coincided with a rapid shift to digitalization that brought 95 percent of public services online by May 2022. This has sparked criticism of the government – for expecting public trust in new e-governance platforms when it has not adequately addressed these cybersecurity breaches;⁶⁸ as well as for failing to properly prepare the public and for overlooking the risk of human rights risks violations extending from inequities faced by individuals lacking digital skills, people with disabilities, and other groups.⁶⁹ In 2022, for instance, less than half of Albanian citizens (47.9 percent) managed to access public e-services independently, without assistance.⁷⁰

Experts interviewed for this research thus questioned the strategy of the Albanian government to over-rely on technology while leaving causal factors and risks un- or under-addressed. They stressed the importance of conducting thorough analyses and consultations before implementing policy in this area, to ensure a comprehensive and well-informed approach that corrects course

⁶² B.S., cybersecurity expert, interview by authors, 12 October 2023.

⁶³ B.B., civil society and media researcher, interview by authors, 27 October 2023.

⁶⁴ F.S., journalist, interview by authors, 17 October 2023.

⁶⁵ See: <https://ec.europa.eu/eurostat/databrowser/bookmark/f9251ed3-7236-4c44-b97b-0b2b44368d17?lang=en>

⁶⁶ B.K., researcher, interview by authors, 18 October 2023.

⁶⁷ B.K., researcher, interview by authors, 18 October 2023; A.H., civil society expert on children's online safety, interview by authors, 23 October 2023; and K.L., investigative journalist, interview by authors, 17 October 2023.

⁶⁸ P.P., journalist, interview by authors, 10 November 2023.

⁶⁹ Friedrich-Ebert-Stiftung, *Cybersecurity in Southeast Europe*.

⁷⁰ Semini, Kuçi, and Dauti, *Opinion Poll 2022: Trust in Governance*.

from the one applied in the aftermath of the cyberattack, which has fallen short in almost every way – in its effectiveness, meticulousness, consistency, and transparency. The poor handling of this and data violation incidents, has impacted public trust, and with it, public engagement. These shortcomings of governance, including the failures to prioritize citizen privacy and ensure institutional accountability, underscore the importance of adopting a more transparent, and citizen-centric approach to cybersecurity and digital governance in Albania, to rebuild trust and uphold integrity.

2.5 Media coverage of the incidents in Albania

A symbiotic relationship between civil society and media, complementing and reinforcing each other, forms the cornerstone of a functioning democracy. The media serves as the eyes and ears of the public, keeping citizens informed, holding power accountable, and facilitating public discourse; while civil society serves as the conscience and strength of the people, mobilizing collective action, advocating for change, and amplifying marginalized voices. In times of crisis, the role of media is particularly vital, as the delivery of timely and accurate information to the public acts as a beacon of truth amid turmoil, uncovering any violations or misuse of authority, energizing civil society into action.

Yet, following the 2022 cyberattack against the Albanian government, media outlets were barred from republishing leaked data and hacked files, as per a directive issued on 19 September by the Prosecution Office in Tirana – which prohibited ‘the publication of any data published by the perpetrators of the cyberattack’ and assigned not only the Police Cyber Unit, but the Authority for Electronic and Postal Communications and the Authority for Audio Visual Media, to enforce this ban across media and social media platforms.⁷¹ The involvement of these two independent bodies, acting on behalf of the Prosecutor’s Office, raised concern among organizations that advocate for media freedom.⁷² More broadly, the directive provoked contentious discussion, with some viewing it as necessary to preserve data confidentiality and others labelling it a form of censorship.⁷³ One IT expert put it bluntly, calling the directive nothing more than ‘*an attempt to limit public awareness*’ of the cyberattack by threatening ‘*media and journalists... that they can be imprisoned if they publish the data.*’⁷⁴

The directive also garnered criticism from both local and international media freedom organizations, in a joint public statement that appealed against the criminal prosecution of journalists,

⁷¹ ‘Notice of the Tirana Prosecutor’s Office regarding the investigations undertaken into the attack on the computer systems of the institutions of the Republic of Albania,’ 19 September 2022. Available at: https://www.pp.gov.al/Tirane/Media/Njoftim_i_Prokurorise_Tirane_ne_lidhje_me_hetimet_e_ndermarra_ndaj_sulmit_ne_sistemet_kompjuterike_te_institucioneve_te_Republikes_se_Shqiperise.html

⁷² See: European Centre for Press and Media Freedom, ‘Albania: Media must not face criminal prosecution for public interest reporting,’ <https://www.ecpmf.eu/albania-media-must-not-face-criminal-prosecution-for-public-interest-reporting/> (accessed 11 April 2024).

⁷³ Balkan Investigative Reporting Network (2023) Digital Rights Violations Annual Report 2022-2023 <https://birn.eu.com/wp-content/uploads/2023/12/01-BIRN-Digital-Rights-Violations-Annual-Report-2022-2023.pdf>

⁷⁴ Balkan Investigative Reporting Network, *Digital Rights in a Time of Crisis: Authoritarianism, Political Tension and Weak Legislation Boost Violations – Digital Rights Violations Annual Report 2022-2023* (2023), p. 32.

editors, or publishers in Albania for sharing ‘accurate information in the public interest.’ The statement urged media to handle sensitive material ‘in a strictly ethical and responsible manner’ but emphasized that threats of criminal investigation and website blocking could stifle reporting and potentially criminalize legitimate journalistic activities.⁷⁵

That said, according to the Prosecution Office in Tirana, the directive remains valid but has never been put into effect, ‘*due to compliance by... media outlets and journalists*.’⁷⁶ This is curious, however, because some media and journalists did in fact report publicly on the cyberattack and on the subsequent leaks, and not all of them did so in an ethical manner, as some relied on sensationalized content and propagated misinformation.⁷⁷ It is possible the directive was issued so swiftly but was not enforced, despite violations, as a means of encouraging self-censorship; however the potential impact of fear of prosecution on censorship cannot be quantified.

Beyond the question of whether leaked data was republished, the quality of media reporting on the cyberattack varied, in the view of experts. Mirroring the approach of government, most media coverage was politically focused, overlooking concerns for the privacy and safety of affected citizens and neglecting the importance of awareness raising. For instance, reporting on the leak of voter data largely ignored its privacy and safety implications, as well as the reasonable fears of those whose data was exposed. Similarly, analyses of the breach that exposed the salaries of public and private sector employees was focused on individual incomes, with little regard for privacy, discussing the highest earners at length and sidelining critical security aspects of the incident.⁷⁸

This failure to explore key questions of public interest was widespread. Still, the work of some outlets was marked by an investigative approach and journalistic integrity.⁷⁹ And, few outlets did provide space for independent experts and civil society actors, welcoming their contributions and working to bring more attention to the issue. A renowned investigative journalist underscored the lack of two-sided debates, attributing it to the government’s refusal to participate, thereby restricting expert input.⁸⁰ While recognizing the legitimacy of security concerns, the government’s hesitancy to engage in debates not only impeded discussions on technical aspects but also resulted in inadequate information for citizens.⁸¹ Cybersecurity experts and journalists agreed that this has created a severe lack of public awareness, the gravity of which is not fully appreciated by decision makers, and that additional efforts are necessary to effectively convey the urgency of the

75 European Centre for Press and Media Freedom, ‘Albania: Media must not face criminal prosecution for public interest reporting.’

76 Information provided by the Prosecutor’s Office in Tirana in response to a FOI request, on 24 November 2023.

77 ‘Portalet viktimë e hackerave iranianë për ministrat në listën e të dyshuarve,’ *Faktoje*, 12 October 2022, <https://faktoje.al/portalet-viktime-e-hackerave-iraniane-per-ministrat-ne-listen-e-te-dyshuarve/>.

78 Xhaferaj, Bino, and Curraj, ‘Working Paper: Mapping personal data violations in Albania’.

79 B.B., civil society and media researcher, interview by authors, 27 October 2023.

80 K.L., investigative journalist, interview by authors, 17 October 2023.

81 B.S., cybersecurity expert, interview by authors, 12 October 2023.

situation to the citizens. Ultimately, security considerations should not disproportionately impact the right of the public to be informed.

Two cybersecurity experts highlighted concerns that censorship is particularly prevalent at media outlets that have been contracted by government bodies to participate in public service promotion. One interviewee claimed to have been censored and denied airtime on these outlets despite being a prominent voice on the subject. He told the authors that his media appearances were cancelled, references to his name and quotes were deleted from articles, and reporting on his own efforts to strengthen accountability and report alleged corruption in the wake of the incidents was suppressed.⁸² From the journalists' perspective, independent experts have found some media coverage. However, one journalist said that experts were more likely to be invited to discuss the 2022 cyberattacks from Iran, than to address the leak of the voter database.⁸³ This suggests that there may be more leeway for public discussions of geopolitical or international security issues than for analysis of domestic cybersecurity issues and challenges. Another journalist disclosed being accused by government representatives of inciting panic, an apparent tactic for censorship.⁸⁴ Either way, there was consensus among interviewees that recent cybersecurity incidents in Albania must be kept in the public eye by media and should not be disregarded as 'old news', given their ongoing impact.

3. Areas for future engagement: insights from the Western Balkans

3.1 Replicable advocacy practices

In the Western Balkans, engaging civil society in cybersecurity governance has been a challenge, but there have been signs of progress. Across the region, a handful of organizations have led the way by playing a pivotal role in efforts to tackle cybersecurity issues through advocacy, research, education, outreach, and capacity-building activities. When breaches have occurred, these organizations have been spurred to action, conducting investigations, collaborating with regulatory bodies, and pressing for accountability.

For instance, the work of the Metamorphosis Foundation in North Macedonia is focused on critical areas such as the impact of disinformation on democratic processes, cybersecurity governance, and the intersection of gender and cybersecurity.⁸⁵ Their initiatives, like the Digital Agenda Observatory and empowering podcasts for CSOs, foster a resilient cybersecurity environment. Despite efforts, only a handful of CSOs actively address cybersecurity in North Macedonia.

⁸² G.P., IT expert and whistleblower, interview by authors, 11 October 2023.

⁸³ F.S., journalist, interview by authors, 17 October 2023.

⁸⁴ Interview with K.L., investigative journalist on 17/10/2023

⁸⁵ M.J., representative of the Metamorphosis Foundation, interview by authors, 7 July 2023.

Similarly, research efforts of other organizations in Albania, Kosovo, North Macedonia, Serbia, Bosnia and Herzegovina, and Montenegro, which form the Western Balkans Cybersecurity Research Network, contribute primarily to policy and awareness raising by producing studies and policy analyses that relate to cybersecurity and human rights.⁸⁶

In Serbia, organizations like SHARE Foundation have over a decade of experience and are significantly involved in the sector. However, the cybersecurity landscape in Serbia predominantly comprises private actors, with civic actors engaging more sporadically—a trend across the entire region. Yet the SHARE Foundation's journey highlights their evolution, from influencing legislation aligned with EU directives and producing educational publications on legal frameworks, to offering technical support – all while embodying a watchdog role that safeguards the public interest.⁸⁷ The impact of the organization has extended beyond national borders as well, through its support for and efforts to bolster the cyber resilience of other organizations in the region. For example, the SHARE Foundation's Digital Security Toolkit, an online resource available in multiple regional languages, aids civil society actors, activists, media professionals, and others in handling cybersecurity incidents, gathering digital evidence, and filing criminal complaints.⁸⁸ Additionally, the organization supports prosecution efforts to counter high-tech crime via a cooperation agreement and has established the SHARE CIRT (Cyber Incident Response Team) for online media and civil society, ensuring a seat at the table in policy discussions with the national CIRT and the Serbian Ministry of Information and Telecommunications. Although this kind of cooperation with civil society has not been widely embraced by the Serbian government, in this particular domain, the SHARE Foundation stands out as a crucial technical partner to decision makers.⁸⁹

Serbia is also the home to the Cybersecurity Network Foundation, an informal platform that facilitates multi-stakeholder engagement among actors from both the public and private sectors, academia, and civil society.⁹⁰ It serves as a hub for policy discussions on cybersecurity development, norms, strategies, and collaborative opportunities, providing a sorely needed forum for exchange in the fragmented and siloed cybersecurity landscape of the Western Balkans. Moreover, via its Cyber Hero initiative, the organization develops an interest in cybersecurity among high school and university students, to ensure a new generation of expertise and innovation.⁹¹

In BiH, which lacks both a state-level cybersecurity strategy and a national Computer Emergency Response Team (CERT), the Cyber Security Excellence Centre – established to deliver a research-based approach to cybersecurity, and engage in training, support, and awareness raising

⁸⁶ The Network includes: the Institute for Democracy and Mediation (Albania); the Balkan Investigative Reporting Network (BiH); the Kosovar Institute for Policy and Research (Kosovo); the Centre for Democratic Transition (Montenegro); the Metamorphosis Foundation (North Macedonia); and the Belgrade Centre for Security Policy (Serbia).

⁸⁷ B.P., representative of the SHARE Foundation, interview by authors, 1 November 2023.

⁸⁸ The Toolkit is available at: <https://toolkit.sharecert.rs/>.

⁸⁹ D.K., Associate Professor of ICT Law at the University of Belgrade, interview by authors, 23 August 2023.

⁹⁰ See the Foundation's website at: <https://cybersecurityserbia.rs/>

⁹¹ See the Cyber Hero website (in local language), at: <https://cyberhero.rs/>.

activities – is currently the only functional CERT in the country. The organization is thus ‘a national CERT-of-last-resort until an official national CERT is established’, while maintaining its focus on developing cybersecurity expertise in academia, independent media, and civil society.⁹² This work reflects a regional trend by which cybersecurity is becoming more academic, as academic institutions and particularly technical faculties play an increasingly significant role by contributing research, developing curriculum, and fostering expertise, in cooperation with civil society. Identified good practices involving cooperation with civil society organizations in this sphere are considered replicable.⁹³

Cooperation of this kind is a necessity in an evolving digital sector that demands a collaborative approach to fortifying cybersecurity frameworks, mitigating risks, and upholding fundamental rights in online spaces. To address skills gaps within the civil society sector, cybersecurity stakeholders should thus acknowledge the option of sourcing technical experts, including cybersecurity IT engineers, from academic institutions. It has been a challenge in the countries of the region to incorporate cybersecurity professionals into CSOs, and their small numbers has in turn made recruitment into the sector more difficult. But targeted outreach, in collaboration with academia, has the potential to attract early-career individuals to engage with or within civil society.⁹⁴

The mutual benefit of cooperative approaches to cybersecurity is inherently exemplified in initiatives such as the Southeast Europe (SEE) Digital Rights Network, a regional coalition formed in 2020 to address ‘digital rights abuses, lack of transparency and expanded use of invasive tech’ by facilitating solution-oriented dialogue among members – which include media and civil society organizations from across the Balkans, and broader.⁹⁵

Indeed, *while there is no universal remedy to guarantee online safety, establishing the community needed to counter and prevent digital risks will clearly require sustained efforts and cross-sector collaboration.* And the experiences of Albania only underscore the importance of strong civil society engagement in cybersecurity issues.

3.2 Opportunities for non-public actors to enhance their contribution to cybersecurity oversight in Albania

Successful ongoing initiatives in the region suggest there are ample opportunities for non-public actors to support informed decision-making in Albania, and to broaden their engagement in efforts to safeguard digital democracy by using data-driven analysis to advocate for policy change.

⁹² Friedrich-Ebert-Stiftung, *Cybersecurity in Southeast Europe*.

⁹³ D.K., Associate Professor of ICT Law at the University of Belgrade, interview by authors, 23 August 2023.

⁹⁴ D.K., Associate Professor of ICT Law at the University of Belgrade, interview by authors, 23 August 2023.

⁹⁵ See the Network’s website at: <https://www.seedigitalrights.network/>

For example, these non-public actors in Albania may assist the government in identifying and addressing cybersecurity vulnerabilities or may carry out community-engaged safety assessments to develop public safety strategies. A case in point is the work of Tirana-based IDRA Research & Consulting to enhance digital democracy by evaluating the digital readiness of local governments. These efforts are supported by the UNDP and produce assessments which are foundational to digitalizing public services in Albania, and to improving their accessibility, security, and efficiency. To that end, the IDRA has carried out a public survey, which found a moderate level of e-readiness among Albanians but a significant gap between digital readiness and accessibility. In other words, many citizens struggle to use or access online services. An evaluation of the cybersecurity preparedness of municipalities was also undertaken, through a review of policies, risk management protocols, and staff capacities.⁹⁶ Insights drawn from both of these assessments reveal critical areas for improvement in Albania's digital transition and provide important data that non-public actors can use to advocate for more inclusive cybersecurity policies and better digital infrastructure.

Among the enhancements that should be made to digital infrastructure in Albania are upgrades to the data collection systems used by public authorities, to facilitate data disaggregation. As highlighted in the discussion of post-cyberattack transparency above, the electronic reporting system currently used by the Prosecution (and State Police) limits disaggregation to such an extent that it affects the ability of public entities to be fully transparent. But such limitations also hinder institutions from effectively analysing data in support of institutional action and decision making. With incidents of cyber violence on the rise, particularly those aimed at minorities, children, women, and other marginalized groups particularly targeted by cybercrime, this lack of comprehensive data disaggregation is thus an obstacle to prevention; as improved data collection would facilitate analysis that sheds better light on the prevalence of cyber violence in Albania, enabling both public and non-public actors to strengthen their preventive efforts.

Overall, *Albanian policymakers and other cybersecurity stakeholders should explore ways to establish cooperation frameworks that empower non-public actors to engage in cybersecurity oversight.* As exemplified in Serbia, non-public actors can play a critical role in identifying and reporting system vulnerabilities, such as when the SHARE Foundation identified security flaws in the country's COVID patient data tracking system, including its publicly accessible login details. After they promptly reported these flaws to the authorities and the national CERT, swift action was taken to secure the system.⁹⁷ This proactive, collaborative approach increases the likelihood that potential threats are addressed before they can be exploited. This case serves as a reminder of the value that non-public actors bring to the table in managing crises, identifying gaps, advocating for enhanced security measures, and ultimately contributing to more informed and effective decision-making processes.

⁹⁶ B.K., researcher, interview by authors, 18 October 2023. Though the survey and evaluation data were not public at the time, the findings were shared in this interview.

⁹⁷ D.K., Associate Professor of ICT Law at the University of Belgrade, interview by authors, 23 August 2023.

Various experts who were interviewed for this research therefore emphasized the need to maintain communication channels between public and non-public cybersecurity professionals, to enable more inclusive and more diverse discussion regarding the handling of cybersecurity threats and the priorities of digital policymaking in Albania. Beyond this, there is room for technical cooperation as well. One IT expert put it bluntly during an event at the 2023 Geneva Peace Week, noting, '*We need resilience planning, because there is no state or company that cannot be hacked.*'⁹⁸ Considering the limited human resources available in the Albanian cybersecurity domain, owing in part to a brain drain from the country, private cybersecurity experts should be incentivized to help with testing for and alerting the NAIS about critical vulnerabilities. These experts should be vetted before they are authorized to conduct penetration tests; contributing to resilience planning and crises management. Following regional examples, the outcomes of these tests should be confidential until all risks are mitigated by Albanian authorities.

Broadly speaking, there is a significant potential for non-public actors in Albania to collaborate meaningfully and advocate effectively to increase accountability in digital governance and cybersecurity. Stronger synergies among these actors could help amplify feedback on legislative changes and shape effective digital policies and could be facilitated by the establishment of a 'community of practice' that enables them to jointly exert pressure on greater cybersecurity oversight.⁹⁹ This will better leverage existing expertise within the private sector and academia to fill gaps in digital policy advocacy. Still, to ensure a more inclusive and successful approach to digital governance and cybersecurity, it will also be necessary to expand the discourse to incorporate and mainstream gender perspectives, given the very gendered nature of much online violence and many cybercrimes.

In Albania, where some unique challenges to cybersecurity oversight practically necessitate a co-operative response involving non-public actors, the few CSOs that are actively engaged in safeguarding digital democracy lack many of the technical skills required to either effectively manage cybersecurity incidents or educate others in how to do so. There is a vital need for these organizations to collaborate more closely among themselves, to jointly develop research and advocacy, and to engage in activities that raise awareness and build capacity within their ranks. Recent cybersecurity breaches against non-public actors – such as those experienced in North Macedonia, where email server vulnerabilities led to ransomware attacks¹⁰⁰ – only make this kind of cooperation and capacity building more urgent. For, while cybersecurity challenges are a regional concern, the priority for Albania is to develop a robust internal network of expertise, including from the private sector, or alternatively, forging synergies with similar CSOs and academia in the region.

⁹⁸ 'Accountability and oversight in state responses to cybersecurity incidents: preparing for the future,' Geneva Peace Week, 31 October 2023.

⁹⁹ B.B., civil society and media researcher, interview by authors, 27 October 2023.

¹⁰⁰ Balkan Investigative Reporting Network, *Digital Rights in a Time of Crisis*.

The inadequate response by Albanian authorities to the various digital breaches that have affected citizens in the country has also demonstrated that there is a pressing need for non-public actors to play a role in raising awareness among the population about personal digital security and responsible data processing. *Efforts must be made to further educate the public on both the rights and risks they face in digital spaces, and how their personal information can be misused.* At the same time, public administration employees must be trained on the importance of data protection. This knowledge sharing is crucial if the country is to build a culture of digital literacy and security awareness at all levels, which is of paramount importance as public services in Albania are swiftly being digitized. In an interview, one expert described the country's shift to digitalization as so rapid that it has not given '*citizens time to absorb what digital really means, as they were mostly forced to accept it because it started during the pandemic and then it became a fait accompli.*'¹⁰¹ Hence, awareness-raising initiatives should provide educational resources that help citizens use public services, browse online safely, and recognize digital threats such as unauthorized social media access or phishing. So far, these efforts have been limited and targeted and have not matched the scope or speed with which services have been digitalized.

Awareness-raising should extend to public administration staff as well, to build institutional resilience against cyberattacks and strengthen data protection and cybersecurity practices, including among municipal-level workers, especially in smaller towns, where it is often a single person who handles sensitive data.¹⁰² Since June 2023, the Albanian School of Public Administration (ASPA) has been offering two tiers of cybersecurity training – basic and advanced – to public employees, but this capacity building should be complemented by targeted awareness raising.¹⁰³ Apart from information security notions, relevant regulations, and standards – these awareness-raising activities should aim to instil a sense of responsibility and caution in handling citizen data. In parallel, public campaigns led by cybersecurity experts should be launched to educate the public on the importance of digital awareness, elucidating the role and impact of new technologies and their associated risks, including digital surveillance, machine learning, and so-called artificial intelligence.¹⁰⁴ Moreover, institutions have a duty to demystify technical policies and cybersecurity measures by communicating them in lay terms.¹⁰⁵ This is where CSOs and technical experts can contribute significantly, by translating these policies into language that non-experts can digest and understand, and advocating for their proper implementation.

¹⁰¹ B.K., researcher, interview by authors, 18 October 2023.

¹⁰² B.K., researcher, interview by authors, 18 October 2023.

¹⁰³ See the ASPA website, at: <https://aspa.gov.al/en/>.

¹⁰⁴ Sinoruka, 'Albanian Plan to Use AI to Align Laws With EU Questioned'.

¹⁰⁵ P.P., journalist, interview by authors, 10 November 2023.

Conclusions

This research underscores the indispensable role of civil society and other non-public actors in addressing challenges to Albania's digital transformation, promoting cybersecurity oversight, and safeguarding digital rights. However, the impact of these actors on decision-making processes remains limited or has yielded minimal impact so far, and to date, their involvement in digital governance has often been superficial. In part, this is due to a deficiency in relevant technical expertise in Albanian civil society and among non-public actors. This has significantly hindered their capacity to meaningfully participate in decision making, effectively monitor state authorities, and increase technical cooperation. For this reason, it is imperative to foster greater cross-sectoral collaboration and support, to help maximize the potential for non-public actors to shape Albanian digital governance. Furthermore, ensuring that CSOs can engage in efforts to safeguard digital democracy without fear of censure or repercussion is vital. The ability to operate freely and without fear of punitive action is essential to the effectiveness of civil society in promoting good governance, particularly in cybersecurity and the protection of digital rights.

Analysed as a case study, the response of Albania to various digital threats sheds light on the ways that systemic deficiencies in institutional accountability and transparency can pose specific challenges to cybersecurity oversight, impacting everything from the effective management and mitigation of cybersecurity risks to the ability of non-public actors to exercise their watchdog role, inform the public, and contribute to crisis control. A paradigm shift towards a governance framework that prioritizes inclusivity, transparency, and accountability is needed in Albania, not only to strengthen its responsiveness but to enhance public trust in its digital infrastructure and governance, which will cultivate a more secure and resilient digital ecosystem overall. To support such a shift, non-public actors can deepen their work to fortify digital democracy and cybersecurity in Albania through capacity building, data-driven assessments, community engagement, and the adoption of successful practices from the region. By leveraging their expertise to advocate for policy reform in the public interest and to address cybersecurity vulnerabilities, non-public actors can thus play a crucial role in shaping Albania's digital future and ensuring the protection of digital rights for all citizens.

It is therefore promising that efforts are underway, spearheaded by CSOs, cybersecurity professionals, and media in Albania, to address the challenges and intricacies of the country's digital transformation in a way that emphasizes good governance and the protection of rights. The focus of these initiatives' ranges, from countering digital rights violations, to capacity building, to digital literacy promotion and cybersecurity advocacy. Nevertheless, the influence of non-public actors on decision making remains limited or has yielded minimal impact so far. In terms of capacity building, there are no publicly available independent evaluations assessing the impact of previous capacity building efforts with public administration staff.

But capacity building is necessary across all sectors, to enable a whole of society approach to cybersecurity. Indeed, cybersecurity, a relatively novel focus for civil society, is approached predominantly through its intersections with human rights such as freedom of information, privacy rights, and the protection of children's and women's rights. As many of the experts interviewed for this research acknowledged, a shortfall in relevant technical expertise within Albanian civil society has prevented the sector from contributing to cybersecurity oversight in any significant way. Collectively, however, donor-supported initiatives aimed at complementing the Albanian government's priorities of cybersecurity preparedness and digitalization of services, combined with the activities of activists, some CSOs, and media to foster accountability, raise awareness, and counter digital rights violations, have the potential to foster a truly secure, inclusive, and transparent digital environment in Albania.

Accountability is one of the most neglected aspects in cybersecurity governance. Accountability in cybersecurity is not often enough discussed and existing tools for state security oversight are not used enough for cybersecurity.

From the chapters in this book the following can be concluded:

Chapter 3 describes the discussions held at international level to find mechanisms for holding those states that commit cyber attacks to account.

Accountability should also ensure that those responsible for providing cybersecurity are held to account if this security is not provided. The other 4 chapters of the book show that there is great potential but also shortcomings in capacities of the traditional oversight actors to ensure state's accountability in cybersecurity.

Chapter 1 sets out case studies of successful oversight of cybersecurity national parliaments.

Chapter 4 further elaborates on the activities that parliaments could take in overseeing cybersecurity. It also gives a warning about the lack of capacities that many parliaments have. It is important to support parliaments with capacity building and help them to better define their mandate for cybersecurity oversight.

Chapter 2 examines the role that of ombuds institutions in the Western Balkans have taken in overseeing cybersecurity. The chapter shows how it is difficult for an oversight actor to get involved in cybersecurity oversight. The institutions are short-staffed and lack expertise; they are concerned with many other important issues that they might consider more closely related to their core mandate.

Chapter 5 is a case study from Albania that shows that civil society is very interested and sees a clear link between human rights, civic rights and good cybersecurity governance. They are keen to examine the state and quality of cybersecurity. But they have difficulty in doing so often because of lack of capacities and funding.

It is essential to ensure that parliaments and independent state bodies, such as ombuds-institutions, are granted a clear legal mandate to engage in cybersecurity oversight. In the same vein, civil society and academic institutions require training and support to contribute meaningfully to this oversight process, ensuring a more robust approach to cybersecurity governance.

Investment in developing education and training programs to cultivate experts in cybersecurity policy is of critical importance. Simultaneously, oversight institutions must find ways and means to attract these specialists. Without access to skilled experts capable of evaluating policies, overseeing their implementation, and assessing their actual or potential impact on all segments of society, oversight institutions will struggle to fulfill their mandates effectively.



Chemin Eugène-Rigot 2E
P.O.Box 1360
CH-1211 Geneva 1
Switzerland

✉ info@dcaf.ch

☎ +41 22 730 94 00



www.dcaf.ch
